



**UNIVERSIDADE FEDERAL RURAL DO RIO DE JANEIRO**

**INSTITUTO DE CIÊNCIAS EXATAS**

**CURSO DE GRADUAÇÃO EM MATEMÁTICA**

**Lucas Corrêa Lopes**

**Os Teoremas de Philip Hall e uma caracterização para  
Grupos Solúveis**

**SEROPÉDICA**

**2018**



Lucas Corrêa Lopes

## Os Teoremas de Philip Hall e uma caracterização para Grupos Solúveis

Monografia apresentada à Banca Examinadora da Universidade Federal Rural do Rio de Janeiro, como requisito parcial para obtenção do título de Bacharel em Matemática, sob a orientação do Prof. Dr. André Luiz Martins Pereira.

SEROPÉDICA

2018

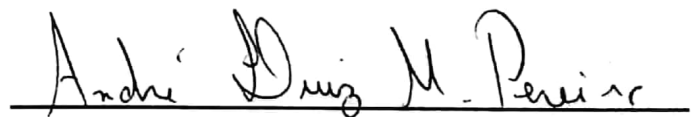
**UNIVERSIDADE FEDERAL RURAL DO RIO DE JANEIRO**  
**INSTITUTO DE CIÊNCIAS EXATAS**  
**DEPARTAMENTO DE MATEMÁTICA**

**COORDENAÇÃO DO CURSO DE GRADUAÇÃO EM**  
**MATEMÁTICA.**

A monografia “OS TEOREMAS DE PHILIP HALL E UMA CARACTERIZAÇÃO PARA GRUPOS SOLÚVEIS”, apresentada e defendida por LUCAS CORRÊA LOPES matrícula 201519028-5 foi aprovada pela Banca Examinadora, com conceito “S” recebendo o número 700.

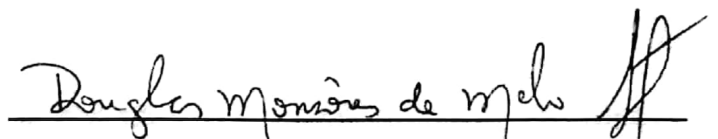
Seropédica, 14 de novembro de 2018.

**BANCA EXAMINADORA**

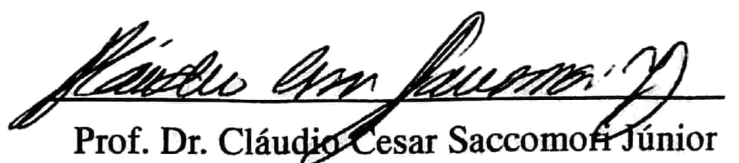


**Prof. Dr. André Luiz Martins Pereira**

**Orientador**



**Prof. Dr. Douglas Monsôres de Melo Santos**



**Prof. Dr. Cláudio Cesar Saccomoni Júnior**

*“Não! Tentar não. Faça ou não  
faça. Tentativa não há”.*

*Star Wars - O Império Contra-Ataca.*

# Agradecimentos

Em primeiro lugar, agradeço a Deus que me deu forças para chegar até aqui, prosperou o meu esforço e foi fundamental em todas as minhas (poucas) conquistas. Não existe nenhum meio de expressar o quanto sou grato por tudo.

Agradeço à minha família, minha avó Ivete, minha mãe Luciene, meu irmão Matheus e meu tio Heitor, que são responsáveis por boa parte do que eu sou hoje. Também por todo apoio que eu recebi. Em especial, ao meu pai, Alexandre, que fez mais do que podia por mim e me deixou ótimas memórias (e muita saudade). Também ao meu avô, José Dutra, por (além de tudo que já foi citado) todo o apoio financeiro durante 3 anos de minha graduação.

Agradeço à minha namorada, Beatriz pela compreensão em todos os momentos que precisei passar a maior parte do tempo com os livros, especialmente nesse ano de 2018. Certamente não é com poucas palavras que poderia agradecê-la como gostaria. Também agradeço aos meus sogros Flávio e Clarice, à Expedito e Dirce, e à Priscilla por serem minha segunda família e me tratarem sempre muito bem.

Agradeço ao meu orientador Prof. Dr. André Martins pelo apoio inestimável durante toda a minha graduação. Pelo curso, a princípio assustador de Cálculo 2, que me fez decidir pela Matemática Pura. Pela excepcional orientação durante a Iniciação Científica, que me fez apreciar um pouquinho do que é a pesquisa em matemática. Pela ajuda na maior parte das matérias da graduação, assim como durante o curso de verão e no início do mestrado.

Agradeço ao Prof. Dr. Douglas Monsôres pelo excelente curso de Álgebra

1 que me fez apreciar a beleza da Álgebra Abstrata e pelo excelente trabalho como coordenador.

Agradeço ao Prof. Dr. Cláudio Saccomori pelas preciosas dicas de  $\text{\LaTeX}$  durante o curso de Introdução às Curvas Algébricas, que melhoraram muito a estética da minha escrita e pouparam muito tempo.

Agradeço aos meus amigos Daniel, Matheus, Victor, Geovane, Ulises e Gabriel por todos os momentos de descontração e também pela ajuda recebida quando precisei. Também a muitos outros que não caberia citar aqui.

Agradeço ao CNPq pelo suporte financeiro que proporcionou o início deste trabalho, como um projeto de Iniciação Científica.

Agradeço à Universidade Federal Rural do Rio de Janeiro por, apesar dos inúmeros problemas, ser um lugar onde ainda se pode buscar conhecimento gratuitamente e de qualidade.

Por fim, agradeço à todos que contribuíram direta, ou indiretamente, para a realização desse trabalho.

## Resumo

O objetivo desta monografia é demonstrar dois dos mais importantes teoremas da Teoria de Grupos Finitos, que são de autoria do matemático inglês Philip Hall. O primeiro Teorema de Philip Hall, que foi provado em 1928, tem como sua principal importância, a generalização do famoso Teorema de Sylow, desde que, admitamos a hipótese do grupo  $G$  ser solúvel, grupos estes que constituem uma das mais importantes classes de grupos. O segundo Teorema de Philip Hall, que foi provado em 1937, tem como ponto principal fornecer uma caracterização dos Grupos Solúveis. Para fornecer uma demonstração acessível ao segundo teorema, precisaremos utilizar outro resultado muito importante da Teoria de Grupos, o Teorema de Burnside. A prova desse teorema será baseada na Teoria da Representação de Grupos e na Teoria dos Caracteres de Grupos.

**Palavras-Chave:** O Teorema de Philip Hall; Teorema de Burnside; Grupos Solúveis; Representações de Grupos; Teoria de Caracteres de Grupos.

## **Abstract**

The purpose of this monography is to demonstrate two of the most important theorems of the Finite Group Theory, which are authored by the english mathematician Philip Hall. The first Philip Hall's Theorem, which was proved in 1928, has as it's main importance the generalization of the famous Sylow's Theorem, provided that we assume the hypothesis of the group  $G$  to be soluble, groups that constitute one of the most important classes of groups. The second Philip Hall's Theorem, which was proved in 1937, has as it's main point to provide a characterization of the Soluble Groups. To provide an accessible demonstration to the second theorem, we will need to use another very important result of Group Theory, the Burnside's Theorem. The proof of this theorem will be based on Group Representation Theory and Character Theory of Groups.

**Key-Words:** The Philip Hall's Theorem; Burnside's Theorem; Soluble Groups; Representations of Groups; Character Theory of Groups.



# Sumário

<b>Introdução</b>	<b>1</b>
<b>Notações</b>	<b>1</b>
<b>1 Resultados Básicos</b>	<b>3</b>
1.1 O Teorema de Lagrange . . . . .	3
1.2 Homomorfismo e Isomorfismo . . . . .	5
1.3 Subgrupo Normal e Grupo Quociente . . . . .	6
1.4 Princípio de Contagem . . . . .	10
<b>2 O Teorema de Sylow</b>	<b>12</b>
2.1 Outro Princípio de Contagem . . . . .	12
2.2 Teorema de Sylow . . . . .	15
<b>3 Grupos Solúveis e Grupos Nilpotentes</b>	<b>21</b>
3.1 Grupos Solúveis . . . . .	21
3.2 Condições suficientes para solubilidade . . . . .	23
3.3 O Teorema de Wielandt . . . . .	27
3.4 Grupos Nilpotentes . . . . .	29
<b>4 O Teorema de Philip Hall (1928)</b>	<b>31</b>
4.1 Subgrupos de Hall e Lemas auxiliares . . . . .	31
4.2 Primeiro Teorema de Philip Hall . . . . .	34

<b>5</b>	<b>Teoria das Representações</b>	<b>42</b>
5.1	Representações de Grupos . . . . .	42
5.2	$FG$ -módulos . . . . .	44
5.3	Módulos irredutíveis . . . . .	46
<b>6</b>	<b>Teoria dos Caracteres</b>	<b>49</b>
6.1	Caracteres de Grupos . . . . .	49
6.2	Produto Interno de Caracteres . . . . .	52
6.3	Tabela de Caracteres e Relações de Ortogonalidade . . . . .	55
6.4	Inteiros Algébricos . . . . .	57
<b>7</b>	<b>O Teorema de Burnside</b>	<b>62</b>
7.1	Números Algébricos . . . . .	62
7.2	Teorema de Burnside . . . . .	65
<b>8</b>	<b>O Teorema de Philip Hall (1937)</b>	<b>67</b>
8.1	Sistema de Sylow e Base de Sylow . . . . .	67
8.2	Segundo Teorema de Philip Hall . . . . .	71
	<b>Considerações Finais</b>	<b>73</b>
	<b>Referências Bibliográficas</b>	<b>74</b>

# Introdução

O nosso objetivo é desenvolver alguns conceitos de Teoria de Grupos a fim de obter uma condição necessária e suficiente para a determinação da solubilidade de um grupo. Esta monografia é um desdobramento do trabalho desenvolvido durante o Programa de Iniciação Científica, que teve como objetivo estudar as propriedades dos Grupos Solúveis a fim de obter uma generalização para o Teorema de Sylow. Começaremos este trabalho apresentando alguns resultados básicos sobre Teoria de Grupos que serão importantes para tudo o que os sucede. Um dos pontos destacados do primeiro capítulo é o Teorema de Lagrange, que nos dá um modo relativamente simples para verificar se determinado subconjunto de um grupo  $G$  pode ser ou não um subgrupo de  $G$ , através da quantidade de elementos. Esse teorema nos diz que se  $H$  é um subgrupo de  $G$ , então  $|H|$  divide  $|G|$ . Uma questão interessante é se a recíproca desse teorema é verdadeira. Caso seja, nos daria um critério que facilitaria muito a determinação dos subgrupos de um determinado grupo. Mas a recíproca é falsa e é relativamente simples encontrar contraexemplos. No entanto, existe um resultado muito famoso que sob certas condições, fornece quase uma recíproca do Teorema de Lagrange, é o Teorema de Sylow que apresentaremos no capítulo 2. No capítulo 3, estudaremos as propriedades dos Grupos Solúveis, que são de extrema importância na Teoria de Grupos. Como exemplo, é devido a não solubilidade do grupo  $A_5$  que pode-se mostrar não existir uma fórmula, por meio de radicais, que forneça as raízes para um polinômio de grau maior ou igual a 5. Ao final do capítulo, estudaremos também os Grupos Nilpotentes, que serão usados na demonstração de um dos principais resultados do trabalho. O capítulo 4 é o motivo do estudo sobre Grupos Solúveis. Nele provaremos o Teorema de Philip Hall de 1928

que é o primeiro resultado central desse trabalho. A importância desse resultado é generalizar o Teorema de Sylow para a classe dos Grupos Solúveis. Nos capítulos 5 e 6 desenvolveremos a Teoria das Representações de Grupos e a Teoria dos Caracteres de Grupos que serão fundamentais para a demonstração de um teorema central neste trabalho, que é o Teorema de Burnside. Esse teorema pode ser provado somente com técnicas da Teoria de Grupos, porém a demonstração é muito mais complexa, exigindo maior profundidade na Teoria de Grupos e muito mais páginas escritas. Por esse motivo usaremos as teorias desenvolvidas nos capítulos 5 e 6. No capítulo 7, tendo em mãos os resultados obtidos nos dois capítulos anteriores, provaremos um primeiro resultado devido à Burnside que implicará diretamente na demonstração do Teorema de Burnside. No capítulo 8, provaremos o último resultado principal, o Teorema de Philip Hall de 1937. Ele fornece uma recíproca para o primeiro teorema e assim, estabelece um critério, através dos subgrupos de Hall, para a caracterização dos Grupos Solúveis. Com a demonstração do segundo teorema, encerramos nosso objetivo. É recomendado que, para a leitura dessa monografia, o leitor tenha conhecimentos prévios sobre Teoria de Grupos. Um curso de graduação sobre Teoria de Grupos desejável.

# Notações

As seguintes notações serão frequentemente usadas:

$G$	–	grupo finito
$g$	–	elemento de $G$
$ G $	–	ordem do grupo
$H \leq G$	–	$H$ subgrupo de $G$
$[G : H]$	–	índice de $H$ em $G$
$gH, Hg$	–	classe lateral de $H$ em $G$
$ gH ,  Hg $	–	cardinalidade da classe lateral
$H \triangleleft G$	–	$H$ subgrupo normal de $G$
$G/H$	–	grupo quociente
$G \simeq H$	–	$G$ isomorfo a $H$
$N^g$	–	conjugado de $N$ por $g$
$C_G(a)$	–	classe de conjugação de $a$ em relação a $G$
$N_G(a)$	–	normalizador de $a$ em $G$
$N_G(H)$	–	normalizador de $H$ em $G$
$Z(G)$	–	centro de $G$
$\dot{\cup}$	–	união disjunta
$[x, y]$	–	comutador de $x$ e $y$
$G'$	–	subgrupo derivado
$\mathcal{D}_i(G)$	–	subgrupo comutador superior
$C_p$	–	grupo cíclico de ordem $p$

$\text{GL}(n, F)$  – grupo das matrizes invertíveis de ordem  $n$  definidas em  $F$

$\text{tr} A$  – traço da matriz  $A$

$\chi$  – caracter de  $G$

$\overline{C}$  – classe da soma

# Capítulo 1

## Resultados Básicos

Neste capítulo, iremos apresentar alguns resultados elementares da teoria de grupos. Esses resultados serão indispensáveis ao longo do texto e sendo assim, é fundamental que o leitor compreenda, de forma clara, este capítulo. Para uma leitura mais completa sobre a teoria elementar de grupos, recomendamos que o leitor consulte [6].

### 1.1 O Teorema de Lagrange

O Teorema de Lagrange é o resultado que motiva o Teorema de Sylow. Esse teorema relaciona as ordens dos subgrupos de um determinado grupo por meio da divisão euclidiana.

**Definição 1.1.1.** Sejam  $G$  um grupo finito e  $H$  um subgrupo de  $G$ . Se  $g \in G$ , os conjuntos  $gH = \{gh \mid h \in H\}$  e  $Hg = \{hg \mid h \in H\}$  são chamados de *classe lateral à esquerda de  $H$  em  $G$*  e *classe lateral à direita de  $H$  em  $G$* , respectivamente. Denotaremos a cardinalidade do conjunto das classes laterais à esquerda (ou à direita) de  $H$  em  $G$  por  $[G : H]$  e tal número será chamado de *índice* de  $H$  em  $G$ .

**Teorema 1.1.2** (Teorema de Lagrange). *Sejam  $G$  um grupo finito e  $H$  um subgrupo de  $G$ , então  $|H|$  divide  $|G|$ .*

A ideia dessa demonstração é bastante intuitiva. Iremos particionar o grupo  $G$  em classes laterais disjuntas em relação à  $H$  e obteremos a ordem de  $G$  em função

da quantidade de classes distintas em relação à  $H$ . Como a ordem das classes laterais de  $H$  em  $G$  é igual à ordem de  $H$ , a relação anterior se tornará uma igualdade entre a ordem de  $G$  e o produto da quantidade de classes laterais com a ordem de  $H$ . Vejamos:

*Demonstração.* Note que como  $H$  é um subgrupo de  $G$ ,  $|H| \leq |G|$ . Fixado  $g \in G$ , considere a função  $\varphi : H \rightarrow gH$  definida por  $\varphi(h) = gh$ . Assim

$$\varphi(h_1) = \varphi(h_2) \implies gh_1 = gh_2 \implies h_1 = h_2,$$

o que mostra a injetividade de  $\varphi$ . É claro que  $|gH| \leq |H|$  e como  $G$  é finito,  $H$  também é. Com isso,  $\varphi$  é bijetora e, portanto,  $|H| = |gH|$ . Novamente, pela finitude de  $G$ , existem finitas classe laterais de  $H$  em  $G$ , ou seja,  $[G : H]$  é finito. Lembrando que uma classe lateral é uma relação de equivalência (ver [6]), vemos que  $g_1H \neq g_2H$  implica  $g_1H \cap g_2H = \emptyset$ . Uma vez que  $[G : H] = d$ , existem  $d$  classes laterias distintas, isto é,  $g_1H, \dots, g_dH$ . Logo,

$$G = \bigcup_{i=1}^d g_iH,$$

onde a união é disjunta. Isso nos permite escrever

$$|G| = \sum_{i=1}^d |g_iH|,$$

Então

$$|G| = \sum_{i=1}^d |g_iH| = \sum_{i=1}^d |H| = d|H|,$$

isto é,

$$\frac{|G|}{|H|} = d.$$

□

Com o Teorema de Lagrange, temos um critério simples para determinar, à primeira vista, se um subconjunto de um grupo não é um subgrupo.

**Exemplo 1.1.3.** Seja  $G$  um conjunto tal que  $|G| = p$  com  $p$  primo maior que 2. Se  $H$  é um subconjunto de  $G$  com  $|H| = n$  onde  $n \in \{2, \dots, p-1\}$ , podemos imediatamente afirmar que  $H$  não é um subgrupo de  $G$ . Se  $G$  for um grupo de ordem ímpar, então  $G$  não possui subgrupos de ordem par.



## 1.2 Homomorfismo e Isomorfismo

Um dos conceitos no qual se baseia boa parte da matemática é a ideia de homomorfismo. Um homomorfismo, basicamente, preserva a estrutura algébrica de certos objetos matemáticos. Dentre todos os tipos de homomorfismos, o isomorfismo tem um papel de protagonismo em diferentes áreas da matemática. O isomorfismo nos permite classificar dois conjuntos de naturezas diferentes numa mesma categoria e com isso, ao invés de estudarmos as propriedades em um conjunto “muito complicado”, podemos obter outro conjunto da mesma categoria que torne nossa análise mais simples. Ao longo desse texto, sempre que for dito homomorfismo, subentende-se que se trata de um homomorfismo de grupos. Quando nos referirmos a homomorfismos em outras estruturas algébricas, o faremos explicitamente.

**Definição 1.2.1.** Sejam  $G, H$  grupos e  $\varphi : G \rightarrow H$ . Dizemos que  $\varphi$  é um *homomorfismo* se  $\varphi$  satisfaz:

$$\varphi(g_1 g_2) = \varphi(g_1) \varphi(g_2), \quad \forall g_1, g_2 \in G$$

Na igualdade acima, o produto do lado esquerdo é o definido em  $G$  e o produto do lado direito é o definido em  $H$ .

**Definição 1.2.2.** Seja  $\varphi : G \rightarrow H$  um homomorfismo. Então

- (i)  $\varphi$  é chamado de *homomorfismo trivial* se  $\varphi(g) = e$  para todo  $g \in G$ .
- (ii)  $\varphi$  é chamado de *endomorfismo* se  $\varphi$  é um homomorfismo e  $G = H$ .
- (iii)  $\varphi$  é chamado de *isomorfismo* se  $\varphi$  é uma bijeção. Nesse caso escrevemos  $G \simeq H$  e dizemos que  $G$  é *isomorfo* à  $H$ .
- (iv)  $\varphi$  é chamado de *automorfismo* se  $\varphi$  é um isomorfismo e  $G = H$ .

Para exemplificar a utilidade dos isomorfismos, por meio deles podemos mostrar que é possível dividir todos os grupos de ordem 6 em duas classes. Mais precisamente, se  $G$  é um grupo de ordem 6 então ou  $G \simeq \mathbb{Z}_6$  ou  $G \simeq S_3$ . Para consultar uma classificação dos grupos de ordem menor ou igual a 15, ver [4].

**Definição 1.2.3.** Seja  $\varphi : G \rightarrow H$  um homomorfismo. O conjunto

$$\{g \in G \mid \varphi(g) = e_H\}$$

é chamado *núcleo* de  $\varphi$ . Denotamos o núcleo de um homomorfismo  $\varphi$  por  $\ker \varphi$ .

**Proposição 1.2.4.** *Sejam  $\varphi : G \rightarrow H$  e  $\psi : H \rightarrow K$  homomorfismos. Então*

- (i)  $\varphi(e_G) = e_H$ .
- (ii)  $\varphi(g^{-1}) = \varphi(g)^{-1}$  para todo  $g \in G$ .
- (iii)  $\psi \circ \varphi : G \rightarrow K$  é um homomorfismo.
- (iv)  $\varphi(G)$  é um subgrupo de  $H$ .
- (v) se  $\varphi$  é isomorfismo, então  $\varphi^{-1}$  também é.
- (vi)  $\varphi$  é injetivo se, e somente se,  $\ker \varphi = \{e\}$ .

*Demonstração.* Ver [14, p. 70].

□

## 1.3 Subgrupo Normal e Grupo Quociente

A Teoria de Galois surgiu após um trabalho do matemático Évarist Galois, que tinha como objetivo estudar a obtenção de raízes para polinômios de grau maior ou igual a 5. A Teoria de Grupos foi protagonista para que Galois pudesse provar que não é possível obter uma fórmula para todo polinômio de grau maior ou igual a 5 apenas em função dos coeficientes do polinômio que fornece suas raízes. Nesse trabalho, uma estrutura chamada de subgrupo normal desempenhou papel fundamental, fazendo uma conexão entre grupos e extensões de corpos. Além disso, o conceito de normalidade gerou um critério para solubilidade de grupos (que veremos adiante), que por sua vez, está relacionada com a solubilidade de polinômios. Também os subgrupos normais, dão origem a uma natureza diferente de grupo, o qual é formado por classes laterais: o *grupo quociente*.

**Definição 1.3.1.** Sejam  $G$  um grupo e  $N$  um subgrupo de  $G$ . Dizemos que  $N$  é um *subgrupo normal* de  $G$  quando  $gN = Ng$  para todo  $g \in G$ . Escrevemos  $N \triangleleft G$  para significar que  $N$  é um subgrupo normal de  $G$ .

Os subgrupos normais podem ser definidos aparentemente de forma um pouco mais geral, isto é,  $N$  é um subgrupo normal de  $G$  quando toda classe lateral à esquerda de  $N$  é uma classe lateral à direita de  $N$ . Contudo, é de fácil verificação que essa definição é equivalente à que demos. Essa equivalência se deve ao fato de duas classes laterais à esquerda (ou à direita) serem iguais ou disjuntas. Além dessas duas caracterizações para um subgrupo ser normal, podemos obter ainda uma terceira que é:  $N$  é um subgrupo normal de  $G$  se, e somente se,  $gNg^{-1} \subset N$  para todo  $g \in G$ . A equivalência dessa definição com as duas já apresentadas também é de verificação imediata ([4]), o que também nos permitiria usá-la de forma justa como definição nesse texto.

Uma última observação é que podemos denotar o conjugado de um grupo  $N$ , isto é, o conjunto  $gNg^{-1}$  para algum  $g \in G$ , por  $N^g$ . Algumas vezes isso é conveniente para reduzir a notação e, assim faremos algumas vezes em capítulos posteriores.

**Exemplo 1.3.2.** Seja  $\varphi : G \rightarrow H$  um homomorfismo. Decorre das propriedades de homomorfismos que  $\ker \varphi$  é um subgrupo de  $G$ . Se  $g \in G$  e  $n \in \ker \varphi$ , então

$$\varphi(gng^{-1}) = \varphi(g)\varphi(n)\varphi(g)^{-1} = e_H.$$

Com isso,  $gng^{-1} \in \ker \varphi$ . Logo,  $g \ker \varphi g^{-1} \subset \ker \varphi$  e, portanto,  $\ker \varphi \triangleleft G$ .

**Proposição 1.3.3.** Sejam  $G$  um grupo e  $N$  um subgrupo normal de  $G$ . O conjunto

$$G/N = \{gN \mid g \in G\}$$

é um grupo com a operação induzida por  $G$  da seguinte maneira:  $(g_1N)(g_2N) = (g_1g_2)N$ . Além disso,  $|G/N| = [G : N]$ .

*Demonstração.* Ver [14, p. 73]. □

**Definição 1.3.4.** O grupo definido na proposição 1.3.3 é chamado de *grupo quociente* de  $G$  por  $N$ .

O leitor mais atento notará que para um homomorfismo  $\varphi$  definido num grupo  $G$ ,  $G/\ker \varphi$  é um grupo quociente. Assim, a estrutura de grupo quociente está visivelmente relacionada com os homomorfismos. Com isso, é de se esperar que os dois conceitos nos forneçam uma propriedade não trivial. É o que veremos nos próximos resultados. A relação entre grupo quociente e homomorfismo nos permitirá obter quatro importantes resultados que serão usados ao longo do texto.

**Teorema 1.3.5** (Primeiro Teorema do Isomorfismo). *Sejam  $G, H$  grupos e  $\varphi : G \rightarrow H$  um homomorfismo. Então*

$$G/\ker \varphi \simeq \text{Im} \varphi.$$

*Demonstração.* Seja  $K = \ker \varphi$  e definamos  $\psi : G/K \rightarrow \text{Im} \varphi$  por

$$\psi(gK) = \varphi(g).$$

Suponha  $g_1K = g_2K$ , então  $g_2^{-1}g_1 \in K$ . Assim,  $\varphi(g_2^{-1}g_1) = e_H$  o que implica  $\varphi(g_2^{-1})\varphi(g_1) = e_H$ , isto é,  $\varphi(g_1) = \varphi(g_2)$ , logo  $\psi$  está bem definido. Como  $\varphi : G \rightarrow \varphi(G)$  é sobrejetivo,  $\psi$  é sobrejetivo. Note que

$$\varphi(g_1) = \varphi(g_2) \implies \varphi(g_1g_2^{-1}) = e_H \implies g_1g_2^{-1} \in K \implies g_1K = g_2K$$

e assim,  $\psi$  é injetivo. Logo,  $\psi$  é uma bijeção. Agora

$$\begin{aligned} \psi((g_1K)(g_2K)) &= \psi(g_1g_2K) \\ &= \varphi(g_1g_2) \\ &= \varphi(g_1)\varphi(g_2) \\ &= \psi(g_1K)\psi(g_2K). \end{aligned}$$

Portanto,  $\psi$  é um isomorfismo. □

**Teorema 1.3.6** (Segundo Teorema do Isomorfismo). *Sejam  $G, H$  e  $K$  grupos. Se  $H$  é subgrupo de  $G$  e  $K \triangleleft G$ , então  $H \cap K \triangleleft H$ ,  $K \triangleleft HK \leq G$  e*

$$H/H \cap K \simeq HK/K.$$

*Demonstração.* Note que  $K \triangleleft G$ , então  $HK$  é um subgrupo de  $G$  e além disso,  $K$  é subgrupo de  $HK$ , logo,  $K \triangleleft HK$  (ver [14]). Assim,  $HK/K$  é um grupo. Definamos  $\varphi : H \rightarrow HK/K$  por  $\varphi(h) = hK$ . Como  $hkK = h(kK) = hK$  para todo  $h \in H$  e  $k \in K$ ,  $\varphi$  é sobrejetivo. Também, da definição de produto de classes laterais, segue que  $\varphi$  é um homomorfismo. Agora,  $h \in \ker \varphi$  se, e somente se,  $hK = K$  e se  $hK = K$ , então  $h \in K$  e assim,  $h \in H \cap K$ . Reciprocamente, se  $h \in H \cap K$ , então  $h \in K$  e  $hK = K$ , isto é,  $h \in \ker \varphi$ . Assim  $\ker \varphi = H \cap K$  e então, pelo exemplo 1.3.2,  $H \cap K \triangleleft H$ . O resultado então segue do Primeiro Teorema do Isomorfismo.  $\square$

**Teorema 1.3.7** (Teorema da Correspondência). *Sejam  $G$  e  $H$  grupos,  $N$  subgrupo de  $G$ ,  $M$  subgrupo de  $H$  e  $\varphi : G \rightarrow H$  um homomorfismo sobrejetivo com  $K = \ker \varphi$ . Assim,  $\varphi(G) \simeq H$  e  $\varphi(K) = \{e\}$ . Além disso*

- (i) *se  $K \leq N \leq G$ , então  $\varphi(N) \leq H$ .*
- (ii) *se  $K \leq N \triangleleft G$ , então  $\varphi(N) \triangleleft H$  e  $G/N \simeq H/\varphi(N)$ .*
- (iii)  *$K \leq \varphi^{-1}(M) \leq G$ .*
- (iv) *se  $M \triangleleft H$ , então  $\varphi^{-1}(M) \triangleleft G$  e  $G/\varphi^{-1}(M) \simeq H/M$ .*

*Demonstração.* Ver [14, p. 78 - 79].  $\square$

**Teorema 1.3.8** (Terceiro Teorema do Isomorfismo). *Sejam  $G$ ,  $H$  e  $K$  grupos. Se  $K \triangleleft G$  e  $K \triangleleft L \triangleleft G$  então*

$$G/L \simeq (G/K)/(L/K).$$

*Demonstração.* No item (iv) do teorema 1.3.7 tome  $H = G/K$  e  $M = L/K$ . Defina  $\varphi : G \rightarrow G/K$  por  $\varphi(g) = gK$ . Uma vez que  $\varphi(L) = L/K$ , segue do Teorema da Correspondência que  $L/K \triangleleft G/K$ . Se  $g \in \varphi^{-1}(L/K)$ , então  $\varphi(g) = hK$  para algum  $h \in L$ . Mas, por definição,  $\varphi(g) = gK$  e então  $gK = hK$ ,  $g \in hK \subset L$ . Assim,  $\varphi^{-1}(L/K) \subset L$  e é claro que  $L \subset \varphi^{-1}(L/K)$ , isto é,  $\varphi^{-1}(L/K) = L$ . Com isso, o resultado segue do item (iv) do Teorema da Correspondência.  $\square$

Algumas vezes é conveniente, ao tratarmos de homomorfismos, denotar o elemento neutro de um grupo  $G$  por  $e_G$ . No entanto, nem sempre se faz necessário dar essa ênfase. Assim, no que se sucede, escrevermos apenas  $e$  para representar o elemento neutro sempre que não houver perigo de confusão.

## 1.4 Princípio de Contagem

Já vimos que resultados como o Teorema de Lagrange, por exemplo, nos permitem obter informações dos subgrupos a partir do grupo original. Teoremas ainda mais fortes, como o Teorema de Sylow, nos dão ainda mais informações não triviais sobre subgrupos. Mas podemos fazer o processo inverso? Isto é, obter informações sobre um determinado grupo a partir dos seus subgrupos? É o que faremos nesta seção para os grupos finitos.

Vamos relembrar a seguinte definição:

**Definição 1.4.1.** Sejam  $G$  um grupo e  $H, K$  subgrupos de  $G$ . O conjunto  $HK$  é definido por

$$HK = \{hk \mid h \in H, k \in K\}.$$

Iremos apenas informar que  $HK$  não é necessariamente um subgrupo de  $G$  em qualquer caso. Contraexemplos para isso podem ser encontrados em diversos livros sobre Teoria dos Grupos. Um critério que pode ser mostrado para determinar quando  $HK$  é um subgrupo é:  $HK$  é subgrupo de  $G$  se, e somente se  $HK = KH$ . Para os contraexemplos e uma demonstração desse critério, sugerimos que o leitor consulte [7].

**Proposição 1.4.2.** Sejam  $G$  um grupo e  $H, K$  subgrupos finitos de  $G$ . Então

$$|HK| = \frac{|H||K|}{|H \cap K|}$$

*Demonstração.* Ver [7, p. 45 - 46]. □

Vejamos um exemplo de como obter informações de um grupo apenas estudando seus subgrupos a partir dos resultados acima:

**Exemplo 1.4.3.** Seja  $G$  um grupo com  $|G| = pq$  onde  $p, q$  são primos com  $p > q$ . Suponha que  $H$  e  $K$  sejam dois subgrupos de  $G$ , distintos e de ordem  $p$ . Pela proposição 1.4.2, temos

$$|HK| = \frac{|H||K|}{|H \cap K|} = \frac{p^2}{|H \cap K|}.$$

Sendo  $H$  e  $K$  subgrupos de ordem  $p$ , então, pelo Teorema de Lagrange, ou  $H \cap K = H = K$  (o que não ocorre por hipótese) ou  $H \cap K = \{e\}$ . Então,

$$|HK| = \frac{p^2}{|\{e\}|} = p^2.$$

Logo, como  $HK \subset G$ , obtemos  $p^2 \leq pq$  o que implica  $p \leq q$ , uma contradição. Assim,  $G$  possui no máximo um subgrupo de ordem  $p$ .

## Capítulo 2

# O Teorema de Sylow

Vimos anteriormente que o Teorema de Lagrange diz: se  $H$  é um subgrupo de  $G$ , então  $|H|$  divide  $|G|$ . Mas e quanto a recíproca? Será que para todo  $d$  que seja divisor da ordem de  $G$ , existe um subgrupo  $H$  de  $G$  com ordem  $d$ ? A resposta é não. Em geral, essa recíproca não é verdadeira, entretanto, existe um resultado que, sob certas hipóteses, pode dar uma resposta afirmativa para essa pergunta e mais algumas informações, é o Teorema de Sylow, que estudaremos neste capítulo.

### 2.1 Outro Princípio de Contagem

Apresentaremos uma outra relação de equivalência em um grupo finito  $G$  que nos permitirá contar os elementos de  $G$  de forma diferente. Superficialmente falando, vamos medir o tamanho das classes de equivalência sob essa relação e com isso, vamos obter uma igualdade entre o número de elementos de  $G$  com a soma das ordens dessas classes de equivalência. Esse método de contar os elementos de  $G$  será de grande ajuda na demonstração do Teorema de Sylow, ele é as vezes chamado de equações de classe.

**Definição 2.1.1.** Sejam  $a, b \in G$ . Dizemos que  $b$  é *conjugado* de  $a$  se existe  $g \in G$  tal que  $b = g^{-1}ag$ . Essa relação será chamada de *conjugação*.

A conjugação define uma relação de equivalência em  $G$ . A verificação disso é simples, contudo, uma demonstração pode ser vista em [7].



Fixe  $a \in G$  e considere o conjunto

$$C_G(a) = \{b \in G \mid b = g^{-1}ag\}.$$

Por definição  $C_G(a)$  é a classe de equivalência de  $a$  com relação a conjugação.

**Definição 2.1.2.** Para cada  $a \in G$ , o conjunto  $C_G(a)$  será chamado *classe de conjugação de  $a$  em  $G$* .

É importante ressaltar que essas definições podem ser feitas para qualquer grupo  $G$ , finito ou não. Estamos considerando, nesta seção,  $G$  um grupo finito pois estamos interessados em um outro método de contagem.

Sendo a conjugação uma classe de equivalência, ela decompõe  $G$  numa união de classes disjuntas e assim, podemos escrever

$$|G| = \sum_a |C_G(a)|,$$

onde cada  $a$  é um representante de classes distintas. A conjugação é uma relação de equivalência menos intuitiva que a definida anteriormente e assim, determinar a ordem de cada classe pode ser menos natural. É isso que faremos agora.

**Definição 2.1.3.** Seja  $a \in G$ . O conjunto  $N_G(a) = \{b \in G \mid ab = ba\}$  é chamado *normalizador de  $a$  em  $G$* .

O normalizador  $N_G(a)$  é o conjunto de todos os elementos de  $G$  que comutam com  $a$ . É claro que  $b \in N_G(a)$ , então  $b^{-1} \in N_G(a)$ . Também se  $b_1, b_2 \in N_G(a)$ , então  $b_1b_2a = b_1ab_2 = ab_1b_2$  e assim,  $b_1b_2 \in N_G(a)$ . Isso prova a

**Proposição 2.1.4.**  $N_G(a)$  é um subgrupo de  $G$ .

**Teorema 2.1.5.** Seja  $G$  um grupo finito, então

$$|C_G(a)| = \frac{|G|}{|N_G(a)|} = [G : N_G(a)].$$

*Demonstração.* Ver [7, p. 84]. □

**Corolário 2.1.6.** Se  $G$  é um grupo finito, então

$$|G| = \sum_a \frac{|G|}{|N_G(a)|},$$

onde cada  $a$  é um representante de classes distintas.

Com esse corolário fica justificado o motivo desse método ser chamado de equações de classe. Agora vamos enunciar algumas consequências das equações de classe que serão úteis na demonstração do Teorema de Sylow.

**Definição 2.1.7.** Seja  $G$  um grupo. O conjunto

$$Z(G) = \{a \in G \mid ab = ba \ \forall b \in G\}$$

é chamado *centro* de  $G$ .

É claro que  $Z(G)$  é um subgrupo de  $G$ . Além disso,

$$\begin{aligned} a \in Z(G) &\iff ab = ba, \forall b \in G \\ &\iff \forall x \in G, x \in N_G(a) \\ &\iff G \subset N_G(a) \\ &\iff G = N_G(a), \end{aligned}$$

ou seja,  $a \in Z(G)$  se, e somente se,  $G = N_G(a)$ . Em particular, se  $G$  é um grupo finito,  $a \in Z(G)$  se, e somente se,  $|G| = |N_G(a)|$ .

**Definição 2.1.8.** Seja  $G$  um grupo finito. Dizemos que  $G$  é um  $p$ -grupo se  $|G| = p^n$  para algum  $n \in \mathbb{N}$ .

Os  $p$ -grupos desempenham um papel muito importante no Teorema de Sylow e em na Teoria de Grupos como um todo, o que justifica a definição acima. Existem alguns resultados importantes para  $p$ -grupos que são consequência das equações de classe. Dentre os resultados que enunciaremos agora, destaca-se o Teorema de Cauchy, que será utilizada explicitamente na prova do Teorema de Sylow.

**Proposição 2.1.9.** Se  $G$  é um  $p$ -grupo, então  $Z(G) \neq \{e\}$ .

*Demonstração.* Ver [7, p. 86]. □

**Proposição 2.1.10.** *Se  $G$  é um  $p$ -grupo com  $|G| = p^2$ , então  $G$  é abeliano.*

*Demonstração.* Ver [7, p. 86]. □

**Teorema 2.1.11** (Teorema de Cauchy). *Seja  $G$  um grupo finito. Se  $p$  é um número primo tal que  $p$  divide  $|G|$ , então  $G$  possui um elemento de ordem  $p$ .*

*Demonstração.* Ver [7, p. 87 - 88]. □

Destaca-se um fato importante que é usado na demonstração do Teorema de Cauchy. A equação de classe de  $G$  nos dá

$$\begin{aligned} |G| &= \sum_a \frac{|G|}{|N_G(a)|} \\ &= \sum_{a; N_G(a)=G} \frac{|G|}{|N_G(a)|} + \sum_{a; N_G(a) \neq G} \frac{|G|}{|N_G(a)|} \\ &= |Z(G)| + \sum_{a \notin Z(G)} \frac{|G|}{|N_G(a)|}. \end{aligned}$$

Assim, podemos reescrever a equação de classe de  $G$  em função do seu centro.

## 2.2 Teorema de Sylow

As aplicações do Teorema de Sylow não se limitam somente a resolver problemas exclusivos da Teoria de Grupos. Uma das muitas demonstrações existentes para o Teorema Fundamental da Álgebra faz uso do Teorema de Sylow. Mas independente de qualquer outra aplicação, a importância desse resultado é facilmente justificada. Com esse teorema podemos obter informações não triviais sobre grupos somente conhecendo a sua ordem. Existem muitas provas elegantes, a que daremos aqui se baseia nas equações de classe e procederemos por indução.

**Definição 2.2.1.** *Seja  $G$  um grupo finito. Um subgrupo de  $G$  de ordem  $p^m$  tal que  $p^m$  divide  $|G|$ , mas  $p^{m+1}$  não divide  $|G|$  é chamado  $p$ -Sylow subgrupo de  $G$ .*

Precisaremos de mais alguns conceitos para podermos enunciar e provar completamente o Teorema de Sylow. São eles:

**Definição 2.2.2.** Sejam  $H, K$  subgrupos de  $G$  e  $a, b \in G$ . Dizemos que  $a$  e  $b$  se relacionam duplamente se existe  $h \in H$  e  $k \in K$  tais que  $b = hak$ .

Para ver que a relação dupla é uma relação de equivalência em  $G$  veja [7].

**Definição 2.2.3.** Se  $a \in G$ , a classe de equivalência de  $a$  na relação dupla é chamada *classe dupla de  $H$  e  $K$  em  $G$*  e é definida pelo conjunto

$$HaK = \{hak \mid h \in H, k \in K\}.$$

**Proposição 2.2.4.** Sejam  $G$  um grupo e  $H, K$  subgrupos finitos de  $G$ . Então

$$|HaK| = \frac{|H||K|}{|H \cap (aKa^{-1})|}.$$

*Demonstração.* Ver [7, p. 98]. □

Agora vamos generalizar a definição de normalizador.

**Definição 2.2.5.** Sejam  $G$  um grupo e  $H$  um subgrupo de  $G$ . O conjunto

$$N_G(H) = \{g \in G \mid g^{-1}Hg = H\}$$

é chamado *normalizador de  $H$  em  $G$* .

O leitor pode verificar facilmente que  $N_G(H)$  é um subgrupo de  $G$ . Além disso, o normalizador possui algumas propriedades úteis.

**Proposição 2.2.6.** Sejam  $G$  um grupo e  $H$  um subgrupo de  $G$ . Então:

- (i)  $N_G(H)$  é um subgrupo de  $G$ .
- (ii)  $H \triangleleft N_G(H)$ .
- (iii) se  $K$  é um subgrupo de  $G$  e  $H \triangleleft K$ , então  $K \subset N_G(H)$ . Em outras palavras,  $N_G(H)$  é o maior subgrupo de  $G$  no qual  $H$  é normal.

*Demonstração.* Os três itens são de verificação imediata a partir da definição de normalizador.  $\square$

Vamos dividir o Teorema de Sylow em três partes e demonstrá-las separadamente. Durante toda essa seção, iremos usar a nomenclatura “Primeiro”, “Segundo” e “Terceiro” Teorema de Sylow. Em todas as três partes adotaremos as seguintes hipóteses:  $G$  é um grupo finito,  $p$  é um número primo tal que  $p^m$  divide  $|G|$  mas  $p^{m+1}$  não divide  $|G|$ .

**Teorema 2.2.7** (Primeiro Teorema de Sylow).  *$G$  tem um subgrupo de ordem  $p^m$ . Mais que isso,  $G$  tem um subgrupo de ordem  $p^i$  para todo  $i = 1, \dots, m$ .*

*Demonstração.* Se  $|G| \leq 2$ , o resultado é claro. Suponhamos o resultado verdadeiro para todo grupo com ordem menor que  $|G|$ . Se  $H$  é um subgrupo próprio de  $G$  tal que  $p^m$  divide  $|H|$  e  $p^{m+1}$  não divide  $|H|$ , então da hipótese de indução segue que  $H$  possui um subgrupo de ordem  $p^m$ , que também é um subgrupo de  $G$ . Assim, podemos supor que  $p^m$  não divide a ordem dos subgrupos próprios de  $G$ . A equação de classe de  $G$  nos dá

$$|G| = |Z(G)| + \sum_{a \notin Z(G)} \frac{|G|}{|N_G(a)|},$$

onde  $a$  é um representante de classes distintas. Para todo  $a \notin Z(G)$ ,  $p^m$  divide  $|G|$  e  $p^m$  não divide  $|N_G(a)|$ . Assim,  $p$  divide  $\frac{|G|}{|N_G(a)|}$  e  $p$  divide  $|G|$ , logo,  $p$  divide  $|Z(G)|$ . Segue do Teorema de Cauchy que  $Z(G)$  possui um elemento de ordem  $p$ , isto é, existe  $b \in Z(G)$  com  $b \neq e$  tal que  $b^p = e$ .

Seja  $N = \langle b \rangle$ . Afirmamos que  $N \triangleleft G$ . Com efeito,  $b \in Z(G)$  implica  $g^{-1}bg = g^{-1}gb = b$  e assim,

$$g^{-1}b^k g = (g^{-1}bg) \cdots (g^{-1}bg) = b^k \in N.$$

Uma vez que  $N \triangleleft G$ , existe o grupo  $G/N$  e

$$|G/N| = \frac{|G|}{|N|} = \frac{|G|}{p} < |G|.$$

Das hipóteses, segue que  $p^{m-1}$  divide  $|G/N|$  e  $p^m$  não divide  $|G/N|$ . Por indução,  $G/N$  possui um subgrupo  $\overline{H}$  com  $|\overline{H}| = p^{m-1}$ .

Considere o conjunto  $H = \{h \in G \mid hN \in \overline{H}\}$ . Se  $h \in N$ , então  $hN = N \in \overline{H}$  e por definição,  $h \in H$ . Logo,  $N \subset H$ . Se  $g, h \in H$ , por definição  $gN, hN \in \overline{H}$ . Como  $\overline{H}$  é um subgrupo de  $G/N$ , então  $ghN = gNhN \in \overline{H}$  e  $g^{-1}N = (gN)^{-1} \in \overline{H}$ . Logo,  $H$  é um subgrupo de  $G$ . Além disso,

$$p^{m-1} = |\overline{H}| = \frac{|H|}{|N|} = \frac{|H|}{p},$$

isto é,

$$|H| = p^m.$$

Portanto,  $G$  possui um subgrupo  $H$  de ordem  $p^m$ . □

**Teorema 2.2.8** (Segundo Teorema de Sylow). *Os  $p$ -Sylow subgrupos de  $G$  são conjugados.*

*Demonstração.* Sejam  $H$  e  $K$  com  $|H| = |K| = p^m$  dois  $p$ -Sylow subgrupos de  $G$ . Podemos decompor  $G$  nas classes duplas de  $H$  e  $K$  e assim

$$G = \dot{\bigcup}_a HaK$$

e

$$|G| = \sum_a |HaK|$$

onde cada  $a$  é um representante de classes distintas. Suponhamos que  $H \neq aKa^{-1}$  para todo  $a \in G$ . Então  $|H \cap (aKa^{-1})| = p^n$  com  $n < m$ . Logo

$$|HaK| = \frac{|H||K|}{|H \cap (aKa^{-1})|} = p^{2m-n}$$

e  $2m - n \geq m + 1$ . Assim,  $p^{m+1}$  divide  $|HaK|$  para todo  $a \in G$  e, portanto, divide  $|G|$ , contradição. □

**Teorema 2.2.9** (Terceiro Teorema de Sylow). *O número  $n_p$  de  $p$ -Sylow subgrupos de  $G$  é dado por*

$$n_p = \frac{|G|}{|\mathcal{N}_G(P)|}$$

onde  $P$  é algum  $p$ -Sylow subgrupo de  $G$ . Além disso,  $n_p \equiv 1 \pmod{p}$ .

*Demonstração.* Seja  $P$  algum  $p$ -Sylow subgrupo de  $G$ . Pelo Segundo Teorema de Sylow, qualquer outro  $p$ -Sylow de  $G$  é conjugado de  $P$ , logo, o número  $n_p$  de  $p$ -Sylows é o número de conjugados de  $P$  distintos. Note que

$$\begin{aligned} a^{-1}Pa = b^{-1}Pb &\iff ba^{-1}Pab^{-1} = P \\ &\iff (ab^{-1})^{-1}P(ab^{-1}) = P \\ &\iff ab^{-1} \in N_G(P) \\ &\iff N_G(P)a = N_G(P)b, \end{aligned}$$

ou seja,  $n_p$  é o número de classes laterais distintas de  $N_G(P)$  em  $G$ , ou equivalentemente, o índice de  $N_G(P)$  em  $G$ . Isso prova a primeira parte do teorema.

Agora, novamente seja  $P$  um  $p$ -Sylow subgrupo de  $G$ . Ao decompor  $G$  nas classes duplas de  $P$  e  $P$ , obtemos

$$G = \dot{\bigcup}_a PaP$$

e

$$|G| = \sum_a |PaP|$$

onde  $a$  é um representante de classes distintas. Se  $a \in N_G(P)$ , então  $aPa^{-1} = P$ , isto é,  $aP = Pa$ . Logo,  $PaP = P(Pa) = Pa$  e assim  $|PaP| = |Pa| = |P| = p^m$ . Se  $a \notin N_G(P)$ , então  $aPa^{-1} \neq P$  e  $P \cap (aPa^{-1}) \neq P$ . Assim,  $|P \cap (aPa^{-1})| = p^n$  com  $n < m$ . Com isso,

$$|PaP| = \frac{|P|^2}{|P \cap (aPa^{-1})|} = \frac{p^{2m}}{p^n} = p^{2m-n}$$

e  $2m - n \geq m + 1$ . Então  $p^{m+1}$  divide  $|PaP|$ . Isso nos dá

$$|G| = \sum_{a \in N_G(P)} |PaP| + \sum_{a \notin N_G(P)} |PaP|$$

onde  $a$  é um representante de classes distintas. Pelos argumentos anteriores, se  $a \in N_G(P)$ ,  $PaP = Pa$  e as classes duplas distintas são classes distintas de  $P$  em  $N_G(P)$ , ou seja,  $[N_G(P) : P]$ . Também dos argumentos anteriores, se  $a \notin N_G(P)$ ,  $p^{m+1}$  divide

$|PaP|$ . Assim,

$$\begin{aligned} |G| &= \sum_{a \in N_G(P)} |PaP| + \sum_{a \notin N_G(P)} |PaP| \\ &= |P| \frac{|N_G(P)|}{|P|} + rp^{m+1} \\ &= |N_G(P)| + rp^{m+1} \end{aligned}$$

para algum  $r \in \mathbb{N}$ . Uma vez que  $|N_G(P)|$  divide  $|G|$ , podemos escrever

$$n_p = \frac{|G|}{|N_G(P)|} = 1 + \frac{rp^{m+1}}{|N_G(P)|}.$$

Note que  $p^m$  divide  $|N_G(P)|$  pois divide  $|G|$  e  $rp^{m+1}$ , mas  $p^{m+1}$  não divide  $|N_G(P)|$  já que não divide  $|G|$ . Logo,  $p$  divide  $\frac{rp^{m+1}}{|N_G(P)|}$  e, portanto,

$$n_p = \frac{|G|}{|N_G(P)|} = 1 + sp$$

para algum  $s \in \mathbb{N}$ . □

Para exemplificar a importância do Teorema de Sylow, vejamos como podemos obter informações e garantir a existência de subgrupos de um determinado grupo apenas conhecendo sua ordem.

**Exemplo 2.2.10.** Seja  $G$  um grupo com  $|G| = 56 = 2^3 \cdot 7$ . Usando o Terceiro Teorema de Sylow, temos

$$n_7 \equiv 1 \pmod{7} \quad \text{e} \quad n_7 | 2^3 \cdot 7,$$

e assim  $n_7 | 8$ , logo,  $n_7 = 1$  ou  $n_7 = 8$ . Se  $n_7 = 1$ , então o 7-Sylow de  $G$  é normal. Se  $n_7 = 8$ , então note que como os 7-Sylow são cíclicos de ordem prima, eles só tem como interseção o elemento neutro. Assim,  $G$  tem  $6 \cdot 8 = 48$  elementos de ordem 7. Além desses, restam 8 elementos em  $G$ . Como  $G$  tem ao menos um subgrupo  $H$  de ordem 8 e nenhum dos elementos de ordem 7 está em  $H$ , o subgrupo  $H$  é formado exatamente pelos 8 elementos restantes em  $G$  e é o único subgrupo de ordem 8 em  $G$ . Logo,  $H$  é um 2-Sylow normal em  $G$ . Apenas conhecendo a ordem do elemento  $G$ , os Teoremas de Sylow nos permitem mostrar que  $G$  possui um subgrupo normal de ordem 7 ou possui um subgrupo normal de ordem 8.



## Capítulo 3

# Grupos Solúveis e Grupos Nilpotentes

Agora estudaremos os Grupos Solúveis e Nilpotentes. É importantíssimo que o leitor tenha bastante cuidado e paciência durante este capítulo, pois praticamente tudo o que vem depois se desenvolve a partir das ideias que serão estudadas aqui. Para os interessados numa exposição mais detalhada sobre Grupos Solúveis e Nilpotentes, sugerimos que o leitor consulte [2].

### 3.1 Grupos Solúveis

Os Grupos Solúveis recebem esse nome pela sua conexão, por meio da Teoria de Galois, com a solubilidade de polinômios. Encontrar raízes de polinômios talvez seja um dos objetivos mais antigos da matemática. Falando de modo superficial, Galois usando uma extensão de corpos  $K/F$ , construiu um grupo de todos os automorfismos de  $K$  que fixam os elementos de  $F$ , que é chamado de grupo de Galois e, posteriormente, provou que um polinômio definido em  $F[x]$  é solúvel por radicais se, e somente se, seu grupo de Galois é solúvel. O leitor que quiser ler mais sobre a Teoria de Galois, veja [12].

**Definição 3.1.1.** Sejam  $G$  um grupo e  $x, y \in G$ . O *comutador de  $x$  e  $y$*  é o elemento:

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

Abaixo, listaremos algumas propriedades dos comutadores.

**Proposição 3.1.2.** *Sejam  $G, H$  grupos,  $\varphi : G \rightarrow H$  um homomorfismo e  $x, y, z \in G$ . Então*

$$(i) \quad [x, y]^{-1} = [y, x].$$

$$(ii) \quad \varphi([x, y]) = [\varphi(x), \varphi(y)].$$

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

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

*Demonstração.* Ver [10, p. 24 - 25]. □

**Definição 3.1.3.** *Seja  $G$  um grupo. O subgrupo derivado  $G'$  de  $G$  é o subgrupo gerado por todos os comutadores de elementos de  $G$ :*

$$G' = \langle [x, y] \mid x, y \in G \rangle.$$

**Exemplo 3.1.4.** Em qualquer grupo abeliano  $G$ ,  $[x, y] = e$  para todo  $x, y \in G$ , então temos que  $G' = \{e\}$ .

**Definição 3.1.5.** *A série derivada de um grupo  $G$  é a cadeia de subgrupos de  $G$  definida por:*

$$G^{(0)} = G,$$

e,

$$G^{(i+1)} = (G^{(i)})' \quad \forall i \geq 0.$$

A série derivada de  $G$  é da forma:

$$G = G^{(0)} \geq G^{(1)} \geq G^{(2)} \geq \dots \geq G^{(d)} \geq \dots$$

Quando a série estaciona em  $d$ , isto é,  $G^d = G_{d+n}$  para todo  $n \in \mathbb{N}$ , dizemos que  $d$  é o *comprimento da série*.

**Exemplo 3.1.6.** No  $S_4$  temos:

$$S_4 > A_4 > \langle (12)(34), (14)(23) \rangle > \langle (12)(34) \rangle > \{e\}.$$

**Definição 3.1.7.** Um grupo  $G$  é *solúvel* se  $G^{(d)} = \{e\}$  para algum  $d$ .

**Exemplo 3.1.8.** Segue do exemplo anterior que  $S_4$  é solúvel. Se  $G$  é um grupo abeliano, então  $G' = \{e\}$ , ou seja, todo grupo abeliano é solúvel.

Alguns teoremas importantes relacionam a solubilidade com a ordem de um grupo, enunciaremos no último capítulo o principal dentre eles, devido à Feit-Thompson. Existe uma sequência interessante que pode ser consultada em [16], onde cada elemento da sequência representa a ordem de um grupo não solúvel.

## 3.2 Condições suficientes para solubilidade

Nesta seção falaremos dos principais resultados sobre grupos solúveis. Apresentaremos alguns critérios mais simples para verificar a solubilidade de grupos que, muitas vezes, podem não ser úteis quando o grupo é muito complicado ou a ordem é muito grande. Além disso provaremos alguns resultados que serão muito utilizados posteriormente.

Antes, vamos enunciar alguns lemas que serão utilizados durante esta seção. Dois desses lemas tratam sobre propriedades básicas dos grupos derivados e grupos solúveis. Sendo assim, daremos uma breve demonstração a fim de exercitar as definições.

**Lema 3.2.1.** *Sejam  $G$ ,  $H$  e  $K$  grupos. Então:*

- (i) *se  $H$  é subgrupo de  $G$ , então  $H'$  é subgrupo de  $G'$ .*
- (ii) *se  $\varphi : G \rightarrow K$  é um homomorfismo, então  $\varphi(G')$  é subgrupo de  $K'$ . Além disso, se  $\varphi$  é sobrejetivo, então  $\varphi(G') = K'$ .*

*Demonstração.* (i) É imediato, uma vez que todo comutador de  $H$  é um comutador de  $G$ .

- (ii) A primeira parte segue imediatamente do item (ii) da proposição 3.1.2. Se  $\varphi$  é sobrejetivo, dados  $a, b \in K$ , podemos escrever  $a = \varphi(x)$  e  $b = \varphi(y)$  com

$x, y \in G$ . Assim,

$$[a, b] = \varphi([x, y]) \in \varphi(G'),$$

donde  $K'$  é subgrupo de  $\varphi(G')$ , logo, o resultado segue.

□

Os lemas abaixo farão praticamente todo o trabalho da demonstração da próxima proposição.

**Lema 3.2.2.** (i) *Subgrupos de grupos solúveis são solúveis.*

(ii) *Imagens homomórficas de grupos solúveis são solúveis.*

(iii) *Quocientes de grupos solúveis são solúveis.*

*Demonstração.* (i) Do item (i) do lema anterior, segue por indução que  $H^{(i)} \leq G^{(i)}$ .

Logo,  $H^{(d)} \leq G^{(d)} = \{e\}$  para algum  $d$ .

(ii) Seja um homomorfismo  $\varphi : G \rightarrow K$  onde  $G$  é um grupo solúvel. Novamente pelo lema anterior, item (ii), segue por indução que  $\varphi(G^{(i)}) \leq K^{(i)}$ . A conclusão se dá por um argumento inteiramente análogo ao do item anterior.

(iii) Pelo Primeiro Teorema do Isomorfismo, um quociente  $G/K$  é isomorfo à imagem homomórfica dada por um homomorfismo  $\varphi$  do qual  $K$  é o núcleo. Assim, o resultado segue do item anterior.

□

**Lema 3.2.3.** *Sejam  $G$  um grupo e  $N$  um subgrupo normal de  $G$ . Então  $G/N$  é abeliano se, e somente se,  $G'$  é subgrupo de  $N$ .*

*Demonstração.* Ver [8, p. 102].

□

A proposição abaixo será utilizada em alguns momentos cruciais, tanto na demonstração do Teorema de Burnside quanto na demonstração do Primeiro Teorema de Philip Hall, por isso, o leitor deve atentar para o seu enunciado.

**Proposição 3.2.4.** *Sejam  $G$  um grupo e  $N$  um subgrupo normal de  $G$ . Então  $G/N$  e  $N$  são grupos solúveis se, e somente se,  $G$  é solúvel.*

*Demonstração.* Seja  $\varphi : G \rightarrow G/N$  o homomorfismo natural. Por hipótese,  $(G/N)^{(d_1)} = e$  para algum  $d_1$  e  $N^{(d_2)} = e$  para algum  $d_2$ . Assim, pelo lema 3.2.2,

$$\varphi(G)^{(d_1)} = (G/N)^{(d_1)} = e,$$

isto é,

$$G^{(d_1)} \subset \ker \varphi = N.$$

Portanto, novamente pelo lema 3.2.2,

$$(G^{(d_1)})^{(d_2)} \leq N^{(d_2)} = e.$$

Logo,  $G$  é solúvel. Reciprocamente, se  $G$  solúvel,  $N$  é solúvel pelo lema anterior. O lema anterior também nos diz que  $G/N$  é solúvel.  $\square$

**Proposição 3.2.5.** *Seja  $G$  um grupo. As condições a seguir são equivalentes:*

- (i)  $G$  é solúvel;
- (ii)  $G$  tem a seguinte cadeia de subgrupos:

$$G = G_0 \geq G_1 \geq \cdots \geq G_n = \{e\},$$

*e ainda,  $G_i$  é um subgrupo normal de  $G$  e  $G_{i-1}/G_i$  é abeliano.*

- (iii)  $G$  tem a seguinte cadeia de subgrupos:

$$G = G_0 \geq G_1 \geq \cdots \geq G_n = \{e\},$$

*e ainda,  $G_i$  é um subgrupo normal de  $G_{i-1}$  e  $G_{i-1}/G_i$  é abeliano.*

*Demonstração.* (i)  $\implies$  (ii): Basta considerar a série derivada

$$G = G_0 \geq G_1 \geq \cdots \geq G_n = \{e\}$$

e as outras condições são automaticamente satisfeitas pelas propriedades do subgrupo derivado.

(ii)  $\implies$  (iii): Note que  $G_i \triangleleft G$  com  $G_i \leq G_{i-1} \leq G$  implica  $G_i \triangleleft G_{i-1}$ .

(iii)  $\implies$  (i): Imediato.

□

**Exemplo 3.2.6.** O  $A_5$  é solúvel? Em sua série derivada não temos satisfeitas a condição (ii) da proposição anterior, uma vez que  $A_5$  é um grupo simples. Assim, o  $A_5$  não pode ser solúvel.

**Lembrete:** Um grupo  $G$  é chamado de *grupo simples* se seus únicos subgrupos normais são os triviais.

**Proposição 3.2.7.** *Seja  $G$  um grupo. As seguintes condições são equivalentes:*

- (i)  $G$  é um grupo solúvel finito;
- (ii)  $G$  tem uma série de composição com todos os fatores de composição cíclicos de ordem prima.

*Demonstração.* (i)  $\implies$  (ii): Seja  $G$  um grupo solúvel finito. Então  $G$  possui uma cadeia de subgrupos

$$G = G_0 > G_1 > \cdots > G_n = \{e\}$$

com  $G_i \triangleleft G_{i-1}$  e  $G_{i-1}/G_i$  abeliano. Como  $G$  é finito, só podem existir finitos termos na série e assim, podemos assumir que a cadeia acima é a maior série de  $G$  com fatores abelianos. Logo, esta série é uma série de composição, senão tendo algum  $G_{i-1}/G_i$  não simples, existiria  $N \triangleleft G_{i-1}$  com  $G_i < N < G_{i-1}$  e com isso, obteríamos uma série maior e além disso, os novos fatores da série satisfazem

$$N/G_i \leq G_{i-1}/G_i,$$

e,

$$G_{i-1}/N \simeq \frac{G_{i-1}/G_i}{N/G_i}$$

pelo Terceiro Teorema do Isomorfismo. Como  $G_{i-1}/G_i$  é abeliano,  $G_{i-1}/N$  e  $N/G_i$  são abelianos, o que contraria a maximalidade da série anterior. Assim, a série é, de fato, uma série de composição e os fatores de composição de  $G$  são abelianos. Note que a série é composta por grupos abelianos simples que são cíclicos de ordem prima, isto é, todos os fatores de composição de  $G$  são cíclicos de ordem prima.

(ii)  $\implies$  (i): Seja

$$G = G_0 > G_1 > \cdots > G_n = \{e\}$$

uma série de composição com fatores cíclicos de ordem prima. Assim,  $G_i \triangleleft G_{i-1}$  e  $G_{i-1}/G_i$  é abeliano para cada  $i$ . A solubilidade de  $G$  segue da proposição 3.2.5. Além disso,

$$|G| = |G_0/G_1| \cdots |G_{n-1}/G_n|$$

e assim,  $G$  é finito.

□

### 3.3 O Teorema de Wielandt

O Teorema de Wielandt provavelmente seria um dos menos destacados deste capítulo se não o tivéssemos separado dos outros resultados. Contudo, ele será de suma importância na prova do Segundo Teorema de Philip Hall.

Antes de demonstrá-lo, precisaremos do seguinte lema:

**Lema 3.3.1.** *Sejam  $G$  um grupo finito e sejam  $U$  e  $V$  subgrupos de  $G$ . Se  $([G : U], [G : V]) = 1$ , então  $G = UV$  e  $[G : U \cap V] = [G : U][G : V]$ .*

*Demonstração.* Seja  $D = U \cap V$ . Como  $\frac{|G|}{|D|} = \frac{|G|}{|U|} \frac{|U|}{|D|}$  e  $\frac{|G|}{|D|} = \frac{|G|}{|V|} \frac{|V|}{|D|}$ , então  $[G : U]$  e  $[G : V]$  dividem  $[G : D]$ . Por hipótese,  $([G : U], [G : V]) = 1$  e então,  $[G : D] = m[G : U][G : V]$  com  $m \in \mathbb{N}$ . Por fim,  $m|G| = \frac{|U||V|}{|D|} = |UV| \leq |G|$  e, portanto,  $m = 1$ ,  $G = UV$  e  $[G : D] = [G : U][G : V]$  □

Antes de provar o teorema, precisamos definir um conceito fundamental ao longo desse texto que precisaremos entender para a demonstração.

**Definição 3.3.2.** Seja  $G$  um grupo finito. Dizemos que  $N$  é um *subgrupo minimal normal* de  $G$  quando  $N$  é um subgrupo normal não trivial tal que se  $M \subset N$  e  $M \triangleleft G$ , então  $M = \{e\}$  ou  $M = N$ .

Também precisaremos de um resultado que envolve alguns conceitos que serão abordados no próximo capítulo, a saber: um subgrupo minimal normal  $M$  de um grupo solúvel finito  $G$  é um  $p$ -grupo abeliano elementar para algum primo  $p$ , isto é,  $g^p = e$  para todo  $g \in G$ . Esse resultado será provado no próximo capítulo.

**Teorema 3.3.3** (Wielandt). *Seja  $G$  um grupo que possui três subgrupos solúveis  $H_1$ ,  $H_2$  e  $H_3$  cujos índices  $[G : H_i]$  são dois a dois coprimos. Então  $G$  é solúvel.*

*Demonstração.* Faremos indução sobre a ordem de  $G$ .

Pelo lema anterior,  $G = H_1H_2 = H_1H_3 = H_2H_3$ . Suponhamos, sem perda de generalidade, que  $H_1 \neq \{e\}$  e seja  $N$  um subgrupo minimal normal de  $H_1$ . Como  $H_1$  é solúvel, um subgrupo minimal normal de  $H_1$  é um  $p$ -grupo abeliano elementar para algum primo  $p$ . Ainda, como  $[G : H_2]$  e  $[G : H_3]$  são coprimos, podemos supor, sem perda de generalidade, que  $p$  não divide  $[G : H_2]$ .

Seja  $D = H_1 \cap H_2$ , como  $N \triangleleft H_1$ ,  $ND$  é um subgrupo de  $H_1$  e  $[N : N \cap D] = [ND : D] = p^\alpha$  divide  $[H_1 : D] = [H_1H_2 : H_2]$ , um absurdo, pois  $p$  não divide  $[G : H_2]$ . Assim,  $[N : N \cap D] = 1$ , isto é,  $N \leq D$ .

Seja  $K = \langle N^G \rangle \triangleleft G$ , então  $K = \langle N^{h_1h_2} \rangle = (N^{h_1})^{h_2} = N^{h_2} : h_1 \in H_1$  e  $h_2 \in H_2$ . Como  $N \leq D \leq H_2$ , temos que  $K \leq H_2$ . Mas,  $H_2$  é solúvel e assim,  $K$  é solúvel. Consequentemente, os subgrupos,  $H_1K/K$ ,  $H_2K/K$  e  $H_3K/K$  são solúveis e seus índices em  $G/K$  são dois a dois coprimos. Como  $N \neq \{e\}$ ,  $K \neq \{e\}$ . Pela hipótese de indução,  $G/K$  é solúvel. Pelo proposição 3.2.4,  $G$  é solúvel.  $\square$

Apesar de sua importância na demonstração do Segundo Teorema de Philip Hall, a demonstração do Teorema de Wielandt envolve apenas técnicas simples de Teoria de Grupos, como certamente foi notado pelo leitor.

Uma observação interessante, é que além do Teorema de Wielandt, o lema que usamos para prová-lo tem uma pequena participação direta na demonstração do



Segundo Teorema de Philip Hall, e é claro, outra indireta devido seu papel na prova do Teorema de Wielandt.

### 3.4 Grupos Nilpotentes

Os Grupos Nilpotentes, apesar de terem um papel mais discreto nesse texto, são extremamente importantes para a matemática, em especial, para a Teoria de Grupos. A Teoria das Álgebras de Lie, que é um campo de pesquisa muito ativo atualmente, está bem relacionada com os Grupos Nilpotentes e seus automorfismos.

Sejam  $G$  e  $H$  grupos, escreveremos  $[G, H]$  para representar o grupo formado pelos elementos da forma  $[g, h]$  com  $g \in G$  e  $h \in H$ .

**Definição 3.4.1.** O  $i$ -ésimo subgrupo comutador superior  $\mathcal{D}_i(G)$  é definido indutivamente por

$$\mathcal{D}_1(G) = G$$

e

$$\mathcal{D}_{i+1}(G) = [\mathcal{D}_i(G), G]$$

É importante o leitor notar que existe uma diferença sutil entre o subgrupo comutador superior e o subgrupo derivado. Os elementos do subgrupo derivado são da forma  $[g, h]$  onde  $g$  e  $h$  estão no mesmo grupo, já nos elementos  $[g, h]$  do subgrupo comutador superior, os elementos  $g$  e  $h$  pertencem à grupos possivelmente diferentes. Assim, fica claro que o subgrupo comutador superior é uma extensão do conceito de subgrupo derivado.

**Definição 3.4.2.** Um grupo  $G$  é chamado *nilpotente com classe  $r$*  se  $r$  é o menor inteiro positivo tal que  $\mathcal{D}_{r+1}(G) = \{e\}$  e  $G$  é chamado *nilpotente* se é nilpotente com classe  $r$  para algum inteiro positivo  $r$ .

É consequência imediata da definição que todo grupo nilpotente é solúvel. A recíproca, no entanto, é falsa. O grupo  $S_3$  é solúvel, mas é um grupo não abeliano com  $Z(S_3) = \{e\}$ , logo, não pode ser nilpotente. Aqui estamos usando o seguinte resultado:

se  $G$  é um grupo com centro trivial, então  $G$  não é nilpotente. Uma demonstração pode ser vista em [14].

A definição de Grupo Nilpotente é muito parecida com a caracterização de Grupos Solúveis, o que pode fazer o leitor pensar que valem propriedades parecidas com as de Grupos Solúveis. De fato, isso é verdade, vejamos.

**Proposição 3.4.3.** (i) *Subgrupos de grupos nilpotentes são nilpotentes.*

(ii) *Imagens homomórficas de grupos nilpotentes são nilpotentes.*

(iii) *Quocientes de grupos nilpotentes é nilpotente.*

*Demonstração.* A demonstração é inteiramente análoga a do lema 3.2.2. □

**Proposição 3.4.4.** *Produto direto finito de grupos nilpotentes é nilpotente.*

*Demonstração.* Ver [14, p. 213]. □

Agora, veremos o principal resultado desta seção sobre grupos nilpotentes. Ele fornece uma caracterização para Grupos Nilpotentes os relacionando com os subgrupos de Sylow.

**Teorema 3.4.5.** *Seja  $G$  um grupo finito. Então  $G$  é nilpotente se, e somente se,  $G$  é o produto direto dos seus subgrupos de Sylow.*

*Demonstração.* Ver [14, p. 216]. □

Vale ressaltar que apesar de falarmos pouco sobre os Grupos Nilpotentes, o leitor não deve subestimar sua importância para a Teoria de Grupos. Eles apenas não têm uma relevância fundamental com a teoria que estamos desenvolvendo aqui, serão necessários apenas em um ponto específico.

## Capítulo 4

### O Teorema de Philip Hall (1928)

Neste capítulo enunciaremos e provaremos o Primeiro Teorema de Philip Hall. A prova do teorema é dividida em muitas partes e, para encurtá-la e facilitar a compreensão, provaremos alguns lemas específicos da Teoria de Grupos que ainda não foram mencionados nesse texto.

#### 4.1 Subgrupos de Hall e Lemas auxiliares

Nesta seção iremos introduzir os conceitos de  $\pi$ -subgrupos de Hall e  $\pi$ -subgrupos. O subgrupos de Hall foram introduzidos pelo matemático Philip Hall. Eles (assim como o teorema central desse capítulo) generalizam os grupos de Sylow. Pode-se mostrar que qualquer subgrupo de Sylow é um subgrupo de Hall.

**Definição 4.1.1.** Seja  $G$  um grupo finito e  $\pi$  um conjunto de números primos. Dizemos que:

- (i) Um  $\pi$ -subgrupo de  $G$  é um subgrupo  $K$  tal que  $|K|$  é um produto envolvendo somente primos em  $\pi$ ;
- (ii) Um  $\pi$ -subgrupo de Hall de  $G$  é um subgrupo  $H$  de  $G$  tal que  $|H|$  é um produto envolvendo primos em  $\pi$  e  $[G : H]$  é um produto envolvendo primos que não estão em  $\pi$ .

O Primeiro Teorema de Philip Hall vai garantir uma “boa relação” dos  $\pi$ -subgrupos de Hall com grupos solúveis. Assim, vamos estudar como se comportam esses subgrupos em grupos não solúveis. Para os exemplos abaixo, considere o grupo alternado  $A_5$  e lembre que  $|A_5| = 60 = 2^2 \cdot 3 \cdot 5$ .

**Exemplo 4.1.2.** Um  $\{2, 3\}$ -subgrupo de Hall  $H$  de  $A_5$  terá ordem  $2^2 \cdot 3 = 12$ . Visto que esse subgrupo de ordem 12 não poderá ter nenhum elemento de ordem 6 (pois é um subgrupo de  $A_5$ ), então sabemos que, a menos de isomorfismo, o  $\{2, 3\}$ -subgrupo de Hall será o  $A_4$ .

**Exemplo 4.1.3.** Um  $\{3, 5\}$ -subgrupo de Hall  $K$  de  $A_5$  terá ordem  $3 \cdot 5$  e índice  $2^2 = 4$ . Note que  $A_5$  age nas classes laterais de  $K$ , com 4 classes distintas, da seguinte forma:

$$A_5/K = \{a_1K, a_2K, a_3K, a_4K\}.$$

Assim, obtemos um homomorfismo  $\varphi : A_5 \rightarrow S_4$ . Como  $A_5$  é um grupo simples,  $\ker \varphi = \{e\}$  ou  $\ker \varphi = A_5$ . Então:

**Caso 1:**  $\ker \varphi = \{e\}$ .

Seque que  $\ker \varphi = \{e\}$  implica  $\varphi$  injetivo, o que é um absurdo pois  $|A_5| = 60 > 24 = |S_4|$ .

**Caso 2:**  $\ker \varphi = A_5$ .

Para todo  $b \in A_5$ , temos  $b(a_iK) = a_iK$  se, e somente se  $b \in a_iK$ , onde  $1 \leq i \leq 4$ , o que é um absurdo pois  $\bigcap (a_iK) = \emptyset$ .

Assim, não pode existir um  $\{3, 5\}$ -subgrupo de Hall de  $A_5$ .

Agora, como preparação para a demonstração do teorema de Hall, veremos alguns resultados que serão necessários. Primeiro, definiremos e somente enunciaremos um resultado sobre subgrupos característicos e para encerrar, provamos três lemas

chaves para as duas etapas em que dividiremos a demonstração. O motivo de estarem aparecendo pela primeira vez nesse capítulo é para que o leitor não deixe de dar a devida importância pelos seus enunciados relativamente simples e por não parecer existir uma conexão direta com os objetivos desse capítulo.

**Definição 4.1.4.** Seja  $G$  um grupo e  $H$  um subgrupo de  $G$ . Se  $\varphi(h) \in H$  para todo  $h \in H$ , para todos os automorfismos  $\varphi$  de  $G$ , então  $H$  é chamado de *subgrupo característico* de  $G$ . Se  $G$  é um grupo não trivial e os únicos subgrupos característicos de  $G$  são  $\{e\}$  e  $G$ , então dizemos que  $G$  é um *grupo caracteristicamente simples*.

**Definição 4.1.5.** Seja  $p$  um número primo. Dizemos que  $G$  é um  *$p$ -grupo abeliano elementar* se  $g^p = e$  para todo  $g \in G$ .

**Proposição 4.1.6.** Um grupo finito  $G$  caracteristicamente simples é isomorfo a um produto direto de grupos simples.

*Demonstração.* Ver [15, p. 106]. □

**Lema 4.1.7.** Um subgrupo minimal normal  $M$  de um grupo solúvel finito  $G$  é um  $p$ -grupo abeliano elementar para algum primo  $p$ .

*Demonstração.* Uma vez que um subgrupo minimal normal  $M$  de um grupo  $G$  é caracteristicamente simples, então o lema anterior diz que  $M$  é isomorfo a um produto direto de grupos simples. Além disso, já que  $G$  é solúvel,  $M$  é produto direto de grupos cíclicos de ordem  $p$ . Note que  $M$  é um  $p$ -grupo abeliano elementar se, e somente se,  $M \simeq C_p \times C_p \times \cdots \times C_p$  onde  $C_p$  é um grupo cíclico de ordem  $p$ . Assim,  $M$  é um  $p$ -grupo abeliano elementar. □

**Lema 4.1.8** (Lei Modular de Dedekind). Sejam  $G$  um grupo finito e  $H, K, L$  subgrupos de  $G$ . Se  $K$  é subgrupo de  $L$ . Então

$$HK \cap L = (H \cap L)K$$

*Demonstração.* Seja  $x \in HK \cap L$ . Então  $x = hk$ , onde  $h \in H$  e  $k \in K$ . Assim,  $x \in HK$  e  $x \in L$ . Como  $K \leq L$ ,

$$\begin{aligned} x = hk \in L &\implies h = xk^{-1} \in L \\ &\implies h \in H \cap L. \end{aligned}$$

e como  $x = hk$ , temos:

$$h \in H \cap L \text{ e } k \in K \implies x = hk \in (H \cap L)K.$$

Assim,  $(HK) \cap L \subset (H \cap L)K$ . Reciprocamente, seja  $x \in (H \cap L)K$ . Então  $x = hk$ , onde  $h \in H \cap L$  e  $k \in K$ . Logo,  $x \in HK$ . Mas, como  $K \leq L$ , temos que  $x \in L$ . Assim,

$$x \in HK \text{ e } x \in L \implies x \in (HK) \cap L.$$

Assim,  $(H \cap L)K \subset (HK) \cap L$ . Portanto,  $(HK) \cap L = (H \cap L)K$ .  $\square$

**Lema 4.1.9** (Argumento de Frattini). *Sejam  $G$  um grupo finito,  $N$  um subgrupo normal de  $G$  e  $P$  um  $p$ -subgrupo de Sylow de  $N$ . Então*

$$G = N_G(P)N.$$

*Demonstração.* Seja  $g \in N_G(P)N$ . Como  $N_G(P)$  e  $N$  são subgrupos de  $G$  e  $g \in N_G(P)N$ ,  $g \in G$ . Assim,  $N_G(P)N \subset G$ . Reciprocamente, seja  $g \in G$ . Uma vez que  $N \triangleleft G$ ,  $N^g = N$  e como  $P \leq N$ , temos  $P^g \leq N$ . Assim  $P^g$  é um  $p$ -subgrupo de Sylow de  $N$ . Pelo Teorema de Sylow,  $P$  e  $P^g$  são conjugados em  $N$ . Logo,  $P^g = P^n$ , para algum  $n \in N$ . Então,  $P^{gn^{-1}} = P$ . Note que  $P \subset N_G(P)$  e  $y = gn^{-1} \in G$ , portanto,  $y = gn^{-1} \in N_G(P)$ . Agora, como  $y = gn^{-1}$ ,  $g = yn$  onde  $y \in N_G(P)$  e  $n \in N$ . Assim  $g \in N_G(P)N$  e, portanto,  $G \subset N_G(P)N$ . Temos então que  $G = N_G(P)N$  e assim, concluímos a demonstração.  $\square$

## 4.2 Primeiro Teorema de Philip Hall

A importância desse primeiro teorema, como já foi mencionado anteriormente, é fornecer “quase” uma generalização do Teorema de Sylow. O leitor certamente perceberá

a semelhança entre o enunciado dos dois teoremas. Além disso, esse teorema é também a primeira parte de um critério que foi estabelecido para classificar um grupo quanto a solubilidade.

A demonstração é um pouco longa e, para torná-la menos cansativa e obter uma melhor organização das ideias, dividiremos a prova em dois casos. O primeiro caso é o mais simples, contudo, o segundo caso requer muito mais trabalho. Assim, também dividiremos o segundo caso em dois subcasos. Ao invés de adotarmos a mesma estratégia que fizemos para a demonstração do Teorema de Sylow, vamos fazer a prova de uma única vez pois a demonstração que daremos está completamente conectada. Sem mais delongas:

**Teorema 4.2.1** (Primeiro Teorema de Philip Hall). *Seja  $G$  um grupo solúvel finito e  $\pi$  um conjunto de números primos. Então:*

- (i)  *$G$  tem um  $\pi$ -subgrupo de Hall;*
- (ii) *Quaisquer dois  $\pi$ -subgrupos de Hall de  $G$  são conjugados;*
- (iii) *Qualquer  $\pi$ -subgrupo de  $G$  está contido em um  $\pi$ -subgrupo de Hall.*

Aqui podemos assumir que  $\pi$  é um conjunto de primos que contém ao menos um elemento que divide a ordem de  $G$  mas, se  $S = \pi \cap \{p_1, \dots, p_k\} = \emptyset$  onde  $|G| = p_1^{r_1} \cdots p_k^{r_k}$ , então podemos definir  $\prod_{s \in S} s = 1$ .

*Demonstração.* A ideia inicial para essa demonstração será usar indução sobre a ordem de  $G$  para concluirmos (i) e (iii).

Seja  $G$  um grupo e  $\pi$  um conjunto de números primos. Suponhamos que  $|G| = mn$  tal que  $m$  é produto de primos em  $\pi$  e  $n$  é produto de primos que não estão em  $\pi$  e, portanto, um  $\pi$ -subgrupo de Hall  $H$  de  $G$  deve ter ordem  $m$ .

Podemos supor  $|G| > 1$  pois de outro modo,  $G = \{e\}$  e assim, (i) e (iii) seriam trivialmente verdadeiras. De forma análoga, assumiremos que  $m > 1$  pois caso contrário,  $H = \{e\}$  e assim, (i) e (iii) seriam trivialmente verdadeiras.

Seja  $M$  um subgrupo minimal normal de  $G$ . Como  $G$  tem ordem finita e é solúvel,  $M$  é um  $p$ -grupo abeliano elementar. Existem duas possibilidades para a ordem de  $M$ :

- $|M| = p^\alpha$  onde  $p \in \pi$ ;
- $|M| = q^\beta$  onde  $q \notin \pi$ .

**Caso 1:**  $M$  é um  $p$ -grupo abeliano elementar com  $p \in \pi$  e  $|M| = p^\alpha$ .

Como  $M \triangleleft G$ ,  $G/M$  será grupo e  $|G/M| = \frac{|G|}{|M|}$ . Uma vez que os fatores da ordem de  $|M|$  estão no mesmo conjunto que os fatores de  $m$ ,  $p^\alpha$  divide  $m$ . Assim:

$$|G/M| = mn/p^\alpha = m_1n,$$

onde  $m = m_1p^\alpha$ . Observe que  $G/M$  é solúvel e que o Teorema da Correspondência nos diz que existe uma correspondência biunívoca entre os subgrupos de  $G$  que contém  $M$  e os subgrupos de  $G/M$  e então, um  $\pi$ -subgrupo de Hall de  $G/M$  é da forma  $H/M$  onde  $M \subset H \leq G$ . Este  $\pi$ -subgrupo de Hall de  $G$  existe devido a hipótese de indução. Como sabemos que  $H/M$  é um  $\pi$ -subgrupo de Hall de  $G/M$ , temos:

$$\frac{|G/M|}{|H/M|} = n \text{ e } |H/M| = m_1,$$

logo,

$$|H| = m_1|M| \implies |H| = m_1p^\alpha \implies |H| = m.$$

Portanto,  $H$  é um  $\pi$ -subgrupo de Hall de  $G$ . Agora considere  $L$  qualquer  $\pi$ -subgrupo de  $G$ . Seja  $\varphi : G \rightarrow G/M$  homomorfismo canônico. Como  $L$  é um  $\pi$ -subgrupo de  $G$ ,  $\varphi(L) = LM/M$  em  $G/M$  é um  $\pi$ -subgrupo de  $G/M$ . Pela hipótese de indução, algum conjugado de  $H/M$  contém  $LM/M$ . Então

$$LM/M \leq (H/M)^{Mx} = (Mx)^{-1}H(Mx)/M,$$

e,

$$(Mx)^{-1}H(Mx)/M = Mx^{-1}HxM/M = MH^xM/M,$$



ainda, como  $M < H^x$ ,

$$MH^xM/M = H^x/M \implies LM \leq H^x,$$

onde  $x \in G$ . Mas  $L \leq LM \leq H^x$ , ou seja,

$$L \leq H^x.$$

Com isso, concluimos o primeiro caso.

**Caso 2:** Nenhum subgrupo minimal normal de  $G$  é um  $p$ -grupo abeliano elementar com  $p \in \pi$ .

Assim,  $|M| = q^\beta$  onde  $q \notin \pi$ . Como  $M \triangleleft G$ ,  $G/M$  será grupo e  $|G/M| = \frac{|G|}{|M|}$ , uma vez que os fatores da ordem de  $M$  não estão no mesmo conjunto que os fatores de  $m$ ,  $q^\beta$  divide  $n$ . Assim:

$$|G/M| = mn/q^\beta = mn_1,$$

onde  $n = n_1q^\beta$ . Devemos considerar duas possibilidades:  $n_1 \neq 1$  e  $n_1 = 1$ .

Se  $n_1 \neq 1$ :

Pela hipótese de indução temos que  $G/M$  tem um  $\pi$ -subgrupo de Hall. Seja  $K/M$  um  $\pi$ -subgrupo de Hall de  $G/M$  onde  $M \subset K \leq G$ . Então

$$|K/M| = m,$$

e assim,

$$|K| = m|M| = mq^\beta = mn/n_1 < mn.$$

Como  $|K| < |G|$ ,  $K$  tem um  $\pi$ -subgrupo de Hall. Seja  $H$  um  $\pi$ -subgrupo de Hall de  $K$ . Pelo Teorema de Lagrange  $|H|$  tem que dividir  $|K|$  e  $|H|$  tem que ser produto envolvendo somente primos em  $\pi$ . Assim,  $|H| = m$  e, portanto,  $H$  é um  $\pi$ -subgrupo de Hall de  $G$ . Agora considere  $L$  um  $\pi$ -subgrupo de  $G$ . Seja  $\sigma : G \rightarrow G/M$  homomorfismo canônico. Já que  $L$  é um  $\pi$ -subgrupo de  $G$ ,  $\sigma(L) = LM/M$  em  $G/M$  é

um  $\pi$ -subgrupo de  $G/M$ . Pela hipótese de indução, algum conjugado de  $K/M$  contém  $LM/M$ . Então,

$$LM/M \leq (K/M)^{Mx} = K^x/M,$$

onde  $x \in G$ . Mas  $L \leq LM \leq K^x$ , ou seja,

$$L \leq K^x.$$

Uma vez que  $L \leq K^x$ ,  $L^{x^{-1}} \leq K$  então  $L^{x^{-1}}$  é um  $\pi$ -subgrupo de  $K$  e como  $|K| < |G|$ , temos pela hipótese de indução que  $L^{x^{-1}} \leq H^y$ . Logo,

$$L^{x^{-1}} \leq H^y \implies L \leq H^{yx}.$$

Com isso, provamos o segundo para  $n_1 \neq 1$ .

Se  $n_1 = 1$ :

Como  $n = n_1 q^\beta$  e  $|G| = mn$  quando  $n_1 = 1$ , temos  $|G| = m q^\beta$ . Temos que  $|G/M| = m$  e  $m > 1$ . Seja  $N/M$  um subgrupo minimal normal de  $G/M$ . Assim  $N/M$  é um  $p$ -grupo abeliano elementar para algum  $p \in \pi$ , então  $|N/M| = p^\alpha$ . Note que  $\frac{G/M}{N/M} \simeq G/N$  e assim,  $N \triangleleft G$ . Logo,

$$|N/M| = p^\alpha = \frac{|N|}{|M|},$$

logo,

$$|N| = p^\alpha |M| \implies |N| = p^\alpha q^\beta.$$

Considere  $P$  um  $p$ -subgrupo de Sylow de  $N$ . O Argumento de Frattini nos diz  $G = N_G(P)N$ . Como  $N = PM$ , temos:

$$G = N_G(P)PM.$$

Como  $P$  é subgrupo de  $N_G(P)$ ,  $N_G(P)P = N_G(P)$  e, portanto,  $G = N_G(P)M$ . Agora, considere  $J = N_G(P) \cap M$ . Uma vez que  $M$  é abeliano,  $J \triangleleft M$  e como  $M \triangleleft G$ ,  $J \triangleleft N_G(P)$ , pois para todo  $g \in N_G(P)$  se tem

$$J^g = (N_G(P) \cap M)^g = N_G(P)^g \cap M^g,$$

e,

$$N_G(P)^g \cap M^g = N_G(P) \cap M = J.$$

Assim,

$$J \triangleleft N_G(P) \implies J \triangleleft N_G(P)M = G \implies J \triangleleft G.$$

Sabemos que  $M$  é um subgrupo minimal normal de  $G$  e como  $J \triangleleft G$ , existem duas possibilidades para  $J$ :  $J = \{e\}$  ou  $J = M$  (mostraremos que  $J = \{e\}$ ). Se  $J = M$ ,  $N_G(P) \cap M = M$  e assim,  $M$  é subgrupo de  $N_G(P)$ . Se  $M \leq N_G(P)$ , então  $N_G(P)M = N_G(P)$  implica  $G = N_G(P)$  e como, por definição,  $P \triangleleft N_G(P)$ ,  $P \triangleleft G$ . Logo,  $P$  é um  $p$ -subgrupo normal de  $G$  e algum subgrupo de  $P$  é um subgrupo minimal normal de  $G$ . Como  $N = PM$  e a ordem de  $M$  é um produto de primos que não estão em  $\pi$ , a ordem de  $P$  é potência de algum primo que está em  $\pi$  e, portanto,  $P$  é um  $p$ -grupo abeliano elementar com  $p \in \pi$ . Isso contraria a suposição inicial do caso 2, logo,  $J = \{e\}$ , isto é,  $N_G(P) \cap M = \{e\}$ . Assim,

$$|G| = |N_G(P)M| = |N_G(P)||M| = mq^\beta.$$

Donde,

$$|N_G(P)| = m,$$

pois  $|M| = q^\beta$ . Portanto,  $H = N_G(P)$  é um  $\pi$ -subgrupo de Hall. Considere  $L$  algum  $\pi$ -subgrupo de  $G$ . Como sabemos que  $G = N_G(P)M$  e  $N_G(P) = H$ ,  $G = HM$ . Assim,

$$LM = LM \cap G = LM \cap HM.$$

Como  $M \subset LM$ , pela Lei Modular de Dedekind,  $LM \cap HM = (LM \cap H)M$ .

Então,

$$LM = (LM \cap H)M.$$

Já que  $LM \cap H$  é um  $\pi$ -subgrupo de  $H$ , então

$$\frac{|LM|}{|LM \cap H|} = \frac{|(LM \cap H)M|}{|LM \cap H|}.$$

Ao desenvolvermos o resultado acima, concluiremos que:

$$\frac{|LM|}{|LM \cap H|} = \frac{|M|}{|LM \cap H \cap M|},$$

onde  $H \cap M = N_G(P) \cap M = \{e\}$ . Com isso,

$$\frac{|M|}{|LM \cap H \cap M|} = \frac{|M|}{|\{e\}|} = |M| = q^\beta.$$

Portanto  $LM \cap H$  é um  $\pi$ -subgrupo de Hall de  $LM$ . Se  $LM \not\leq G$ , pela hipótese de indução,  $L$  está contido em algum conjugado de  $LM \cap H$ . Então,

$$L \leq (LM \cap H)^x \leq H^x,$$

para algum  $x \in G$ . Se  $LM = G$ . Como  $L$  e  $M$  têm ordens coprimas,  $L \cap M = \{e\}$  e assim,  $|G| = |LM| = |L||M|$ . Mas  $|G| = mq^\beta$  e  $|M| = q^\beta$ ,  $|L| = m$ . Como  $M$  é subgrupo de  $N$ ,  $G = LM = LN$ , então

$$|G| = |LN| = \frac{|L||N|}{|L \cap N|},$$

e portanto,

$$|L \cap N| = \frac{|L||N|}{|G|} = \frac{mq^\beta p^\alpha}{mq^\beta} = p^\alpha.$$

Ainda,  $|N| = p^\alpha q^\beta$ , logo,  $L \cap N$  é um  $p$ -subgrupo de Sylow de  $N$ . O Teorema de Sylow nos diz que  $L \cap N$  é um conjugado do  $p$ -subgrupo de Sylow  $P$ . Logo,  $L \cap N = P^x$ , onde  $x \in N$ . Como  $N \triangleleft G$ ,  $L \cap N \triangleleft L$ . Então,

$$L \leq N_G(L \cap N) = N_G(P^x),$$

Sabemos que  $N_G(P^x) = N_G(P)^x = H^x$ , pois  $N_G(P^x) = \{g \in G \mid g^{-1}P^xg = P^x\}$ .

Mas,

$$g^{-1}x^{-1}P^xg = x^{-1}P^x \iff x(xg)^{-1}P(xg)x^{-1} = P,$$

e portanto,

$$N_G(P^x) = N_G(P)^x = H^x.$$

Com isso, temos que

$$L \leq H^x.$$

Portanto,  $L$  está contido em um conjugado de um  $\pi$ -subgrupo de Hall de  $G$ . Concluimos assim, a demonstração de (i) e (iii). Agora vamos provar (ii).

Considere  $K$  qualquer  $\pi$ -subgrupo de Hall de  $G$ . Como (iii) já foi mostrado,  $K \leq H^x$  para algum  $x \in G$ . Uma vez que  $K$  e  $H^x$  são  $\pi$ -subgrupos de Hall de  $G$ , ambos têm a mesma ordem, isto é,  $|K| = |H^x|$  e então  $K = H^x$ . Finalmente, com isso terminamos a demonstração.  $\square$

## Capítulo 5

# Teoria das Representações

Neste capítulo estudaremos a Teoria das Representações, que conecta duas áreas distintas da matemática, permitindo resolver os problemas de uma, usando a outra. Faremos exatamente isso na demonstração do Teorema de Burnside. Além disso, podemos aplicá-la à Física para descrever como um grupo de simetrias de um dado sistema físico afeta as soluções das equações que descrevem esse sistema. Contudo, falaremos somente o suficiente sobre representações para não fugir ao objetivo do texto. Daremos mais ênfase ao próximo capítulo, de onde sairão os resultados que usaremos diretamente na demonstração do Teorema de Burnside. O leitor que tiver interesse em estudá-la, consulte [9].

### 5.1 Representações de Grupos

A Teoria das Representação de Grupos basicamente nos permite fazer uma ponte entre a Teoria Abstrata de Grupos e a Álgebra Linear. Com isso, podemos resolver alguns problemas abstratos de Teoria de Grupos com Álgebra Linear, o que é extremamente útil, visto que a Álgebra Linear já é uma área de estudos bastante completa e fechada.

**Definição 5.1.1.** Sejam  $G$  um grupo e  $F$  um corpo tal que  $F = \mathbb{R}$  ou  $F = \mathbb{C}$ . Uma *representação de  $G$  sobre  $F$*  é um homomorfismo  $\varphi$  de  $G$  em  $\text{GL}(n, F)$  para algum inteiro  $n$ . O *grau* de  $\varphi$  é o inteiro  $n$ .

**Lembrete:**  $\text{GL}(n, F)$  é o grupo das matrizes invertíveis de ordem  $n \times n$  com entradas em  $F$ .

**Exemplo 5.1.2.** Seja  $G$  um grupo e definamos  $\varphi : G \rightarrow \text{GL}(n, F)$  por

$$\varphi(g) = I_n$$

para todo  $g \in G$ , onde  $I_n$  é a matriz identidade de ordem  $n$ . Então

$$\varphi(gh) = I_n = I_n I_n = \varphi(g)\varphi(h).$$

Assim,  $\varphi$  é uma representação de  $G$ . Note  $n$  foi escolhido arbitrariamente, o que mostra existirem representações de grau arbitrariamente grandes para qualquer grupo  $G$ .

**Definição 5.1.3.** Sejam  $\varphi$  e  $\psi$  duas representações de grau  $m$  e  $n$ , respectivamente. Dizemos que  $\varphi$  e  $\psi$  são *equivalentes* se  $n = m$  e existe uma matriz invertível  $T$   $n \times n$  tal que para todo  $g \in G$

$$\psi(g) = T^{-1}\varphi(g)T.$$

O leitor pode verificar sem grandes dificuldades que as representações equivalentes definem uma relação de equivalência.

**Definição 5.1.4.** Uma representação  $\varphi : G \rightarrow \text{GL}(2, F)$  definida por

$$\varphi(g) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

para todo  $g \in G$ , é chamada *representação trivial*.

Uma vez que uma representação é equivalente a um homomorfismo, as propriedades do núcleo de uma representação (que é definido de forma semelhante ao núcleo de um homomorfismo) são análogas as propriedades do núcleo de um homomorfismo. Em particular, temos o seguinte resultado

**Proposição 5.1.5.** Uma representação  $\varphi$  de um grupo finito  $G$  é injetora se, e somente se,  $\text{Im}\varphi$  é isomorfo a  $G$ .

**Exemplo 5.1.6.** Uma vez que  $T^{-1}AT = I$  se, e somente se,  $A = I$ , todas as representações que são equivalentes a uma representação injetora, são injetoras.

## 5.2 *FG*-módulos

Um módulo definido sobre um anel é a generalização de espaços vetorial. Nesse texto trabalharemos apenas com módulos definidos sobre corpos, apesar de serem muito mais gerais. Os módulos, além da Teoria das Representações, estão presentes em muitas outras áreas da matemática como a Geometria Algébrica e formam um conceito fundamental na Álgebra Comutativa.

**Definição 5.2.1.** Sejam  $V$  um espaço vetorial sobre  $F$  e  $G$  um grupo. Suponha que o produto  $vg$  está definido, satisfazendo as condições abaixo para todo  $u, v \in V$ ,  $\lambda \in F$  e  $g, h \in G$ :

- (i)  $vg \in V$ ,
- (ii)  $v(gh) = (vg)h$ ,
- (iii)  $ve = v$ ,
- (iv)  $\lambda(vg) = (\lambda v)g$ ,
- (v)  $(u + v)g = uv + ug$ .

Nesse caso, dizemos que  $V$  é um *FG-módulo*.

As condições (i), (iv) e (v) da definição mostram que a função  $v \mapsto vg$  é um endomorfismo de  $V$ , para todo  $g \in G$ . Neste momento o leitor certamente notou o motivo dos módulos serem uma extensão da ideia de espaço vetorial.

**Definição 5.2.2.** Sejam  $V$  um *FG-módulo* e  $\beta$  uma base do espaço vetorial  $V$ . Para cada  $g \in G$

$$[g]_{\beta}$$

denota a matriz relativa a base  $\beta$  do endomorfismo  $v \mapsto vg$  de  $V$ .

O próximo resultado vai deixar claro a conexão entre *FG*-módulos e representações de grupos. Antes disso, se  $\varphi$  é uma representação de grau  $n$  de  $G$  sobre  $F$  escrevemos  $V = F^n$  para denotar o espaço vetorial de todos os vetores linha  $(\lambda_1, \dots, \lambda_n) \in F^n$ .



**Proposição 5.2.3.** (i) se  $\varphi$  é uma representação de grau  $n$  de  $G$  sobre  $F$  e  $V = F^n$ , então  $V$  se torna um  $FG$ -módulo se definirmos a multiplicação  $vg$  por  $vg = v\varphi(g)$ .

(ii) se  $V$  é um  $FG$ -módulo e  $\beta$  uma base de  $V$ , então a função

$$g \mapsto [g]_\beta$$

com  $g \in G$  é uma representação de  $G$  sobre  $F$ .

*Demonstração.* Ver [9, p. 40]. □

A garantia de que um espaço vetorial  $V$  possa ser visto como um  $FG$ -módulo depende da definição dada para o produto. O próximo resultado vai nos ajudar a mostrar quando um produto torna  $V$  um  $FG$ -módulo.

**Proposição 5.2.4.** Seja  $\{v_1, \dots, v_n\}$  uma base para um espaço vetorial  $V$  sobre  $F$ . Suponha que tenhamos um produto  $vg$  para todo  $v \in V$  e todo  $g \in G$  tal que para todo  $i = 1, \dots, n$ , todo  $g, h \in G$  e todo  $\lambda_1, \dots, \lambda_n \in F$  satisfaz as seguintes condições:

(i)  $v_i g \in V$ ;

(ii)  $v_i(gh) = (v_i g)h$ ;

(iii)  $v_i e = v_i$ ;

(iv)  $(\lambda_1 v_1 + \dots + \lambda_n v_n)g = \lambda_1(v_1)g + \dots + \lambda_n(v_n)g$ .

Então  $V$  é um  $FG$ -módulo.

*Demonstração.* Ver [9, p. 43]. □

Para finalizar esse capítulo, definiremos homomorfismos e isomorfismos entre módulos com a finalidade de estabelecer um critério para que dois módulos sejam isomorfos.

**Definição 5.2.5.** Sejam  $V$  e  $W$   $FG$ -módulos. Uma função  $\varphi : V \rightarrow W$  é um  $FG$ -homomorfismo se  $\varphi$  é uma transformação linear que satisfaz:

$$\varphi(vg) = \varphi(v)g$$

para todo  $v \in V$  e todo  $g \in G$ .

**Definição 5.2.6.** Sejam  $V$  e  $W$   $FG$ -módulos. Dizemos que uma função  $\varphi : V \rightarrow W$  é um  $FG$ -isomorfismo se  $\varphi$  é um  $FG$ -homomorfismo e  $\varphi$  é invertível. Quando  $\varphi$  for um  $FG$ -isomorfismo, dizemos que  $V$  e  $W$  são  $FG$ -módulos isomorfos e escrevemos  $V \simeq W$ .

**Proposição 5.2.7.** Sejam  $V$  e  $W$   $FG$ -módulos. Então  $V$  e  $W$  são isomorfos se, e somente se, existe uma base  $\beta_1$  de  $V$  uma base  $\beta_2$  de  $W$  tais que

$$[g]_{\beta_1} = [g]_{\beta_2}$$

para todo  $g \in G$ .

*Demonstração.* Ver [9, p. 64]. □

## 5.3 Módulos irredutíveis

A ideia de irredutibilidade está obviamente, relacionada com a redutibilidade. Sendo assim, para que módulos possam ser irredutíveis, precisamos ter uma definição de quando eles são redutíveis e para isso, precisa existir algo “menor” do que os módulos para que possamos reduzi-los. Assim, começaremos por definir quem são esses elementos “menores”.

**Definição 5.3.1.** Seja  $V$  um  $FG$ -módulo. Um subconjunto  $W$  de  $V$  é chamado de  $FG$ -submódulo de  $V$  se  $W$  é um subespaço e  $wg \in W$  para todo  $w \in W$  e todo  $g \in G$ , isto é, um  $FG$ -submódulo é um subespaço que também é um  $FG$ -módulo.

Agora já estamos em condição de definir o que é um  $FG$ -módulo irredutível.

**Definição 5.3.2.** Um  $FG$ -módulo  $V$  é *irredutível* se é não trivial e não possui nenhum  $FG$ -submódulo diferente de  $\{0\}$  e  $V$ . Se  $V$  tem um  $FG$ -submódulo diferente de  $\{0\}$  e  $V$ , então  $V$  é *reduzível*.

Na seção anterior, mostrarmos a relação existente entre representações e módulos. Assim, é de se esperar também uma definição de quando uma representação é irredutível.

**Exemplo 5.3.3.** Para todo  $FG$ -módulo  $V$ ,  $\{0\}$  e  $V$  são  $FG$ -submódulos de  $V$ .

**Definição 5.3.4.** Uma representação  $\varphi$  de grau  $n$  é *irredutível* se  $\varphi$  corresponde a um  $FG$ -módulo  $F^n$  dado por  $vg = v\varphi(g)$  com  $v \in F^n$  e  $g \in G$  que é irredutível. Se  $F^n$  é reduzível, então  $\varphi$  é *reduzível*.

Suponha que  $V$  seja um  $FG$ -módulo reduzível, então existe um  $FG$ -submódulo  $W$  com  $0 < \dim W < \dim V$ . Seja  $\alpha$  uma base para  $W$  e estenda  $\alpha$  à uma base  $\beta$  de  $V$ . Assim, dado  $g \in G$  a matriz  $[g]_\beta$  definida anteriormente tem a forma

$$\left( \begin{array}{c|c} X_g & 0 \\ \hline Y_g & Z_g \end{array} \right) \quad (1)$$

para algumas matrizes  $X_g$ ,  $Y_g$  e  $Z_g$  onde  $X_g$  é uma matriz  $m \times m$  com  $m = \dim W$ . Logo, uma representação de grau  $n$  é reduzível se, e somente se, é equivalente a uma representação da forma (1), onde  $X_g$  é uma matriz  $m \times m$  com  $0 < m < n$ .

Para finalizar, vamos enunciar alguns resultados importantes sobre representações.

**Teorema 5.3.5** (Teorema de Maschke). *Seja  $G$  um grupo finito,  $F = \mathbb{R}$  ou  $F = \mathbb{C}$  e  $V$  um  $FG$ -módulo. Se  $U$  é um  $FG$ -submódulo de  $V$ , então existe um  $FG$ -submódulo  $W$  de  $V$  tal que*

$$V = U \oplus W.$$

A notação  $\oplus$  significa soma direta.

*Demonstração.* Ver [9, p. 71 - 72]. □

**Teorema 5.3.6** (Lema de Schur). *Sejam  $V$  e  $W$   $\mathbb{C}G$ -módulos irredutíveis.*

- (i) *se  $\varphi : V \rightarrow W$  é um  $\mathbb{C}G$ -homomorfismo, então  $\varphi$  é um  $\mathbb{C}G$ -isomorfismo ou  $\varphi \equiv 0$ .*
- (ii) *se  $\varphi : V \rightarrow V$  é um  $\mathbb{C}G$ -isomorfismo, então  $\varphi$  é um múltiplo escalar do endomorfismo identidade.*

*Demonstração.* Ver [9, p. 78 - 79].

□

## Capítulo 6

# Teoria dos Caracteres

Os caracteres de grupos tem propriedades destacáveis e, além disso, são fundamentais em cálculos na Teoria das Representações. Neste capítulo faremos um estudo básico sobre a Teoria de Caracteres, na qual se baseia totalmente a demonstração que daremos para o Teorema de Burnside. Para os capítulos posteriores, é fundamental que o leitor entenda com clareza os conceitos e propriedades que serão apresentadas aqui. Se o leitor estiver interessado num estudo mais completo sobre a Teoria dos Caracteres, recomendamos que consulte [9].

### 6.1 Caracteres de Grupos

Dada uma representação  $\varphi$  de  $G$ , a cada  $\varphi(g)$  (que é uma matriz de ordem  $n$ ) iremos associá-la ao número complexo definido pela soma dos elementos da diagonal principal e esse elemento será um caracter. Com essa teoria, poderemos resolver problemas sobre representações, como determinar se um módulo é irredutível ou não, com simples somas aritméticas, através do que definiremos como caracter de uma representação.

**Definição 6.1.1.** Seja  $A$  uma matriz  $n \times n$ . O *traço* de  $A$  é dado por

$$\text{tr} A = \sum_{i=1}^n a_{ii}.$$

Em outros termos, o traço de  $A$  é a soma de todos os elementos da diagonal principal da matriz  $A$ .

Quando definirmos o que é um caracter, o faremos por meio de uma função que, a princípio, não poderemos garantir que está bem definida. Para solucionar este problema, desenvolveremos alguns resultados úteis.

**Proposição 6.1.2.** *Sejam  $A$  e  $B$  matrizes  $n \times n$ . Então*

$$\text{tr}(A + B) = \text{tr}A + \text{tr}B$$

e

$$\text{tr}(AB) = \text{tr}(BA).$$

*Se  $T$  é uma matriz invertível  $n \times n$ , então*

$$\text{tr}(TAT^{-1}) = \text{tr}A.$$

*Demonstração.* Ver [9, p. 118]. □

**Definição 6.1.3.** Suponha que  $V$  seja um  $\mathbb{C}G$ -módulo na base  $\beta$ . Um *character* de  $V$  é a função  $\chi : G \rightarrow \mathbb{C}$  definida por

$$\chi(g) = \text{tr}[g]_{\beta}.$$

Nesta definição, apesar de ser arbitrária, a base escolhida está fixada e assim é natural a pergunta: se mudarmos o representante, teremos problemas? Isto é, a função está bem definida? Observe que dada qualquer outra base  $\beta'$  existe uma matriz invertível  $T$  tal que

$$[g]_{\beta'} = T[g]_{\beta}T^{-1}$$

e assim,

$$\text{tr}[g]_{\beta'} = \text{tr}(T[g]_{\beta}T^{-1}) = \text{tr}[g]_{\beta}.$$

De modo natural, temos a

**Definição 6.1.4.** Seja  $\varphi$  uma representação de  $G$  em  $\text{GL}(n, \mathbb{C})$ . Um *caracter*  $\chi$  da representação  $\varphi$  é dado por

$$\chi(g) = \text{tr}\varphi(g).$$

**Exemplo 6.1.5.** Sejam  $G = D_4 = \langle a, b \mid a^4 = b^2 = e, b^{-1}ab = a^{-1} \rangle$  e  $\varphi : G \rightarrow \text{GL}(2, \mathbb{C})$  a representação dada por

$$\varphi(a) = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \quad \text{e} \quad \varphi(b) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Vamos obter o caracter de  $\varphi$ :

$g$	$e$	$a$	$a^2$	$a^3$
$\varphi(g)$	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$	$\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$	$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$
$\chi(g)$	2	0	-2	0

$g$	$b$	$ab$	$a^2b$	$a^3b$
$\varphi(g)$	$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$	$\begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}$	$\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$
$\chi(g)$	0	0	0	0

**Definição 6.1.6.** Seja  $G$  um grupo. Dizemos que  $\chi$  é um *caracter* de  $G$  se  $\chi$  é um caracter de algum  $\mathbb{C}G$ -módulo. Além disso,  $\chi$  é um caracter *irredutível* de  $G$  se  $\chi$  é um caracter de algum  $\mathbb{C}G$ -módulo irredutível e  $\chi$  é um caracter *reduzível* de  $G$  se  $\chi$  é um caracter de algum  $\mathbb{C}G$ -módulo reduzível.

Encerraremos esta seção fazendo a demonstração de um resultado importante sobre caracteres.

**Proposição 6.1.7.** (i) Se  $V$  e  $W$  são  $\mathbb{C}G$ -módulos isomorfos, então eles têm o mesmo caracter.

(ii) Se  $g$  e  $h$  são conjugados em  $G$  então  $\chi(g) = \chi(h)$  para todo caracter  $\chi$  de  $G$ .

*Demonstração.* (i) Sejam  $V$  e  $W$   $\mathbb{C}G$ -módulos isomorfos. Pela proposição 5.2.7, existe uma base  $\beta_1$  de  $V$  e  $\beta_2$  de  $W$  tais que

$$[g]_{\beta_1} = [g]_{\beta_2}$$

para todo  $g \in G$ . Logo,  $\text{tr}[g]_{\beta_1} = \text{tr}[g]_{\beta_2}$  para todo  $g \in G$ , ou seja,  $V$  e  $W$  têm o mesmo caracter.

(ii) Sejam  $g$  e  $h$  conjugados em  $G$ , isto é,  $g = \alpha^{-1}h\alpha$  para algum  $\alpha \in G$ . Se  $V$  é um  $\mathbb{C}G$ -módulo e  $\beta$  uma base para  $V$ , então

$$[g]_{\beta} = [\alpha^{-1}h\alpha]_{\beta} = [\alpha^{-1}]_{\beta}[h]_{\beta}[\alpha]_{\beta}.$$

Segue da proposição 6.1.2 que  $\text{tr}[g]_{\beta} = \text{tr}[h]_{\beta}$ . Portanto,  $\chi(g) = \chi(h)$  onde  $\chi$  é um caracter de  $G$ .

□

Uma observação importante é que a recíproca do item (i) é verdadeira, isto é, dois  $\mathbb{C}G$ -módulos que tem o mesmo caracter são isomorfos. A prova desse resultado pode ser encontrada em [9].

## 6.2 Produto Interno de Caracteres

Vamos introduzir o produto interno de caracteres e apresentar algumas de suas propriedades. Não faremos aqui, mas o produto interno de caracteres nos permite obter um método para decompor um  $\mathbb{C}G$ -módulo como soma direta de  $\mathbb{C}G$ -submódulos irredutíveis. Esse método pode ser encontrado em [9].

Seja  $\mathcal{C}(G, \mathbb{C})$  o conjunto de todas as funções de  $G$  em  $\mathbb{C}$ . Se adotarmos a soma e produto usual de números complexos,  $\mathcal{C}(G, \mathbb{C})$  se torna um espaço vetorial. Sendo  $\mathcal{C}(G, \mathbb{C})$  um espaço vetorial, podemos definir um produto interno, isto é, cada  $\langle \varphi, \psi \rangle \in \mathbb{C}$  associado às funções  $\varphi$  e  $\psi$  satisfaz



1.  $\langle \varphi, \psi \rangle = \overline{\langle \psi, \varphi \rangle},$
2.  $\langle \lambda_1 \varphi_1 + \lambda_2 \varphi_2, \psi \rangle = \lambda_1 \langle \varphi_1, \psi \rangle + \lambda_2 \langle \varphi_2, \psi \rangle,$
3.  $\langle \varphi, \varphi \rangle \geq 0,$

para  $\lambda_1, \lambda_2 \in \mathbb{C}$ . Assim, a igualdade

$$\langle \varphi, \psi \rangle = \frac{1}{|G|} \sum_{g \in G} \varphi(g) \overline{\psi(g)}$$

define um produto interno.

Uma vez que um caracter é uma função de  $G$  em  $\mathbb{C}$ , acabamos de definir o produto interno entre dois caracteres. Agora vamos calcular o produto interno de dois caracteres. O fato de um caracter ser constante nas classes de conjugação nos permite simplificar o cálculo do produto interno.

**Proposição 6.2.1.** *Seja  $G$  um grupo. Suponha que  $G$  tenha uma única classe de conjugação com representantes  $g_1, \dots, g_n$ . Se  $\chi$  e  $\psi$  são caracteres de  $G$ , então:*

- (i)  $\langle \chi, \psi \rangle = \langle \psi, \chi \rangle = \frac{1}{|G|} \sum_{g \in G} \chi(g) \psi(g^{-1}).$
- (ii)  $\langle \chi, \psi \rangle = \sum_{i=1}^n \frac{\chi(g_i) \overline{\psi(g_i)}}{|C_G(g_i)|}.$

*Demonstração.* Ver [9, p. 135 - 136]. □

Como foi citado no primeiro parágrafo desta seção, como consequência do produto interno entre dois caracteres, podemos escrever um  $\mathbb{C}G$ -módulo como soma de  $\mathbb{C}G$ -submódulos irredutíveis, o que será útil para o nosso estudo. Nos resultados que estudaremos abaixo vamos considerar  $\mathbb{C}G = W_1 \oplus W_2$  onde  $W_1$  e  $W_2$  são  $\mathbb{C}G$ -submódulos sem fatores de composição em comum. Seja  $e = e_{W_1} + e_{W_2}$ .

**Proposição 6.2.2.** *Seja  $\chi$  um caracter de um  $\mathbb{C}G$ -módulo  $W_1$ . Então*

$$e_{W_1} = \frac{1}{|G|} \sum_{g \in G} \chi(g^{-1})g.$$

*Além disso,*

$$\langle \chi, \chi \rangle = \chi(e)$$

*Demonstração.* Ver [9, p. 139 - 140]. □

**Proposição 6.2.3.** *Sejam  $V$  e  $W$   $\mathbb{C}G$ -módulos irredutíveis não isomorfos com caracteres  $\chi$  e  $\psi$ , respectivamente. Então*

$$\langle \chi, \chi \rangle = 1,$$

e

$$\langle \chi, \psi \rangle = 0.$$

*Demonstração.* Ver [9, p. 140 - 141]. □

Seja  $\mathcal{V} = \{V_1, \dots, V_n\}$  um conjunto de  $\mathbb{C}G$ -módulos. Considere duas hipóteses feitas sobre  $\mathcal{V}$ :

1. Todo  $\mathbb{C}G$ -módulo irredutível é isomorfo a um  $V_i$ .
2. Para  $i \neq j$ ,  $V_i$  não é isomorfo a  $V_j$ .

Agora, considere  $G$  um grupo finito e  $\mathcal{V}$  um conjunto de  $\mathbb{C}G$ -módulos como descrito acima. Se  $\chi_i$  é um caracter de  $V_i$  então a proposição 6.2.3 implica

$$\langle \chi_i, \chi_j \rangle = \delta_{ij}$$

onde  $\delta_{ij}$  é função delta de Kronecker (isto é,  $\delta_{ij} = 1$  se  $i = j$  e 0 senão). Em particular, se os caracteres  $\chi_1, \dots, \chi_n$  não forem todos distintos, então  $\langle \chi_i, \chi_j \rangle = 1$  para algum  $i \neq j$ , o que não pode acontecer. Dessa observação, pode-se mostrar o seguinte resultado

**Proposição 6.2.4.** *Sejam  $\chi_1, \dots, \chi_n$  caracteres distintos de  $G$ . Se  $\psi$  é algum caracter de  $G$ , então*

$$\psi = \lambda_1 \chi_1 + \dots + \lambda_n \chi_n$$

para  $\lambda_i \geq 0$ .

*Demonstração.* Ver [9, p. 141]. □

## 6.3 Tabela de Caracteres e Relações de Ortogonalidade

Nesta seção veremos alguns exemplos sobre a construção de tabelas de caracteres de um grupo. Além disso, olharemos as tabelas do ponto de vista da Álgebra Linear (considerando como matrizes) e por fim, apresentaremos duas interessantes relações entre linhas e entre colunas da tabela de caracteres.

**Definição 6.3.1.** Sejam  $\chi_1, \dots, \chi_n$  caracteres irredutíveis de  $G$  e  $g_1, \dots, g_n$  representações das classes de conjugação de  $G$ . A matriz  $n \times n$  com entradas  $ij$  dadas por  $\chi_i(g_j)$  é chamada de *tabela de caracteres* de  $G$ .

É usual denotar  $\chi_1$  pelo caracter trivial e  $g_1$  pelo elemento neutro de  $G$ .

O leitor talvez tenha se perguntado se podemos garantir que o número de caracteres irredutíveis é o mesmo número de classes de conjugação de  $G$ , afinal, sem isso, a definição não teria sentido. A resposta para essa pergunta é afirmativa. Uma demonstração pode ser encontrada em [9].

**Exemplo 6.3.2.** Seja  $G = D_3 = \langle a, b \mid a^3 = b^2 = e, b^{-1}ab = a^{-1} \rangle$ . O cálculo dos caracteres de  $G$  pode ser encontrado em [9] e a prova da irredutibilidade de  $\chi_1, \chi_2$  e  $\chi_3$  em [9]. Assim:

$g$	$e$	$a$	$a^2$	$b$	$ab$	$a^2b$
$\chi_1$	1	1	1	1	1	1
$\chi_2$	1	1	1	-1	-1	-1
$\chi_3$	2	-1	-1	0	0	0

Escolhendo  $e, a$  e  $b$  como representações das classes de conjugação de  $G$  (a escolha das representações é livre desde que não se escolha dois elementos que representam a mesma classe), a tabela de caracteres é dada por

**Exemplo 6.3.3.** Seja  $G = D_8 = \langle a, b \mid a^4 = b^2 = e, b^1ab = a^{-1} \rangle$ . As representações irredutíveis de  $G$  podem ser vistas em [9] e as classes de conjugação de  $G$  em [9]. Procedendo como no exemplo anterior, obtemos:

$g$	$e$	$a$	$b$
$\chi_1$	1	1	1
$\chi_2$	1	1	-1
$\chi_3$	2	-1	0

$g$	$e$	$a^2$	$a$	$b$	$ab$
$\chi_1$	1	1	1	1	1
$\chi_2$	1	1	1	-1	-1
$\chi_3$	1	1	-1	1	-1
$\chi_4$	1	1	-1	-1	1
$\chi_5$	2	-2	0	0	0

Note que as matrizes

$$A = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & -1 \\ 2 & -1 & 0 \end{pmatrix},$$

e

$$B = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & -1 & -1 \\ 1 & 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 & 1 \\ 2 & -2 & 0 & 0 & 0 \end{pmatrix}$$

do exemplo anterior satisfazem  $\det A = -6$  e  $\det B = -64$ , ou seja,  $A$  e  $B$  são invertíveis. Isso não é apenas uma coincidência. Decorre das propriedades do produto interno de caracteres que os caracteres irredutíveis de um grupo  $G$  são linearmente independentes (pode ser visto em [9]) e com isso, as linhas da matriz da tabela de caracteres também o são. Assim, podemos enunciar a

**Proposição 6.3.4.** *A tabela de caracteres de um grupo  $G$  é uma matriz invertível.*

Ne seção anterior vimos a relação

$$\langle \chi_i, \chi_j \rangle = \delta_{ij}$$

para os caracteres irredutíveis  $\chi_1, \dots, \chi_n$  de  $G$ . Essa relação pode ser expressas em função das linhas da tabela de caracteres de  $G$  da forma

$$\sum_{k=1}^n \frac{\chi_i(g_k) \overline{\chi_j(g_k)}}{|C_G(g_k)|} = \delta_{ij}.$$

Motivados por isso, podemos obter um resultado interessante sobre as linhas e colunas da tabela de caracteres de um grupo  $G$ .

**Proposição 6.3.5.** *Sejam  $\chi_1, \dots, \chi_n$  caracteres irredutíveis de  $G$  e  $g_1, \dots, g_n$  representantes das classes de conjugação de  $G$ . As seguintes relações valem para cada  $r, s \in \{1, \dots, n\}$ :*

(i) *Relações de ortogonalidade das linhas:*

$$\sum_{i=1}^n \frac{\chi_r(g_i) \overline{\chi_s(g_i)}}{|C_G(g_i)|} = \delta_{rs}.$$

(ii) *Relações de ortogonalidade das colunas:*

$$\sum_{i=1}^n \chi_i(g_r) \overline{\chi_i(g_s)} = \delta_{rs} |C_G(g_r)|.$$

*Demonstração.* Ver [9, p. 161 - 162]. □

## 6.4 Inteiros Algébricos

Nesta seção estudaremos alguns resultados interessantes sobre caracteres. Iremos um pouco além do necessário para o nosso objetivo. Desenvolveremos essa seção com o intuito de mostrar que o grau de um caracter irredutível divide a ordem de  $G$ .

**Definição 6.4.1.** Seja  $\lambda$  um número complexo. Dizemos que  $\lambda$  é um *inteiro algébrico* se  $\lambda$  é autovalor de uma matriz com todas as entradas inteiras.

Recordemos que  $\lambda$  é autovalor da matriz  $A$  se a matriz  $A - \lambda I$  for singular, isto é,  $\det(A - \lambda I) = 0$ . Assim, podemos dizer que  $\lambda$  é um inteiro algébrico se satisfaz  $\det(A - \lambda I) = 0$  para alguma matriz  $A$  com todas as entradas inteiras.

O leitor mais acostumado com a linguagem da Álgebra Abstrata notará rapidamente que um inteiro algébrico é usualmente definido como a raiz de um polinômio mônico com coeficientes inteiros (são casos particulares dos números algébricos, que definiremos no próximo capítulo). De fato, suponha que  $\lambda$  é autovalor de uma matriz quadrada  $A$  com todas as entradas inteiras. Assim,  $\lambda$  é raiz do polinômio característico associado a matriz  $A$ , que é da forma

$$x^n + a_{n-1}x^{n-1} + \cdots + a_0$$

onde  $a_i \in \mathbb{Z}$ . Reciprocamente, suponha que  $\lambda$  é raiz de um polinômio  $p(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$  com  $a_i \in \mathbb{Z}$ . Considere a matriz

$$A = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ 0 & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ a_0 & a_1 & a_2 & \cdots & a_{n-1} \end{pmatrix}.$$

É fácil verificar que  $\det(A - xI) = p(x)$ . Logo,  $\lambda$  é autovalor de  $A$ , que tem todas as entradas inteiras. Com isso, podemos afirmar justamente que as duas definições são equivalentes.

**Proposição 6.4.2.** *O conjunto dos inteiros algébricos é fechado para a soma e o produto.*

*Demonstração.* Ver [9, p. 245 - 246]. □

Na verdade, podemos obter quase uma generalização desse resultado e mostrar que o conjunto dos números algébricos é um corpo.

Uma consequência dessa demonstração para os caracteres é que dado um caracter  $\chi$  de  $G$  e algum  $g \in G$ , então  $\chi(g)$  é um inteiro algébrico. A demonstração pode ser vista em [9, p. 246].

**Proposição 6.4.3.** *Se  $\lambda$  é racional e inteiro algébrico, então  $\lambda$  é um inteiro.*

*Demonstração.* Suponhamos que  $\lambda$  seja um racional não inteiro. Seja  $\lambda = \frac{m}{n}$  com  $m, n$  coprimos e  $|n| \neq 1$ . Seja  $p$  um primo que divide  $n$ . Para toda matriz  $A$   $k \times k$  de inteiros, as entradas de  $nA - mI$  que não estão na diagonal são divisíveis por  $n$  e então, por  $p$ . Logo,

$$\det(nA - mI) = dp + (-m)^j$$

para algum  $d \in \mathbb{Z}$ . Como  $m$  e  $n$  são coprimos,  $p$  não divide  $m$  e assim,  $\det(nA - mI) \neq 0$ . Portanto,

$$\det(A - \lambda I) = \left(\frac{1}{n}\right)^j \det(nA - mI) \neq 0,$$

ou seja,  $\lambda$  não é um inteiro algébrico. □

Da observação de que  $\chi(g)$  é um inteiro algébrico e da proposição acima, segue imediatamente que:

**Corolário 6.4.4.** *Sejam  $\chi$  um caracter de  $G$  e  $g \in G$ . Se  $\chi(g)$  é um número racional, então  $\chi(g)$  é inteiro.*

De agora em diante, vamos começar a nos preparar para concluir o objetivo desta seção, isto é, mostrar que o grau de um caracter irredutível de um grupo  $G$  divide  $|G|$ .

O grau de um caracter é definido por:

**Definição 6.4.5.** Se  $\chi$  é um caracter de um  $\mathbb{C}G$ -módulo  $V$ , então o grau de  $\chi$  é a dimensão de  $V$ .

Se  $C$  é uma classe de conjugação de  $G$ , então

$$\overline{C} = \sum_{x \in C} x \in \mathbb{C}G$$

define uma outra classe que será útil para o caminha da demonstração do próximo corolário. Nas literaturas, as vezes é comum encontrar  $\overline{C}$  sendo definido como *classe da soma*.

**Lema 6.4.6.** *Sejam  $g \in G$ ,  $C$  uma classe de conjugação contendo  $G$  e  $V$  um  $\mathbb{C}G$ -módulo irredutível com caracter  $\chi$ . Então*

$$v\overline{C} = \lambda v$$

para todo  $v \in V$ , onde

$$\lambda = \frac{|G|\chi(g)}{|C_G(g)|\chi(e)}.$$

*Demonstração.* Ver [9, p. 248]. □

**Lema 6.4.7.** *Sejam*

$$r = \sum_{g \in G} a_g g \in \mathbb{C}G$$

com  $a_g \in \mathbb{Z}$  e  $v$  um elemento não nulo de  $\mathbb{C}G$  tal que

$$vr = \lambda v$$

onde  $\lambda \in \mathbb{C}$ . Então  $\lambda$  é um inteiro algébrico.

*Demonstração.* Ver [9, p. 248 - 249]. □

**Corolário 6.4.8.** *Se  $\chi$  é um caracter irredutível de  $G$  e  $g \in G$ , então*

$$\lambda = \frac{|G|\chi(g)}{|C_G(g)|\chi(e)}$$

*é um inteiro algébrico.*

*Demonstração.* Seja  $V$  um  $\mathbb{C}G$ -submódulo irredutível de  $\mathbb{C}G$  com caracter  $\chi$  e  $\overline{C}$  a soma dos elementos na classe de conjugação de  $G$  que contém  $g$ . Então, pelo lema 6.4.6,  $v\overline{C} = \lambda v$  para todo  $v \in V$ . Assim,  $\lambda$  é um inteiro algébrico pelo lema 6.4.7. □

Como consequência desses resultados, temos o

**Teorema 6.4.9.** *Se  $\chi$  é um caracter irredutível de  $G$ , então o grau de  $\chi$  divide  $|G|$ .*



*Demonstração.* Sejam  $g_1, \dots, g_n$  representantes das classes de conjugação de  $G$ . Assim,

$$\frac{|G|\chi(g_i)}{|C_G(g_i)|\chi(e)} \text{ e } \overline{\chi(e)}$$

são inteiros algébricos. Então

$$\sum_{i=1}^n \frac{|G|\chi(g_i)\overline{\chi(g_i)}}{|C_G(g_i)|\chi(e)}$$

é um inteiro algébrico. Segue da proposição 6.3.5 item (i) que

$$\sum_{i=1}^n \frac{|G|\chi(g_i)\overline{\chi(g_i)}}{|C_G(g_i)|\chi(e)} = \frac{|G|}{\chi(e)}.$$

Mas,  $\frac{|G|}{\chi(e)}$  é racional e então, pelo corolário 6.4.4,  $\frac{|G|}{\chi(e)}$  é um inteiro, isto é,  $\chi(e)$  divide  $|G|$ .

Seja  $d = \dim V$  e  $\beta$  uma base para  $V$ . Assim,  $[1]_\beta = I$  e então

$$\chi(e) = \text{tr}[1]_\beta = \text{tr}I = d,$$

ou seja,  $\chi(e) = \dim V$ . Portanto, o grau de  $\chi$  divide  $|G|$ . □

Precisaremos estender um pouco mais esses conceitos. Faremos isso no próximo capítulo, apresentando os números algébricos, dos quais os inteiros algébricos são apenas uma pequena parte.

# Capítulo 7

## O Teorema de Burnside

O Teorema de Burnside tem importância fundamental na demonstração do segundo Teorema de P. Hall. Vale a pena ressaltar que é possível demonstrá-lo sem o uso da Teoria de Representações e Caracteres, apenas usando conceitos de Teoria dos Grupos. No entanto, essa demonstração é mais complicada, exigindo um bom domínio de Teoria de Grupos e a compreensão de ideias nada intuitivas, o que foge ao escopo desse texto. Para o leitor interessado nesta outra demonstração, consultar [1], [5] e [11].

### 7.1 Números Algébricos

Vamos introduzir alguns conceitos preliminares como preparação para a demonstração do Teorema de Burnside. Os conceitos que serão estudados nesta seção envolvem polinômios definidos sobre corpos abstratos mas, sobre o corpo dos números reais, agem de forma semelhante a propriedade da separabilidade dos números reais fornecida pela divisão  $\mathbb{R} = \mathbb{Q} \cup (\mathbb{R} \setminus \mathbb{Q})$ . Para uma leitura mais completa sobre anéis, corpos e polinômios veja [6].

Para o nosso objetivo, é suficiente estudar os números algébricos definidos sobre o corpo dos números complexos. Vale ressaltar que eles não se limitam somente  $\mathbb{C}$ , mas podem ser definidos sobre corpos muito mais abstratos.

**Definição 7.1.1.** Seja  $\mathbb{C}$  o corpo dos números complexos. Dizemos que  $\alpha \in \mathbb{C}$  é um

número algébrico se  $p(\alpha) = 0$  para algum polinômio  $p(x) \in \mathbb{Q}[x]$ .

É comum encontrar na literatura disponível a exigência do polinômio  $p$  ser *mônico*, isto é, o coeficiente líder ser 1. As vezes pode ser conveniente usar isso como definição quando se tem em vista demonstrações específicas, no entanto, não é necessário pois, uma vez que o polinômio está definido sobre um corpo, podemos evidenciar o coeficiente líder obtendo  $p(x) = \ell q(x)$  onde  $q(x)$  é um polinômio mônico. Esclarecidos esses detalhes, continuemos.

**Definição 7.1.2.** Seja  $\alpha$  um número algébrico e  $p(x)$  o polinômio mônico de menor grau possível que tem  $\alpha$  como raiz. Dizemos que  $p(x)$  é o *polinômio minimal* de  $\alpha$ . Se  $p(x)$  é o polinômio minimal, dizemos que as raízes de  $p(x)$  são os *conjugados* de  $\alpha$ .

Os números algébricos e os polinômios minimais são de grande importância na Teoria de Corpos. Por meio deles definimos as extensões algébricas, que são estruturas fundamentais na Teoria de Galois. O leitor que estiver interessado em mais detalhes, consulte [12].

A proposição abaixo é usada na demonstração de um importante lema, apesar de não prová-la nesse texto ela faz conexões importantes entre caracteres e inteiros algébricos. Com isso achamos válido apresentá-la ao leitor.

**Proposição 7.1.3.** *Sejam  $\alpha, \beta$  números algébricos e  $\tilde{\alpha}, \tilde{\beta}$  os conjugados de  $\alpha$  e  $\beta$ , respectivamente. Então todo conjugado de  $\alpha + \beta$  é da forma  $\tilde{\alpha} + \tilde{\beta}$ . Além disso, se  $r \in \mathbb{Q}$ , então qualquer conjugado de  $r\alpha$  é da forma  $r\tilde{\alpha}$ .*

*Demonstração.* Ver [13, p. 64 - 65]. □

A título de curiosidade, nós podemos dividir um corpo  $K$  em dois conjuntos, o conjunto dos números algébricos e dos transcendentos. Os números algébricos estão conectados com as extensões algébricas, que por sua vez, têm um papel muito importante na Teoria de Galois. Os números transcendentos representam ainda um campo muito ativo de estudo na Teoria dos Números. Ainda existem problemas relativamente simples na sua formulação que, no entanto, são extremamente difíceis de se

demonstrar. Um fato interessante é que se pensarmos no corpo  $\mathbb{R}$ , ambos os conjuntos são densos, isto é, eles estão espalhados pela reta real de modo que, fixado um ponto da reta, por mais que você possa se aproximar desse ponto sempre existirão tanto números algébricos quanto transcendentos ao redor do ponto em questão. Isso nos faz pensar que os dois conjuntos são “muito grandes”. Talvez o leitor se surpreenda em saber que na verdade, o conjunto dos números de transcendentos é muito maior que o conjunto dos números algébricos e além disso, existe um conjunto infinito de números transcendentos, os números de Liouville, que tem o “mesmo tamanho” do conjunto dos algébricos, ou seja, esse conjunto de transcendentos tem representação quase irrelevante dentro do conjunto de todos os transcendentos. Com isso queremos mostrar que o estudo de números algébricos vai muito além das aplicações que estamos dando aqui.

Antes de chegarmos ao resultado final desta seção, lembremos que um número complexo  $\omega$  é chamado *raiz  $m$ -ésima da unidade* quando  $\omega^m = 1$  e, pelo Teorema Fundamental da Álgebra, essa equação possui exatamente  $m$  raízes em  $\mathbb{C}$ .

**Lema 7.1.4.** *Sejam  $\chi$  um caracter de um grupo finito  $G$  e  $g \in G$ . Então*

$$|\chi(g)/\chi(e)| \leq 1$$

e se

$$0 < |\chi(g)/\chi(e)| < 1$$

então  $\chi(g)/\chi(e)$  não é um inteiro algébrico.

*Demonstração.* Primeiro, é uma consequência do Lema de Schur que  $\chi(g)$  é uma soma de  $m$ -ésimas raízes da unidade (o resultado pode ser encontrado em [9], p. 123).

Seja  $\chi(e) = d$ . Então

$$\chi(g)/\chi(e) = \frac{\omega_1 + \cdots + \omega_d}{d}$$

onde cada  $\omega_i$  é uma raiz da unidade. Da desigualdade triangular, temos que  $|\chi(g)| \leq |\omega_1| + \cdots + |\omega_d| = d$ , isto é  $|\chi(g)/\chi(e)| \leq 1$ .

Agora, suponhamos que  $\alpha = \chi(g)/\chi(e)$  seja um inteiro algébrico e  $|\alpha| < 1$ .

Seja

$$p(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$$

o polinômio minimal de  $\alpha$ . Pela proposição 7.1.3, um conjugado de  $\alpha$  é da forma

$$\frac{\tilde{\omega}_1 + \cdots + \tilde{\omega}_d}{d}$$

onde  $\tilde{\omega}_i$  é raiz da unidade. Assim, os conjugados de  $\alpha$  tem módulo no máximo 1. Se  $\lambda$  é o produto de todos os conjugados de  $\alpha$ , então  $|\lambda| < 1$ . Mas cada conjugado de  $\alpha$  também é raiz de  $p(x)$  e, uma vez que o coeficiente líder é 1, segue das Relações de Girard que o produto de todas as raízes é igual a  $\pm a_0$ , ou seja,  $\lambda = \pm a_0$ . Mas  $a_0 \in \mathbb{Z}$  e  $|a_0| < 1$ , logo,  $a_0 = 0$ . Uma vez que  $p(x)$  é irredutível,  $p(x) = x$ . Assim,  $\alpha = 0$  o que implica  $\chi(g) = 0$ .  $\square$

## 7.2 Teorema de Burnside

Usando alguns resultados na Teoria de Caracteres e dois lemas (um da seção anterior), vamos provar um resultado também devido à Burnside. Com esse resultado e alguns outros sobre Grupos Solúveis, concluiremos o famoso Teorema de Burnside para grupos solúveis.

**Lema 7.2.1.** *Sejam  $p$  um número primo e  $r \in \mathbb{N}$ . Suponha que  $G$  seja um grupo finito com uma classe de conjugação de ordem  $p^r$ , então  $G$  não é simples.*

*Demonstração.* Ver [9, p. 363 - 364].  $\square$

**Teorema 7.2.2** (Burnside  $p^\alpha q^\beta$ ). *Sejam  $p, q$  números primos e  $\alpha, \beta \in \mathbb{N}$  com  $\alpha + \beta \geq 2$ . Se  $G$  é um grupo com  $|G| = p^\alpha q^\beta$  então  $G$  não é simples.*

*Demonstração.* Primeiro, suponhamos que  $\alpha = 0$  ou  $\beta = 0$ , então  $G$  é um  $p$ -grupo e pela proposição 2.1.9,  $Z(G) \neq \{e\}$ . Seja  $g \in Z(G)$  um elemento de ordem prima. Assim,  $\langle g \rangle \triangleleft G$ . Uma vez que  $\langle g \rangle \neq \{e\}$  e  $\langle g \rangle \neq G$ , então  $G$  não é simples. Suponhamos agora  $\alpha, \beta > 0$ . Pelo Teorema de Sylow,  $G$  tem um subgrupo  $Q$  com  $|Q| = q^\beta$ . Temos

que  $Z(G) \neq \{e\}$ . Seja  $g \in Z(G)$  com  $g \neq e$ . Assim,  $\langle g \rangle$  é um subgrupo de  $C_G(g)$  e então

$$|g^G| = [G : C_G(g)] = p^r,$$

para algum  $r$ . Se  $p^r = 1$ , então  $g \in Z(G)$  e  $Z(G) \neq \{e\}$ , isto é,  $G$  não é simples. Se  $p^r > 1$ ,  $G$  não é simples pelo lema 7.2.1.  $\square$

Neste momento já temos todas as ferramentas para demonstrar o Teorema de Burnside para Grupos Solúveis. Mãos à obra!

**Teorema 7.2.3** (Teorema de Burnside). *Se  $G$  é um grupo com  $|G| = p^\alpha q^\beta$ , então  $G$  é solúvel.*

*Demonstração.* Se  $\alpha + \beta \leq 1$ , o resultado é imediato ( $G$  é cíclico de ordem prima, logo, abeliano e, portanto, solúvel). Assim, vamos assumir que  $\alpha + \beta \geq 2$ .

Seja  $G$  um grupo de ordem  $p^\alpha q^\beta$  com  $\alpha + \beta \geq 2$ . Pelo teorema 7.2.2,  $G$  não é um grupo simples, isto é, existe um subgrupo não trivial  $H$  de  $G$  com  $H \triangleleft G$ . Temos que  $H$  e  $G/H$  são grupos com ordem um produto de potências de  $p$  e  $q$  e, pela hipótese de indução, ambos são solúveis. Pela proposição 3.2.4,  $G$  é solúvel.  $\square$

Com o fim desse capítulo, todo o trabalho está essencialmente feito para que possamos demonstrar o Segundo Teorema de Philip Hall. Precisaremos apenas definir mais alguns conceitos e de alguns resultados mais diretos.

## Capítulo 8

### O Teorema de Philip Hall (1937)

Este segundo teorema fornece uma recíproca para o primeiro e com isso, podemos obter uma condição necessária e suficiente, isto é, um resultado para determinar se um dado grupo é solúvel ou não. Antes de provar de fato esse trabalho, precisamos desenvolver um pouco dos Sistemas e Bases de Sylow.

#### 8.1 Sistema de Sylow e Base de Sylow

Os sistemas de Sylow e as bases de Sylow agem de forma muito semelhante aos grupos de Sylow. Eles são o mais perto de uma generalização dos grupos de Sylow para um conjunto de grupos dados. Assim como o Teorema de Sylow garante a existência e conjugação entre grupos de Sylow, provaremos nesta seção que valem resultados semelhantes para sistemas de Sylow e bases de Sylow.

**Definição 8.1.1.** Sejam  $G$  um grupo finito e  $p_1, \dots, p_k$  primos distintos que dividem  $|G|$ . Suponha que  $Q_i$  seja um  $p'_i$ -subgrupo de Hall de  $G$ , então o conjunto  $\{Q_1, \dots, Q_k\}$  é chamado de *sistema de Sylow*.

Observe que  $p'$  representa o conjunto de todos os primos diferentes de  $p$ , ou seja,  $p'$  representa o complementar do  $p$ . Falado isso, podemos dizer que um  $p'$ -subgrupo de Hall de um grupo finito  $G$  é chamado de *p-complemento*.

**Proposição 8.1.2.** Se  $G$  é um grupo solúvel finito, então existe um sistema de Sylow.

*Demonstração.* É uma consequência imediata do Primeiro Teorema de Philip Hall, uma vez que sendo  $G$  um grupo solúvel finito,  $G$  possui um  $\pi$ -subgrupo de Hall para  $\pi = \{p_1, \dots, p_k\}$ .  $\square$

**Definição 8.1.3.** Sejam  $G$  um grupo e  $P_1, \dots, P_k$  elementos de um conjunto  $\mathcal{C}$  tal que  $P_i$  seja um  $p_i$ -subgrupo de Sylow de  $G$  para  $i = 1, \dots, k$  e  $\mathcal{C}$  é mutuamente permutável, então  $\mathcal{C}$  é chamado de *base de Sylow*.

**Proposição 8.1.4.** Seja  $\{Q_1, \dots, Q_k\}$  um sistema de Sylow de um grupo solúvel finito  $G$ . Então:

(i) Se  $\pi$  é um conjunto de primos quaisquer, então

$$\bigcap_{p_i \notin \pi} Q_i$$

é um  $\pi$ -subgrupo de Hall de  $G$ . Em particular,

$$P_i = \bigcap_{j \neq i} Q_j$$

é um  $p_i$ -subgrupo de Sylow de  $G$ .

(ii) Os subgrupos de Sylow  $P_1, \dots, P_k$  são permutáveis em pares, isto é,  $P_i P_j = P_j P_i$ .

*Demonstração.* Seja  $|G| = p_1^{n_1} \dots p_k^{n_k}$ , onde  $|G : Q_i| = p_i^{n_i}$ . Assim,

$$H = \bigcap_{p_i \notin \pi} Q_i$$

tem índice

$$\prod_{p_i \notin \pi} p_i^{n_i}.$$

De fato,

$$|G : H| \leq p_1^{n_1} \dots p_k^{n_k} = \prod_{p_i \notin \pi} |G : Q_i| = \prod_{p_i \notin \pi} p_i^{n_i},$$

mas como os índices de  $|G : Q_i|$  com  $p_i \notin \pi$  são coprimos, pelo lema 3.3.1

$$|G : H| = \prod_{p_i \notin \pi} p_i^{n_i}.$$



Portanto, concluímos que  $H$  é um  $\pi$ -subgrupo de Hall de  $G$ . Aplicando este resultado para  $\pi = \{p_i, p_j\}$  com  $i \neq j$ , temos que

$$K = \bigcap_{k \neq i, j} Q_k$$

é um  $\pi$ -subgrupo de Hall com ordem  $p_i^{n_i} p_j^{n_j}$  contendo  $P_i$  e  $P_j$ . Como  $|P_i P_j| = p_i^{n_i} p_j^{n_j}$ , temos que  $P_i P_j = K = P_j P_i$ .  $\square$

Pela proposição 8.1.4, se  $\mathcal{S} = \{Q_1, \dots, Q_k\}$  é um conjunto de sistemas de Sylow de um grupo solúvel finito  $G$ , então existe uma correspondente base de Sylow.

$$\mathcal{S}^* = \{P_1, \dots, P_k\},$$

dada por

$$P_i = \bigcap_{j \neq i} Q_j.$$

Claro que a recíproca também vale, pois

$$Q_j = \prod_{i \neq j} P_i.$$

Assim, obtemos os seguintes corolários:

**Corolário 8.1.5.** *Um grupo solúvel finito possui um sistema de Sylow e uma base de Sylow.*

**Corolário 8.1.6.** *Se  $G$  é um grupo solúvel finito, a função  $\mathcal{S} \rightarrow \mathcal{S}^*$  é um bijeção entre o conjunto de sistema de Sylow e o conjunto das bases de Sylow.*

**Definição 8.1.7.** Dois sistemas de Sylow  $\{Q_1, \dots, Q_k\}$  e  $\{\bar{Q}_1, \dots, \bar{Q}_k\}$  são ditos *conjugados* em  $G$  se existe  $g \in G$  tal que  $Q_i^g = \bar{Q}_i$ , para  $i = 1, \dots, k$ .

**Definição 8.1.8.** Duas bases de Sylow  $\{P_1, \dots, P_j\}$  e  $\{\bar{P}_1, \dots, \bar{P}_j\}$  são ditas *conjugadas* em  $G$  se existe  $g \in G$  tal que  $P_i^g = \bar{P}_i$ , para  $i = 1, \dots, j$ .

Assim como relacionamos a conjugação entre dois subgrupos de Sylow, podemos relacionar dois sistemas de Sylow e duas bases de Sylow via conjugação.

**Proposição 8.1.9.** *Em um grupo solúvel finito  $G$ , quaisquer dois sistemas de Sylow são conjugados, assim como quaisquer duas bases de Sylow.*

*Demonstração.* Considere  $\zeta_i$  o conjunto de todos os  $p'_i$ -subgrupos de Hall de  $G$ . Definiremos uma ação de  $G$  nesse conjunto via conjugação. Pelo Primeiro Teorema de Philip Hall sabemos que todos os  $\pi$ -subgrupos de Hall em  $G$  são conjugados e assim, temos que a ação de  $G$  é transitiva ( $\forall Q_1, Q_2 \in \zeta_i$ , existe  $g \in G$  tal que  $Q_1^g = Q_2$ ). Consequentemente

$$|\zeta_i| = [G : N_G(Q_i)],$$

com  $Q_i \in \zeta_i$ . Mas

$$[G : Q_i] = [G : N_G(Q_i)] [N_G(Q_i) : Q_i],$$

logo,  $|\zeta_i|$  divide  $[G : Q_i] = p_i^{\alpha}$ .

Agora,  $G$  age via conjugação no conjunto  $\zeta = \zeta_1 \times \cdots \times \zeta_k$  de todos os sistemas de Sylow. Um elemento de  $G$  fixa  $(Q_1, \dots, Q_k)$  se, e somente se, normaliza cada  $Q_i$  e, portanto, o estabilizador de  $(Q_1, \dots, Q_k)$  em  $G$  é a interseção de todos os  $N_G(Q_i)$ , o qual tem índice igual a

$$\prod_{i=1}^k |\zeta_i| = |\zeta|,$$

pois como os índices  $[G : N_G(Q_i)]$  são coprimos, pelo lema 3.3.1,

$$\left[ G : \bigcap_{i=1}^k N_G(Q_i) \right] = \prod_{i=1}^k [G : N_G(Q_i)] = |\zeta|.$$

Assim, concluímos que  $G$  é transitivo em  $\zeta$ , pois

$$|G| = |\zeta| \left| \bigcap_{i=1}^k N_G(Q_i) \right|,$$

o que nos diz que quaisquer sistemas de Sylow são conjugados.

Aplicando o corolário 8.1.6, lembrando a bijeção

$$\mathcal{S} \rightarrow \mathcal{S}^* : Q_i \rightarrow \bigcap_{i \neq j} Q_j = P_i,$$

deduzimos que

$$Q_i^g \rightarrow \bigcap_{i \neq j} Q_j^g = \left( \bigcap_{i \neq j} Q_j \right)^g = P_i^g,$$

logo, concluímos que quaisquer duas bases de Sylow são conjugadas.  $\square$

## 8.2 Segundo Teorema de Philip Hall

Finalmente já estamos em condições de demonstrar o Segundo Teorema de Philip Hall e então estabelecer um critério para classificação de grupos quanto a solubilidade. Os pontos chaves para essa demonstração são o Teorema de Wielandt e o Teorema de Burnside. Procederemos por indução.

**Teorema 8.2.1** (Segundo Teorema de Philip Hall). *Seja  $G$  um grupo que possui  $p'$ -subgrupo de Hall para todo primo  $p$ , então  $G$  é solúvel.*

*Demonstração.* Usaremos indução em  $r = |\pi(G)|$ .

Se  $r = 1$ , então  $G$  é um  $p$ -grupo e como todo  $p$ -grupo é nilpotente, e grupos nilpotentes são solúveis logo,  $G$  é solúvel. Se  $r = 2$ , então  $|G| = p^\alpha q^\beta$ , com  $p$  e  $q$  primos. Pelo teorema de Burnside,  $G$  é solúvel. Se  $r \geq 3$ , então  $G$  possui subgrupos  $S_1, S_2$  e  $S_3$  que são  $p'_i$ -subgrupos de Hall. Observe também que  $[G : S_1] = p_1^{\alpha_1}$ ,  $[G : S_2] = p_2^{\alpha_2}$  e  $[G : S_3] = p_3^{\alpha_3}$ , logo os índices são dois a dois coprimos. Sejam  $1 \leq i \neq j \leq r$  e  $T_{ij} = S_i \cap S_j$ . Temos que  $[G : T_{ij}] = [G : S_i][G : S_j]$ , pelo lema 3.3.1. Assim,

$$\frac{|G|}{|T_{ij}|} = \frac{|G|}{|S_i|} \frac{|G|}{|S_j|} \iff \frac{|S_i||S_j|}{|T_{ij}|} = |G|,$$

mas  $\frac{|S_i||S_j|}{|T_{ij}|} = |S_i S_j|$  e, portanto,  $S_i S_j = G$ . Como

$$p_j^{\alpha_j} = \frac{|G|}{|S_j|} = \frac{|S_i|}{|T_{ij}|} = \frac{|p_1^{\alpha_1} \dots p_{i-1}^{\alpha_{i-1}} p_{i+1}^{\alpha_{i+1}} \dots p_r^{\alpha_r}|}{|T_{ij}|},$$

$T_{ij}$  é um  $p_j$ -complemento de Sylow de  $S_i$ , isto é,  $T_{ij}$  é um  $p'_j$ -subgrupo de Hall de  $S_i$ . Assim,  $S_i$  está nas hipóteses do teorema e como  $|\pi(S_i)| = r - 1$ , por indução,  $S_i$  é solúvel. Concluimos então que  $S_1, S_2$  e  $S_3$  são solúveis. Pelo Teorema de Wielandt,  $G$  é solúvel.  $\square$

Com a demonstração desse segundo teorema, podemos estabelecer o seguinte critério:

**Teorema 8.2.2.** *Um grupo  $G$  é solúvel se, e somente se, possui um  $p'$ -subgrupo de Hall para todo primo  $p$ .*

Com isso, concluímos o nosso objetivo.

Existe um artigo muito interessante publicado na edição de 1981 do Journal of Algebra que traz um novo critério para solubilidade de grupos proveniente do critério de Philip Hall. A título de curiosidade, o critério é:

**Teorema 8.2.3.** *Um grupo  $G$  é solúvel se, e somente se, tem um  $2'$ -subgrupo de Hall e um  $3'$ -subgrupo de Hall.*

O artigo traz uma demonstração para um caso particular, para grupos com os fatores de composição sendo grupos simples. O leitor que estiver interessado, veja [17].

Além desses critérios para solubilidade de grupos, existe um resultado muito famoso que apesar de não ser um critério para a determinação de solubilidade, é um resultado fortíssimo, a saber:

**Teorema 8.2.4** (Feit-Thompson). *Todo grupo de ordem ímpar é solúvel.*

A demonstração pode ser lida em [3].

## Considerações Finais

O objetivo desta monografia foi estudar não somente um critério que classifica grupos quanto à solubilidade, mas construir um caminho para isso explorando as conexões entre grupos, representações e caracteres. Apresentamos duas classes de grupos, os solúveis e os nilpotentes, que normalmente não são estudadas em um curso de graduação, o que faz uma excelente complementação ao conteúdo estudado num curso regular de Teoria de Grupos.

O interesse do autor por esse trabalho se originou durante sua participação no Programa de Iniciação Científica fomentado pelo CNPq. Além disso, o estudo dos Teoremas de Hall teve um papel muito importante na escolha do autor sobre o seu prosseguimento na matemática após a graduação, optando por dar prosseguimento ao estudo da Teoria de Grupos num curso de Mestrado em Matemática. O tempo investido nesse estudo trouxe não só mais conhecimento, mas uma nova forma de enxergar a Matemática. Além disso, trouxe independência para estudar matemática, o que foi extremamente útil durante a graduação.

## Referências Bibliográficas

- [1] BENDER, H. *A group theoretic proof of Burnside's  $p^a q^b$ -theorem*, Math. Z. 126 (1972), 327-338
- [2] DOERK, K.; HAWKES, T. *Finite Soluble Groups*, Walter de Gruyter, New York, 1992.
- [3] FEIT, W.; THOMPSON, J. *Solvability of Groups of odd order*, Pacific Journal of Mathematics 3 (1963). 775-1029.
- [4] GARCIA A.; LEQUAIN Y. *Elementos de Álgebra*, IMPA, Rio de Janeiro, 2015.
- [5] GOLDSCHMIDT, D.M. *A group-theoretic proof of the  $p^a q^b$ -theorem for odd primes*, Math. Z. 113 (1970), 373-375.
- [6] GONÇALVES, A. *Introdução à álgebra*, IMPA, Rio de Janeiro, 2006.
- [7] HERSTEIN, I. N. *Topics in Algebra*, John Wiley & Sons, New York, 1975.
- [8] HUNGERFORD, T. W. *Algebra*, Springer-Verlag, New York, 1974.
- [9] JAMES, G.; LIEBECK, M. *Representations and Characters of Groups*, Cambridge University Press, New York, 2003.
- [10] KURZWEIL, H.; STELLMACHER, B. *Theory of Finite Groups*, Springer-Verlag, New York, 2004.
- [11] MATSUYAMA, H. *Solvability of groups of order  $2^a p^b$* , Osaka Journal of Mathematics 10 (1973), 375-378.

- [12] MORANDI, P. *Field and Galois Theory*, Springer-Verlag, New York, 1996.
- [13] POLLARD, H.; DIAMOND, G. H. *The Theory of Algebraic Numbers*, Mathematical Association of America, USA, 1975.
- [14] ROSE, H.E. *A Course on Finite Groups*, Springer, New York, 2009.
- [15] ROTMAN, J.J. *An Introduction to the Theory of Groups*, Sringer-Verlag, New York, 1995.
- [16] SLOANE, N. J. A. The on-line encyclopedia of integer sequence. *Order of non-solvable groups, i.e, numbers that are not solvable numbers*. 1964. Disponível em: <<https://oeis.org/A056866>>. Acesso em: 1 set 2018.
- [17] WARD, M. B.; ARAD Z. *New criteria for the Solvability of Finite Groups*, Journal of Algebra 77 (1981). 234-246.