Universidade do Estado da Bahia
Departamento de Ciências Humanas - Campus VI
Curso de Licenciatura em Matemática
Trabalho de Conclusão de Curso

UMA GENERALIZAÇÃO PARA OS TEOREMAS DE SYLOW

JOSÉ MARCOS GOMES DOS SANTOS

Caetité - BA

2025

JOSÉ MARCOS GOMES DOS SANTOS

UMA GENERALIZAÇÃO PARA OS TEOREMAS DE SYLOW

Monografia apresentada ao Curso de Licenciatura em Matemática do Departamento de Ciências Humanas, campus VI, da Universidade do Estado da Bahia, como requisito para obtenção do grau de Licenciado em Matemática.

Orientador:
Prof. Dr. Genildo de Jesus Nery

Caetité - BA

2025

Universidade do Estado da Bahia
Departamento de Ciências Humanas
Curso de Licenciatura em Matemática

UMA GENERALIZAÇÃO PARA OS TEOREMAS DE SYLOW

por

JOSÉ MARCOS GOMES DOS SANTOS

Monografia apresentada ao Curso de Licenciatura em Matemática do Departamento de Ciências Humanas, campus VI, da Universidade do Estado da Bahia, como parte dos requisitos para obtenção do grau de

Licenciado em Matemática.

Caetité - BA, 23 de dezembro de 2024.

Comissão Examinadora:

Prof. Dr. Genildo de Jesus Nery - UNEB (Orientador)

Profa. Dra. Nathália Nogueira Gonçalves - UnB

Prof. MSc. Leandro Correia Araújo - UESB

"A essência da matemática é a liberdade."

— Georg Cantor

Agradecimentos

Gostaria de expressar minha profunda gratidão a todos que contribuíram para a realização deste trabalho.

À minha querida mãe, Marlúcia, por seu amor incondicional e apoio constante, que sempre foram a base de tudo que conquistei. Ao meu irmão, Mauro, por sempre me incentivar nos estudos. À minha irmã Pâmela, por proporcionar momentos de felicidade quando se fez mais necessário.

Aos meus amigos da faculdade, que tornaram essa jornada mais leve e divertida. Suas companhias foram essenciais nos momentos mais difíceis, e juntos compartilhamos muitas risadas e desafios.

Ao meu orientador, Genildo de Jesus Nery, por sua orientação, paciência e sabedoria. Suas valiosas contribuições foram fundamentais para a conclusão deste trabalho.

Por fim, agradeço a meu ídolo, Lionel Messi, cuja história de superação e dedicação é uma fonte de inspiração para mim.

A todos vocês, o meu mais sincero obrigado.

Resumo

Neste trabalho apresentamos uma generalização para os Teoremas de Sylow, devido a Philip Hall, em termos de grupos solúveis finitos.

Palavras-chave: Grupos finitos; Teoremas de Sylow; Teoremas de Hall.

Abstract

In this work we present a generalization for Sylow's Theorems, due to Philip Hall, in terms of finite soluble groups.

Keywords: Finite groups; Sylow's Theorems; Hall's Theorems.

Notação

$\mathbb{Z}, \mathbb{Q}, \mathbb{R}$	conjuntos dos números inteiros, números racionais, números reais
$\text{mdc}(a, b)$	máximo divisor comum de a, b
$a \mid b$, $a \nmid b$	a divide b, a não divide b
$n\mathbb{Z}$	grupo dos múltiplos de n
$\mathbb{Z}_n$	grupo $\{0, 1, \ldots, n-1\}$ sob adição módulo n
$\lvert G \rvert$	ordem do grupo G
$\lvert g \rvert$	ordem do elemento g
$H \subset G$	H está contido propriamente em G
$H \subseteq G$	H está contido em G
$H \supset G$	H contém propriamente G
$H \supseteq G$	H contém G
$H \leqslant G$	H é subgrupo de G
$H < G$	H é subgrupo próprio de G
$H \triangleleft G$	H é subgrupo normal de G
$G \triangleright H$	H é subgrupo normal de G
$H \text{char } G$	H é subgrupo característico de G
G/H	grupo quociente
$\lvert G : H \rvert$	índice de H em G
$\text{Ker}(f)$	núcleo do homomorfismo f
S_n	grupo simétrico ou grupo das permutações
K_4	grupo de Klein
A_n	grupo alternado
$Stab_G(x)$	$\{g \in G \mid g \cdot x = x\}$ estabilizador de x em G
$Orb_G(x)$	$\{g \cdot x \mid g \in G\}$ órbita de x
$[x, y]$	comutador de x e y
$G' := [G, G]$	subgrupo derivado de G

Sumário

Introdução

Na Teoria de Grupos Finitos, um dos resultados centrais é o Teorema de Lagrange, que diz que para um grupo finito G, a ordem de qualquer subgrupo de G divide a ordem de G. Aqui, a ordem de G é definida como sendo o número de elementos de G.

Um fato curioso, é que a teoria de grupos ainda não tinha sido inventada quando o matemático italiano Joseph Louis Lagrange apresentou a primeira versão desse resultado. A primeira versão do Teorema de Lagrange foi publicada em 1770, em um trabalho que tratava sobre a resolução de polinômios de grau maior que 4. A versão que usaremos neste trabalho, provavelmente foi provada pelo matemático francês Évariste Galois, uma vez que existem registros publicados no Diário de Liouville em 1846 que evidencia esse fato (ver [10], para mais detalhes).

Vale salientar que a recíproca do Teorema de Lagrange, não é verdade em geral. O contraexemplo mais conhecido é o grupo alternado A_4, que é um subgrupo do grupo simétrico S_4, formado por todas as permutações pares. O grupo A_4 tem ordem 12, mas não possui subgrupo de ordem 6 (ver [3, Exemplo 5, p. 149]).

Em 1872, o matemático norueguês Ludwig Sylow, provou que dado um grupo finito G, se p^k, com p sendo um número primo, divide a ordem de G, então G tem pelo menos um subgrupo de ordem p^k. Esse resultado é conhecido como Primeiro Teorema de Sylow, uma homenagem a Ludwig Sylow, que foi o primeiro a demonstrá-lo. Nota-se que esse teorema nos dá uma recíproca parcial para o Teorema de Lagrange.

Existem mais dois teoremas devido Ludwig Sylow, que também são ferramentas valiosas dentro da teoria dos grupos finitos e, quando utilizados em conjunto com o Primeiro Teorema de Sylow, formam um método poderoso a identificação de grupos simples finitos. Essa classe de grupo são os "blocos de construção" de todos os grupos finitos, assim como os números primos são para os números inteiros positivos maiores que 1, isto é, qualquer grupo finito pode ser decomposto em grupos simples, tornando essencial o conhecimento de todos os possíveis grupos simples. Com isso em mente, os matemáticos Camille Jordan e Otto Hölder, em meados do século XX, iniciaram o processo de classificação dos grupos simples finitos. A classificação completa dos grupos simples finitos, contudo, só se deu após trinta anos e envolveu os esforços combinados de centenas de matemáticos de todo o mundo, abrangendo cerca de 10.000 páginas de revistas científicas (ver [5]).

Devido a importância dos Teoremas de Sylow para o desenvolvimento da Teoria de Grupos Finitos, é interessante identificar classes de grupos finitos para as quais valem uma generalização desses teoremas. Nesse trabalho, apresentamos uma generalização, devido a Philip Hall [7], para a classe dos grupos solúveis finitos.

Organizamos esta monografia em três capítulos. O primeiro capítulo é composto por todo o arcabouço necessário para compreender os resultados apresentados nos capítulos subsequentes. No segundo capítulo enunciamos e provamos os três teoremas de Sylow. Além disso, apresentamos também algumas aplicações desses teoremas. Por fim, no terceiro capítulo, enunciamos e provamos os Teoremas de Hall.

Capítulo

1

Preliminares

Neste capítulo, apresentaremos noções básicas da Teoria de Grupos e alguns resultados que serão úteis para o entendimento desta monografia.

1.1 Grupos e subgrupos

Definição 1.1.1. *Um conjunto G não vazio munido com uma operação binária*

$$\begin{aligned} * : \ G \times G &\to G \\ (a,b) &\mapsto a*b \end{aligned}$$

é um grupo se as propriedades de (i)–(iv) são válidas:

(i) $a * b \in G$ *para todos* $a, b \in G$;

(ii) $(a * b) * c = a * (b * c)$ *para todos* $a, b, c \in G$;

(iii) Existe um elemento e em G, que chamaremos de identidade de G, tal que

$$a * e = e * a = a;$$

(iv) Para todo elemento a de G existe um elemento a' em G, que chamaremos de inverso de a, tal que

$$a * a' = a' * a = e.$$

Se, além disso, a operação $*$ em G satisfaz a propriedade

(v) $a * b = b * a$ *para todos* $a, b \in G$;

dizemos que G é um grupo abeliano.

Às vezes, quando for necessário destacar a operação de um grupo G, escreveremos $(G, *)$ em vez de G. Além disso, quando não houver ambiguidade, utilizaremos a notação multiplicativa ab para denotar $a * b$. Assim, com essa notação escreveremos a^{-1} para denotar o inverso do elemento a e 1 para denotar o elemento identidade de G.

Exemplo 1.1.2.

1. *O conjunto dos número inteiros $\mathbb{Z}$ munido a operação de adição usual é um grupo abeliano.*

2. *O conjunto de todas as matrizes inversíveis $n \times n$ com entradas reais é um grupo, denotado por $\mathrm{GL}(n, \mathbb{R})$, chamado de* ***grupo linear geral****: aqui a operação é a multiplicação usual de matrizes, 1 é a matriz identidade $n \times n$ e A^{-1} é a inversa da matriz A. Se $n \geq 2$, então $\mathrm{GL}(n, \mathbb{R})$ é não abeliano.*

3. *Seja C um conjunto qualquer não vazio. O conjunto*

$$Bij(C) = \{f : C \to C \mid f \text{é uma bijeção}\}$$

munido com a operação de composição de funções, é um grupo, não abeliano em geral. Caso o conjunto C tenha um número finito n de elementos, $Bij(C)$ será denotado por S_n e será chamado ***grupo simétrico*** *ou* ***grupo das permutações****.*

Proposição 1.1.3. *Em um grupo G, vale as seguintes propriedades:*

(i) O elemento identidade de G é único;

(ii) O inverso de cada elemento de G é único.

Demonstração. (i) Suponhamos que e e e' sejam duas identidades no grupo G. Então,

$$\begin{aligned} e &= ee' \quad (\text{pois } e' \text{ é identidade}) \\ &= e' \quad (\text{pois } e \text{ é identidade}). \end{aligned}$$

Portanto, $e = e'$.

(ii) Sejam b e c dois inversos do elemento a no grupo G. Vamos mostrar que $b = c$. Note que,

$$\begin{aligned} b &= be \\ &= b(ac) \quad (\text{pois } c \text{ é inverso de } a) \\ &= (ba)c \\ &= ec \quad (\text{pois } b \text{ é inverso de } a) \\ &= c. \end{aligned}$$

Portanto, $b = c$ e está provado que o inverso de cada elemento é único.

□

A próxima proposição nos diz como obter o inverso do produto de dois elementos de um grupo.

Proposição 1.1.4. *Se a e b são elementos de um grupo G, então $(ab)^{-1} = b^{-1}a^{-1}$.*

Demonstração. Note que,

$$\begin{aligned}(ab)(b^{-1}a^{-1}) &= a(bb^{-1})a^{-1}\\ &= (ae)a^{-1}\\ &= aa^{-1}\\ &= e\end{aligned}$$

e

$$\begin{aligned}(b^{-1}a^{-1})(ab) &= b^{-1}(a^{-1}a)b\\ &= (b^{-1}e)b\\ &= b^{-1}b\\ &= e.\end{aligned}$$

Assim, pela unicidade dos inversos vista no item (ii) da Proposição 1.1.3, $(ab)^{-1} = b^{-1}a^{-1}$. □

Observação 1.1.5. *Vale salientar que, se G é um grupo abeliano, então*

$$(ab)^{-1} = a^{-1}b^{-1}.$$

Em um grupo, vale a lei do cancelamento.

Proposição 1.1.6. *Sejam a e b elementos de um grupo G. Se $ba = ca$, então $b = c$; e se $ab = ac$, então $b = c$;*

Demonstração. Suponhamos que $ba = ca$. Operando a^{-1} à direita, em ambos o membros desta equação, obtemos

$$\begin{aligned}(ba)a^{-1} = (ca)a^{-1} &\Rightarrow b(aa^{-1}) = c(aa^{-1})\\ &\Rightarrow be = ce\\ &\Rightarrow b = c.\end{aligned}$$

Analogamente, prova-se que se $ab = ac$, então $b = c$. □

Considerar subconjuntos de um grupo que preservam as propriedades que define um grupo, são úteis para a caracterização dessas estruturas.

Definição 1.1.7. *Se um subconjunto H de um grupo G é ele próprio um grupo com a operação de G, dizemos que H é um subgrupo de G. Escreveremos $H \leqslant G$ para denotar que H é um subgrupo de G.*

Para determinarmos se um subconjunto H de um grupo G é um subgrupo de G, podemos aplicar o seguinte teste.

Proposição 1.1.8 (Teste de Subgrupo)**.** *Um subconjunto H de um grupo G é um subgrupo de G se, e somente se,*

(i) $ab \in H$ *para todos* $a, b \in H$*;*

(ii) o elemento identidade de G pertence a H;

(iii) para cada $h \in H$*, tem-se que* $h^{-1} \in H$*.*

Demonstração. ($\Rightarrow$) Suponhamos que H seja um subgrupo de G. Em particular, H é um grupo com a operação de G. Desse modo, os itens (i) e (iii) são satisfeitos. Agora, sejam $a \in H \subseteq G$, e_H a identidade de H e e_G a identidade de G. Então,

$$\begin{aligned} e_H a = a &\Rightarrow (e_H a)a^{-1} = aa^{-1} \\ &\Rightarrow e_H(aa^{-1}) = e_G \\ &\Rightarrow e_H e_G = e_G \\ &\Rightarrow e_H = e_G. \end{aligned}$$

Portanto, $e_G \in H$.

($\Leftarrow$) Suponhamos que os itens $(i), (ii)$ e (iii) sejam satisfeitos. Vamos mostrar que o subconjunto H é um subgrupo de G, isto é, H é um grupo sobre a operação de G. Do item (i), segue que a operação é fechada em H. A operação em H é associativa, uma vez que a mesma é associativa em G. Do item (ii) segue que H possui um elemento identidade. Por fim, segue do item (iii) que todo elemento de H possui inverso. Portanto, o subconjunto H de G é um grupo e, consequentemente, é um subgrupo de G. □

Veremos agora alguns exemplos de subgrupos.

Exemplo 1.1.9. *Seja G um grupo.*

1. *Os subconjuntos de G, $\{e\}$ e próprio G, são claramente subgrupos de G. Esses subgrupos serão chamados de* ***subgrupos triviais*** *de G.*

2. *O subconjunto*

$$Z(G) = \{a \in G \mid ax = xa, \text{ para todo } x \in G\}$$

de G, que chamaremos de ***centro*** *do grupo G, é um subgrupo de G. De fato, dados $a, b \in Z(G)$ e $x \in G$, temos*

$$\begin{aligned}(ab)x &= a(bx)\\ &= a(xb)\\ &= (ax)b\\ &= (xa)b\\ &= x(ab).\end{aligned}$$

Logo, $ab \in Z(G)$. Claramente, a identidade de G, e, pertence a $Z(G)$. Agora, seja $a \in Z(G)$. Então, para todo $x \in G$, tem-se que

$$\begin{aligned}ax = xa &\Rightarrow a^{-1}(ax)a^{-1} = a^{-1}(xa)a^{-1}\\ &\Rightarrow (a^{-1}a)xa^{-1} = a^{-1}x(aa^{-1})\\ &\Rightarrow exa^{-1} = a^{-1}xe\\ &\Rightarrow xa^{-1} = a^{-1}x.\end{aligned}$$

Logo, $a^{-1} \in Z(G)$ e, portanto, segue pelo teste de subgrupo que $Z(G)$ é um subgrupo de G.

3. *Fixado um elemento $a \in G$, definimos o* ***centralizador de*** *a* ***em*** *G como sendo o conjunto*

$$C(a) = \{g \in G \mid ga = ag\}.$$

Vamos mostrar que $C(a)$ é um subgrupo de G. Para isso, dados $x, y \in C(a)$, temos

$$\begin{aligned}(xy)a &= x(ya)\\ &= x(ay)\\ &= (xa)y\\ &= (ax)y\\ &= a(xy).\end{aligned}$$

Logo, $xy \in C(a)$. Claramente, a identidade de G, e, pertence a $C(a)$. Agora, seja $x \in C(a)$. Então,

$$\begin{aligned} xa = ax &\Rightarrow x^{-1}(xa)x^{-1} = x^{-1}(ax)x^{-1} \\ &\Rightarrow (x^{-1}x)ax^{-1} = x^{-1}a(xx^{-1}) \\ &\Rightarrow eax^{-1} = x^{-1}ae \\ &\Rightarrow ax^{-1} = x^{-1}a. \end{aligned}$$

Logo, $x^{-1} \in C(a)$. *Portanto,* $C(a) \leqslant G$.

1.1.1 Grupos Cíclicos

Sejam G um grupo e S um subconjunto não-vazio do grupo G. Para o que segue, S^{-1} denotará o conjunto $\{a^{-1} \mid a \in S\}$ e a^0 denotará a identidade de G. Consideremos o conjunto

$$\langle S \rangle := \{a_1 a_2 \dots a_n \mid n \in \mathbb{N}, a_i \in S \text{ ou } a_i \in S^{-1}\}.$$

Afirmamos que $\langle S \rangle \leqslant G$. De fato, sejam $x, y \in \langle S \rangle$. Então $x = a_1 a_2 \dots a_n$, com $a_i \in S$ ou $a_i \in S^{-1}$ e $y = b_1 b_2 \dots b_m$, com $b_j \in S$ ou $b_j \in S^{-1}$. Note que,

$$xy = a_1 a_2 \dots a_n b_1 b_2 \dots b_m \in \langle S \rangle$$

e

$$x^{-1} = a_n^{-1} a_{n-1}^{-1} \dots a_2^{-1} a_1^{-1} \in \langle S \rangle.$$

Além disso,

$$xx^{-1} = (a_1 a_2 \dots a_n a_n^{-1} \dots a_2^{-1} a_1^{-1}) = (a_1 a_2 \dots a^0 \dots a_2^{-1} a_1^{-1}) = \dots = a_1 a_1^{-1} = a^0.$$

Portanto $a^0 \in \langle S \rangle$ e, pelo Teste de Subgrupo, $\langle S \rangle$ é subgrupo de G.

Definição 1.1.10. *Seja G um grupo. O subgrupo $\langle S \rangle$ é chamado de subgrupo gerado por um subconjunto S não-vazio de G. Em particular, se $S = \{a\}$, o subgrupo $\langle a \rangle := \langle \{a\} \rangle$ é chamado de subgrupo cíclico de G gerado por a. Além disso, se $G = \langle a \rangle$, dizemos que G é um grupo cíclico gerado por a.*

Note que se G é um grupo cíclico gerado por a, segue diretamente da definição que

$$G = \{a^n \mid n \in \mathbb{Z}\}.$$

Observação 1.1.11. *Para um grupo cíclico $G = \langle a \rangle$, há duas possibilidades:*

(i) $a^n = e$ para algum inteiro positivo n. Neste caso, G é finito.

(ii) $a^n \neq e$ *para todo inteiro positivo* n. *Neste caso, todas as potências de* a *são distintas e, portanto,* G *é infinito.*

Proposição 1.1.12. *Todo grupo cíclico é abeliano.*

Demonstração. Sejam G um grupo cíclico e $a \in G$ tal que $G = \{a^n \mid n \in \mathbb{Z}\}$. Se $x_1, x_2 \in G$, então $x_1 = a^{n_1}$ e $x_2 = a^{n_2}$, com $n_1, n_2 \in \mathbb{Z}$. Daí,

$$\begin{aligned} x_1 x_2 &= a^{n_1} a^{n_2} \\ &= a^{n_1+n_2} \\ &= a^{n_2+n_1} \\ &= a^{n_2} a^{n_1} \\ &= x_2 x_1. \end{aligned}$$

Portanto, G é abeliano. □

Proposição 1.1.13. *Todo subgrupo de um grupo cíclico é cíclico.*

Demonstração. Seja G um grupo cíclico. Então, existe $a \in G$ tal que $G = \langle a \rangle$. Se $H \leqslant G$, então existem três possibilidades, que são: H é um subgrupo trivial, ou seja, $H = \{e\}$ ou $H = G$. Em ambos os casos temos que H é cíclico. A outra possibilidade é H ser um subgrupo próprio de G, isto é, $H \neq \{e\}$ e $H \neq G$. Neste caso, existe um menor inteiro positivo n tal que $a^n \in H$. Claramente, temos que $\langle a^n \rangle \subseteq H$. Por outro lado, se $h \in H$, então h é da forma a^m, pois H é um subgrupo de G, que é um grupo cíclico. Pelo algoritmo da divisão de Euclides, existem inteiros q e r tais que $m = nq + r$ com $0 \leq r < n$. Assim,

$$a^m = a^{nq+r} = a^{nq} a^r, \quad \text{com } 0 \leq r < n,$$

ou seja,

$$a^r = a^{-nq} a^m \in H.$$

Dessa forma, podemos ter somente $r = 0$, já que supomos que n é o menor inteiro positivo para o qual $a^n \in H$. Assim, todo elemento $h \in H$ é da forma a^{qn}, o que nos leva a concluir que $H \subseteq \langle a^n \rangle$. Consequentemente, por conta da dupla inclusão, temos $H = \langle a^n \rangle$ e, portanto, H é cíclico.

□

A definição seguinte desempenha um papel fundamental para o estudo dos grupos finitos.

Definição 1.1.14. *A ordem de um grupo* G, *denotada por* $|G|$, *indica a quantidade de elementos de* G. *A ordem de um elemento* $g \in G$, *é igual à ordem do subgrupo cíclico gerado por ele.*

1.1.2 Grupos de Permutação

Nesta seção vamos apresentar algumas propriedades dos grupos

$$S_n := Bij(S) = \{\sigma : S \to S \,|\, \sigma \text{ é uma bijeção}\}$$

das permutações de um conjunto finito $S = \{a_1, \ldots, a_n\}$ (ver Exemplo 1.1.2). Uma permutação $\sigma \in S_n$ também pode ser representada na forma de arranjo:

$$\begin{pmatrix} a_1 & a_2 & a_3 & \cdots & a_n \\ \sigma(a_1) & \sigma(a_2) & \sigma(a_3) & \cdots & \sigma(a_n) \end{pmatrix}.$$

Com base na definição acima, é fácil calcular a ordem de S_n. Note que existem n escolhas para definir $\sigma(a_1)$, $(n-1)$ escolhas para definir $\sigma(a_2)$, $(n-2)$ escolhas para definir $\sigma(a_3)$ e assim, sucessivamente, de modo que

$$|S_n| = n \cdot (n-1) \cdot (n-2) \ldots 3 \cdot 2 \cdot 1 = n!$$

O matemático francês Cauchy, em 1815, introduziu uma nova notação para expressar uma permutação σ, a **notação cíclica**. Essa notação possui vantagens teóricas porque certas propriedades importantes podem ser facilmente determinadas quando a notação cíclica é utilizada.

Definição 1.1.15. *Uma permutação $\sigma \in S_n$ chama-se r-ciclo, quando existem $a_1, a_2, \ldots, a_r \in \{1, 2, 3, \ldots, r\}$ tais que $\sigma(a_1) = a_2, \sigma(a_2) = a_3, \ldots, \sigma(a_{r-1}) = a_r, \sigma(a_r) = a_1$, e $\sigma(i) = i$, para todo $i \in \{1, 2, 3, \ldots, r\} \backslash \{a_1, a_2, \ldots, a_r\}$; tal r-ciclo será denotado por $\sigma = (a_1 a_2 \ldots a_r)$; o número r é chamado o comprimento do ciclo. Em particular, um 2-ciclo chama-se transposição.*

Exemplo 1.1.16. *A permutação*

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix}$$

em notação cíclica, é dada por

$$\sigma = (12345).$$

Observação 1.1.17. *1. Note que pela definição de r-ciclos, a ordem dos elementos de cada ciclo não interfere na representação da permutação. Assim, para a permutação σ do exemplo 1.1.16, também é válida a seguinte notação em ciclos:*

$$\sigma = (23451), \text{ ou } \sigma = (34512), \text{ ou } \sigma = (45123), \text{ ou } \sigma = (51234).$$

2. *A identidade, ε, de S_n em notação cíclica é denotada apenas por um ciclo. Por exemplo,*

$$\varepsilon = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix}$$

pode ser escrita como $\varepsilon = (1)$. Lembrando sempre que os elementos ausentes são fixos.

Proposição 1.1.18. *Toda permutação de um conjunto finito pode ser escrita como um ciclo ou como o produto de ciclos disjuntos.*

Demonstração. Ver [3, Theorem 5.1, p.104-105] . □

Exemplo 1.1.19. *A permutação*

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 5 & 4 \end{pmatrix}$$

é representada da seguinte forma em notação cíclica:

$$\sigma = (12)(3)(45).$$

Proposição 1.1.20. *Toda permutação em S_n, $n > 1$, pode ser escrita como um produto de transposições.*

Demonstração. Primeiramente, note que a identidade ε de S_n pode ser expressa como $(12)(12)$, e assim, é o produto de transposições. Pela Proposição 1.1.18, toda permutação pode ser escrita na forma

$$(a_1a_2\cdots a_k)(b_1b_2\cdots b_t)\cdots(c_1c_2\cdots c_s).$$

Um cálculo direto mostra que isso é o mesmo que

$$(a_1a_k)(a_1a_{k-1})\cdots(a_1a_2)(b_1b_t)\cdots(b_1b_{t-1})\cdots(b_1b_2)\cdots(c_1c_s)(c_1c_{s-1})\cdots(c_1c_2).$$

□

Exemplo 1.1.21. *A permutação*

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix}$$

pode ser representada da seguinte forma:

$$\sigma = (12345) = (15)(14)(13)(12).$$

A definição seguinte será importante para definirmos um subgrupo especial do grupo simétrico S_n.

Definição 1.1.22. *Uma permutação $\sigma \in S_n$ é par se σ pode ser escrita como um produto de um número par de transposições; e σ é ímpar quando σ pode ser escrita como um produto de um número ímpar de transposições.*

O conjunto de todas as permutações pares de S_n, denotado por A_n, é um grupo. Com efeito, a identidade ε de S_n está em A_n, pois é uma permutação par, como visto na demonstração da Proposição 1.1.20. Sejam $\sigma, \pi \in A_n$. Então,

$$\sigma = \underbrace{(a_1a_k)(a_1a_{k-1})\cdots(a_1a_2)}_{\text{número par de transposições}}$$

e

$$\pi = \underbrace{(b_1b_t)(b_1b_{t-1})\cdots(b_1b_2)}_{\text{número par de transposições}}.$$

Daí,

$$\sigma\pi = \underbrace{(a_1a_k)(a_1a_{k-1})\cdots(a_1a_2)(b_1b_t)(b_1b_{t-1})\cdots(b_1b_2)}_{\text{número par de transposições}}$$

de modo que $\sigma\pi \in A_n$. Uma vez que

$$\sigma^{-1} = \underbrace{(a_1a_2)(a_1a_3)\cdots(a_1a_k)}_{\text{número par de transposições}},$$

segue que $\sigma^{-1} \in A_n$. Portanto, segue pelo Teste de Subgrupo que A_n é um subgrupo de S_n e, consequentemente, A_n é um grupo.

Definição 1.1.23. *O grupo A_n é chamado de grupo alternado.*

Proposição 1.1.24. *A ordem de A_n é $n!/2$.*

Demonstração. É claro que se $n = 1$, então $|A_n| = 1$, pois $\varepsilon \in S_1$ é uma permutação par. Assim, vamos supor que $n \geq 2$. Seja B_n o conjunto das permutações ímpares de S_n. Consideremos a transposição $\alpha = (12)$ e a aplicação

$$\begin{aligned} f_\alpha : \ A_n &\to B_n \\ \beta &\mapsto \alpha\beta. \end{aligned}$$

Inicialmente, note que f_α está bem-definida, pois α é uma transposição, de modo que $\alpha\beta \in B_n$. Agora, sejam $\beta_1, \beta_2 \in A_n$ com $f_\alpha(\beta_1) = f_\alpha(\beta_2)$, então,

$$\begin{aligned} f_\alpha(\beta_1) = f_\alpha(\beta_2) &\Rightarrow \alpha\beta_1 = \alpha\beta_2 \\ &\Rightarrow \beta_1 = \beta_2. \end{aligned}$$

Logo, f_α é injetora.

Por outro lado, dado $\theta \in B_n$, segue que $\alpha\theta$ é uma permutação par. Além disso, como $\alpha^2 = \varepsilon$, temos que

$$f_\alpha(\alpha\theta) = \alpha(\alpha\theta) = \alpha^2\theta = \varepsilon\theta = \theta.$$

Logo f_α é sobrejetora e, portanto, bijetora. Assim, A_n e B_n têm a mesma cardinalidade. Uma vez que

$$S_n = A_n \cup B_n \text{ e } A_n \cap B_n = \emptyset,$$

temos que

$$\begin{aligned} |A_n| + |B_n| = |S_n| &\Rightarrow 2|A_n| = n! \\ &\Rightarrow |A_n| = \frac{n!}{2}. \end{aligned}$$

Portanto, a ordem de A_n é $n!/2$.

□

1.2 Subgrupos Normais e Grupo quociente

Sejam H um subgrupo de um grupo G e $a, b \in G$. Definimos as relações $\sim_E$ e $\sim_D$ em G por

$$a \sim_E b \text{ se, e somente se, } a^{-1}b \in H$$

e

$$a \sim_D b \text{ se, e somente se, } ab^{-1} \in H.$$

Proposição 1.2.1. *As relações $\sim_E$ e $\sim_D$ são relações de equivalência em G.*

Demonstração. Por definição, uma relação é dita ser uma relação de equivalência, se ela for reflexiva, simétrica e transitiva. Desse modo, vamos verificar se $\sim_E$ e $\sim_D$ satisfazem essas três propriedades. Iniciaremos por $\sim_E$. Note que, para $a, b, c \in G$, tem-se que

- como $a^{-1}a = e \in H$, então $a \sim_E a$ e, portanto, a relação é $\sim_E$ reflexiva.
- se $a \sim_E b$, então $a^{-1}b \in H$. Como H é um subgrupo de G, temos que

$$(a^{-1}b)^{-1} = b^{-1}a \in H.$$

Assim, $b \sim_E a$ e, portanto, a relação $\sim_E$ é simétrica.

- se $a \sim_E b$ e $b \sim_E c$, então $(a^{-1}b), (b^{-1}c) \in H$. Daí,

$$(a^{-1}b)(b^{-1}c) = a^{-1}c \in H.$$

Logo, $a \sim_E c$ e, portanto, a relação $\sim_E$ é transitiva.

Portanto, a relação $\sim_E$ é uma relação de equivalência. A demonstração para a relação $\sim_D$ é análoga.

□

O conjunto

$$\overline{a}_E = \{x \in G \mid x \sim_E a\}$$

é a classe de equivalência que contém o elemento a com respeito a relação $\sim_E$. Similarmente,

$$\overline{a}_D = \{x \in G \mid x \sim_D a\}$$

é a classe de equivalência que contém o elemento a com respeito a relação $\sim_D$.

Proposição 1.2.2. *Sejam H um subgrupo de um grupo G e $a \in G$. Então,*

$$\overline{a}_E = aH = \{ah \mid h \in H\} \quad e \quad \overline{a}_D = Ha = \{ha \mid h \in H\}.$$

Demonstração. Se $x \in \overline{a}_E$, então $x \sim_E a$, ou seja, $x^{-1}a \in H$. Portanto, $x^{-1}a = h$ para algum $h \in H$. Daí,

$$\begin{aligned} x^{-1}a = h &\Rightarrow (xx^{-1})a = xh \\ &\Rightarrow ah^{-1} = x(hh^{-1}) \\ &\Rightarrow ah^{-1} = x. \end{aligned}$$

Logo, $x \in aH$ e, portanto, $\overline{a}_E \subseteq aH$.

Por outro lado, se $x \in aH$, então $x = ah$ para algum $h \in H$. Então,

$$\begin{aligned} x = ah &\Rightarrow xh^{-1} = a(hh^{-1}) \\ &\Rightarrow (x^{-1}x)h^{-1} = x^{-1}a \\ &\Rightarrow h^{-1} = x^{-1}a. \end{aligned}$$

Logo, $x^{-1}a \in H$, o que implica, $x \sim_E a$ e, assim, $x \in \overline{a}_E$. Portanto, $aH \subseteq \overline{a}_E$.

Dos dois parágrafos anteriores concluímos que $\overline{a}_E = aH$. De forma similar, mostra-se que $\overline{a}_D = Ha$. □

O conjunto aH será chamado de **classe lateral à esquerda de H em G contendo** a, enquanto que Ha será chamado de **classe lateral à direita de H em G contendo** a. Em ambos os casos, o elemento a será chamado de **representante da classe**.

Definição 1.2.3. *A cardinalidade do conjunto das classes laterais à esquerda (ou direita) é o índice de H em G, que aqui denotaremos por $|G : H|$.*

Definição 1.2.4. *Um subgrupo H de um grupo G é chamado de subgrupo normal de G, e denotaremos por $H \triangleleft G$, se $gH = Hg$ para todo $g \in G$.*

Sejam G um grupo e $H \leqslant G$. Para o que segue, consideremos o conjunto

$$gHg^{-1} = \{ghg^{-1} \mid h \in H\},$$

para um elemento fixado $g \in G$.

Proposição 1.2.5 (Teste de Subgrupo Normal)**.** *Seja H um subgrupo de um grupo G. As afirmações seguintes são equivalentes:*

(i) $gH = Hg$ *para todo* $g \in G$*;*

(ii) $gHg^{-1} = H$ *para todo* $g \in G$*;*

(iii) $ghg^{-1} \in H$ *para todos* $g \in G, h \in H$*.*

Demonstração. $(i) \Rightarrow (ii)$. Multiplique cada termo da igualdade por g^{-1} à direita.
$(ii) \Rightarrow (iii)$. É imediato.
$(iii) \Rightarrow (i)$. Seja $h \in H$ e $g \in G$. Então,

$$hg = (gg^{-1})hg = g(g^{-1}hg) = g(g^{-1}h(g^{-1})^{-1}) \in gH$$

e

$$gh = gh(g^{-1}g) = (ghg^{-1})g \in Hg.$$

Portanto, $gH = Hg$.

□

Exemplo 1.2.6.

(a) É imediato verificar que, todo subgrupo de um grupo abeliano é normal.

(b) O centro, $Z(G)$, de qualquer grupo G é sempre normal em G. Com efeito, seja $u \in xZ(G)x^{-1}$ para todo $x \in G$. Então, existe $a \in Z(G)$ tal que $u = xax^{-1}$. Uma vez que os elementos de $Z(G)$ comutam com todo elemento de G, temos que

$$u = xax^{-1} = axx^{-1} = ae = a \in Z(G).$$

Portanto, $u \in Z(G)$ e assim $xZ(G)x^{-1} \subset Z(G)$. Logo, pelo teste de subgrupo normal temos que $Z(G) \triangleleft G$.

Definição 1.2.7. *Um subgrupo normal H de um grupo G é um subgrupo normal minimal se $H \neq \{1\}$ e não existe um subgrupo normal K de G tal que $\{1\} < K < H$.*

Note que todo grupo finito não-trivial sempre possui um subgrupo normal minimal. De fato, seja H_1 um subgrupo normal de um grupo G. Se H_1 satisfaz a condição da Definição 1.2.7, terminamos; se não satisfaz, então existe um subgrupo normal $H_2 \subset H_1$. Se H_2 satisfaz a condição da Definição 1.2.7, terminamos; se não satisfaz, repetimos o processo feito em H_1. Esse processo deve necessariamente acabar, pois obtemos subgrupos normais $H_1, H_2, \ldots$ cada vez menores, enquanto que o grupo G é finito.

Lema 1.2.8. *Sejam H e K subgrupos de um grupo G. Se H é normal em G, então $HK := \{hk \,|\, h \in H, k \in K\}$ é um subgrupo de G.*

Demonstração. Vamos utilizar o Teste de Subgrupo. Como $e \in H$ e $e \in K$, então $e = ee \in HK$. Sejam $a, b \in HK$, então $a = h_1k_1$ e $b = h_2k_2$, com $h_1, h_2 \in H$ e $k_1, k_2 \in K$. Como $H \triangleleft G$ e $k_1 \in G$, existe $h' = k_1h_2k_1^{-1} \in H$. Daí,

$$ab = (h_1k_1)(h_2k_2) = h_1(k_1h_2k_1^{-1}k_1)k_2 = h_1(k_1h_2k_1^{-1})(k_1k_2) = (h_1h')(k_1k_2),$$

assim, $ab \in HK$.

Note que $a^{-1} = (h_1k_1)^{-1} = (k_1^{-1}h_1^{-1})$, para $h_1 \in H$ e $k_1 \in K$. Como $H \triangleleft G$ e $k_1 \in G$, existe $h' = k_1^{-1}h_1^{-1}k_1 \in H$. Daí,

$$a^{-1} = (k_1^{-1}h_1^{-1}) = (k_1^{-1}h_1^{-1})(k_1k_1^{-1}) = (k_1^{-1}h_1^{-1}k_1)k_1^{-1} = h'k_1^{-1},$$

assim, $a^{-1} \in HK$.

Portanto, segue pelo Teste de Subgrupo que HK é um subgrupo de G. □

Proposição 1.2.9. *A interseção de todos os subgrupos normais de um grupo G é um subgrupo normal de G.*

Demonstração. Seja S a interseção de todos os subgrupos normais de G. Claramente, a identidade e de G está em S. Agora, seja $s \in S$. Dessa forma, s pertence a cada subgrupo normal de G, de modo que gsg^{-1} pertence a cada subgrupo normal de G para todo $g \in G$. Consequentemente, $gsg^{-1} \in S$ e, portanto, S é um subgrupo normal do grupo G. □

Usando subgrupos normais, podemos construir mais exemplos de grupos. Seja N um subgrupo normal de um grupo G. Consideremos o conjunto

$$G/N = \{aN \mid a \in G\}.$$

Queremos definir uma estrutura de grupo em G/N. Para isso, equipamos esse conjunto com a seguinte operação binária

$$(aN)(bN) = abN,\ a, b \in G. \tag{1.1}$$

Lema 1.2.10. *A operação binária* (1.1) *em* G/N *é bem definida.*

Demonstração. Precisamos mostrar que, dados $x \in aN$ e $y \in bN$, $xyN = abN$, ou seja, que $xy \sim_E ab$. Como $x \in aN$, então $x^{-1}a \in N$. Daí, $(x^{-1}a)b \in Nb = bN = yN$, pois N é um subgrupo normal. Logo, existe $n \in N$ tal que

$$x^{-1}ab = yn \Rightarrow y^{-1}x^{-1}ab = n \Rightarrow (xy)^{-1}ab = n.$$

Portanto, $xy \sim_E ab$ e a operação definida em (1.1) está bem definida. □

Proposição 1.2.11. *Se* G *é um grupo e* $N \lhd G$*, então* G/N *munido com a operação definida em* (1.1) *é um grupo.*

Demonstração. Vamos verificar se G/N munido com a operação definida em (1.1) satisfaz as propriedades de (i) a (iv) da Definição 1.1.1.

Claramente a operação é fechada. A associatividade é satisfeita, pois dados $aN, bN, cN \in G/N$ tem-se que

$$\begin{aligned} aN((bN)(cN)) &= aN(bc)N \\ &= a(bc)N \\ &= (ab)cN \\ &= (ab)NcN \\ &= ((aN)(bN))cN. \end{aligned}$$

O conjunto G/N possui uma identidade com respeito a operação (1.1), pois, se e a identidade de G e $aN \in G/N$, tem-se

$$(eN)(aN) = (ea)N = aN$$

e

$$(aN)(eN) = (ae)N = aN.$$

Portanto, $eN = N$ é o elemento identidade em G/N com respeito a operação (1.1).

Cada elemento de G/N possui inverso com respeito a operação (1.1). De fato, seja $aN \in G/N$. Note que,

$$(aN)(a^{-1}N) = (aa^{-1})N = N$$

e

$$(a^{-1}N)(aN) = (a^{-1}a)N = N.$$

Logo, $a^{-1}N$ é o inverso de aN em G/N quando esse conjunto está munido com a operação (1.1).

Portanto, G/N é um grupo.

□

Exemplo 1.2.12. *Uma vez que $\mathbb{Z}$ é um grupo abeliano, temos que $n\mathbb{Z} \lhd \mathbb{Z}$. Assim, $\mathbb{Z}/n\mathbb{Z}$ é um grupo. Esse grupo possui exatamente n elementos. De fato, temos que os elementos de $\mathbb{Z}/n\mathbb{Z}$ são classes de equivalências da forma $x + n\mathbb{Z}$, para $x \in \mathbb{Z}$. Vamos listar algumas dessas classes:*

$$0 + n\mathbb{Z}, 1 + n\mathbb{Z}, 2 + n\mathbb{Z}, \ldots, (n-1) + n\mathbb{Z}.$$

Observe que se tomarmos $n + n\mathbb{Z}$, recaíremos na classe $0 + n\mathbb{Z} = n\mathbb{Z}$, uma vez que $n \in nZ$. Ao tomarmos $(n+1) + n\mathbb{Z}$ recaíremos na classe $1 + n\mathbb{Z}$ e assim, sucessivamente. Portanto, concluímos que $\mathbb{Z}/n\mathbb{Z} = \{n\mathbb{Z}, 1 + n\mathbb{Z}, 2 + n\mathbb{Z}, \ldots, (n-1) + n\mathbb{Z}\}$, onde $n\mathbb{Z}$ é o elemento identidade.

Proposição 1.2.13. *Sejam G um grupo abeliano e N um subgrupo de G. Então, G/N é um grupo abeliano.*

Demonstração. Uma vez que G é um grupo abeliano, temos que $N \lhd G$ e, assim, G/N é um grupo. Vamos mostrar que G/N é abeliano. Dados $aN, bN \in G/N$, temos que

$$\begin{aligned}(aN)(bN) &= (ab)N \\ &= (ba)N \quad \text{(porque } G \text{ é abeliano)} \\ &= (bN)(aN).\end{aligned}$$

Portanto, G/N é um grupo abeliano. □

Quando um subgrupo H de um grupo G não é normal, às vezes é interessante considerar o maior subgrupo de G no qual H é normal.

Definição 1.2.14. *Seja H um subgrupo de um grupo G. O normalizador de H em G é o conjunto $N_G(H) = \{x \in G \,|\, xHx^{-1} = H\}$.*

Proposição 1.2.15. *O normalizador de H em G é um subgrupo de G.*

Demonstração. Uma vez que

$$eHe^{-1} = H,$$

segue que $e \in N_G(H)$.

Agora, sejam $x, y \in N_G(H)$. Então, $xHx^{-1} = H$ e $yHy^{-1} = H$. Note que,

$$\begin{aligned}(xy)H(xy)^{-1} &= (xy)H(y^{-1}x^{-1}) \\ &= x(yHy^{-1})x^{-1} \\ &= xHx^{-1} \\ &= H.\end{aligned}$$

Logo, $xy \in N_G(H)$.

Por fim, seja $x \in N_G(H)$. Vamos mostrar que $x^{-1} \in N_G(H)$. Observe que,

$$\begin{aligned}xHx^{-1} = H &\Rightarrow (x^{-1}x)H(x^{-1}x) = x^{-1}Hx \\ &\Rightarrow eHe = x^{-1}Hx \\ &\Rightarrow H = x^{-1}Hx.\end{aligned}$$

Logo, $x^{-1} \in N_G(H)$ e, pela Proposição 1.1.8, $N_G(H)$ é um subgrupo de G. □

Os subgrupos de um grupo quociente são caracterizados a seguir.

Lema 1.2.16 (Lema da Correspondência)**.** *Sejam G um grupo e N um subgrupo normal de G. Para todo subgrupo $\overline{H}$ de G/N, existe um subgrupo H de G tal que $\overline{H} = H/N$. Além disso, se $\overline{H} \triangleleft G/N$, então $H \triangleleft G$.*

Demonstração. Inicialmente, notemos que se $\overline{H} = \{N\}$, então $H = N$. Suponhamos que $\overline{H} \neq \{N\}$. Consideremos o conjunto

$$H = \{g \in G \mid gN \in \overline{H}\}.$$

Vamos mostrar que H é um subgrupo de G.

Sejam $g_1, g_2 \in H$, então $g_1N \in \overline{H}$ e $g_2N \in \overline{H}$. Como $\overline{H}$ é um subgrupo de G/N,

$$(g_1N)(g_2N) = (g_1g_2)N \in \overline{H}.$$

Portanto, $g_1g_2 \in H$.

Note que, $e \in H$, pois $eN = N \in \overline{H}$, uma vez que $\overline{H} \leq G/N$.

Agora, seja $g \in H$. Então $gN \in \overline{H}$. Como $\overline{H}$ é um subgrupo de G/N,

$$(gN)^{-1} = g^{-1}N \in \overline{H}.$$

Portanto, $g^{-1} \in H$. Pela Proposição 1.1.8 concluímos que H é um subgrupo de G de modo que $\overline{H} = H/N$.

Agora, suponhamos que $\overline{H} \triangleleft G/N$. Vamos mostrar que $H \triangleleft G$. Para isso, seja $g \in G$ qualquer. Temos que,

$$H \triangleleft G \Leftrightarrow gHg^{-1} \subseteq H \Leftrightarrow (gN)\overline{H}(g^{-1}N) \subseteq \overline{H} \Leftrightarrow \overline{H} \triangleleft G/N.$$

□

1.3 Teorema de Lagrange e consequências

Até o momento, vimos propriedades válidas para os grupos em geral. Contudo, a partir desse momento, nos restringiremos apenas à classe dos grupos finitos, por ser o principal objeto de estudo deste trabalho.

Os grupos finitos são parte essencial da Teoria de Grupos. Dotados de diversas propriedades, eles possuem aplicações em várias áreas da Matemática e em outras ciências, por exemplo na Ciência da Computação e na Criptografia.

O próximo lema será útil para a prova do principal resultado desta seção.

Lema 1.3.1. *Seja H um subgrupo de um grupo finito G. Então, para todo $a \in G$, $|aH| = |H|$.*

Demonstração. Para provar que $|aH| = |H|$ é preciso mostrar que existe uma bijeção entre aH e H. Para isso, considere a função

$$\begin{aligned} f: \ H &\to aH \\ h &\mapsto ah. \end{aligned}$$

Inicialmente, vamos mostrar a injetividade dessa função. Tomemos $h_1, h_2 \in H$ e suponhamos que $f(h_1) = f(h_2)$. Daí,

$$\begin{aligned} f(h_1) = f(h_2) &\Leftrightarrow ah_1 = ah_2 \\ &\Leftrightarrow h_1 = h_2. \end{aligned}$$

Logo, f é injetiva. A sobrejetividade de f é imediata. Portanto, a função f é uma bijeção e, assim, $|aH| = |H|$. □

Como vimos anteriormente, as classes laterais de um subgrupo H de um grupo G são classes de equivalências, portanto, elas particionam o grupo G. Dessa forma, o resultado do lema acima nos permite inferir que as classes laterais de H em G, particionam G em subconjuntos que possuem a mesma cardinalidade de H, ou seja, a ordem de G é um múltiplo da ordem de H.

Essa descoberta levou a um dos principais resultado da Teoria de Grupos Finitos, o Teorema de Langrange. Este teorema merece destaque dentro da Teoria de Grupos Finitos por causa das suas inúmeras aplicações. Uma delas é: esse teorema nos permite identificar as possíveis ordens dos subgrupos e dos elementos de um grupo finito. Além disso, o Teorema de Lagrange tem papel crucial na demonstração de outros resultados importantes da Teoria de Grupos, por exemplo: na prova do Teorema de Cauchy para grupos abelianos, que veremos no Capítulo 2; na prova dos Teoremas de Sylow, que são o cerne de nosso trabalho; entre outros.

Teorema 1.3.2 (Teorema de Lagrange)**.** *Para um grupo finito G, a ordem de qualquer subgrupo de G divide a ordem de G.*

Demonstração. Seja H um subgrupo de G. Sejam $a_1H, a_2H, \cdots, a_rH$ todas as classes laterais à esquerda de H em G. Pelas Proposições 1.2.1 e 1.2.2 essas classes determinam uma partição em G, ou seja, duas a duas elas são disjuntas e

$$G = a_1H \cup \cdots \cup a_rH.$$

Logo,

$$|G| = |a_1H| + |a_2H| + \cdots + |a_rH|.$$

Pelo Lema 1.3.1, $|a_iH| = |H|$ para todo $i = 1, \cdots, r$. Assim

$$\begin{aligned} |G| &= \underbrace{|H| + \cdots + |H|}_{r \text{ vezes}} \\ &= r|H|. \end{aligned}$$

Portanto, $|H|$ divide $|G|$. □

Uma consequência imediata da prova do Teorema de Lagrange é a seguinte.

Corolário 1.3.3. *Seja H um subgrupo de um grupo finito G, então o índice de H em G, $|G : H|$, é igual a $|G|/|H|$.*

Corolário 1.3.4. *Num grupo finito, a ordem de cada elemento do grupo divide a ordem do grupo.*

Demonstração. Seja a um elemento de um grupo finito G. Pela Definição 1.1.14, $|a| = |\langle a \rangle|$. Pelo Teorema 1.3.2, $|\langle a \rangle|$ divide $|G|$, donde concluímos que $|a|$ divide $|G|$. □

Corolário 1.3.5. *Um grupo de ordem prima é cíclico.*

Demonstração. Suponha que G tem ordem prima. Seja $a \in G$ com $a \neq e$. Pelo Teorema de Lagrange, $|\langle a \rangle|$ divide $|G|$. Como $|\langle a \rangle| \neq 1$ e $|G|$ é prima, segue que $|\langle a \rangle| = |G|$. Logo, $G = \langle a \rangle$. □

Observação 1.3.6. *Vale salientar que, a recíproca do Teorema 1.3.2, não é verdade em geral. O contra-exemplo mais conhecido é o grupo alternado A_4, que é um subgrupo do grupo simétrico S_4, formado por todas as permutações pares. O grupo A_4 tem ordem 12, mas não possui subgrupo de ordem 6 (Ver [3, Exemplo 5, p. 149]).*

Os próximos resultados serão úteis futuramente.

Proposição 1.3.7. *Sejam G um grupo e H um subgrupo de G tal que $|G : H| = 2$. Então, H é subgrupo normal de G.*

Demonstração. Como $|G : H| = 2$, H possui duas classes laterais em G, a classe do elemento neutro H e uma classe lateral à esquerda gH para algum $g \in G\backslash H$, visto que as classes laterais particionam o grupo G em conjuntos distintos. Se $g \in H$, temos que

$$gH = H = Hg \Rightarrow gHg^{-1} = H.$$

Se $g \in G\backslash H$, temos a classe lateral à esquerda gH e a classe lateral à direita Hg. Como existe apenas uma outra classe lateral além de H, temos que

$$gH = Hg \Rightarrow gHg^{-1} = H.$$

Portanto, segue pelo Teste de Subgrupo Normal que H é subgrupo normal de G.

□

Exemplo 1.3.8. *O grupo alternado A_n é um subgrupo normal de S_n. De fato, pelo Teorema de Lagrange,*

$$|S_n : A_n| = \frac{|S_n|}{|A_n|} = \frac{n!}{\frac{n!}{2}} = 2.$$

Assim, A_n é um subgrupo de S_n de índice 2 e, pela Proposição 1.3.7, A_n é subgrupo normal de S_n.

Proposição 1.3.9. *Sejam H e K subgrupos de um grupo finito G.*

(i) Se $H \subseteq K \subseteq G$, então $|G : H| = |G : K||K : H|$.

(ii) Então,

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

Demonstração.

(i) Pelo Teorema 1.3.2,

$$|G| = |G : H||H|,\ |G| = |G : K||K| \text{ e } |K| = |K : H||H|$$

Daí,

$$\begin{aligned} |G:H| &= \frac{|G|}{|H|} \\ &= \frac{|G:K||K|}{|H|} \\ &= \frac{|G:K||K:H||H|}{|H|} \\ &= |G:K||K:H|. \end{aligned}$$

(ii) Embora o conjunto HK tenha $|H||K|$ produtos hk, podemos ter $hk = h'k'$, onde $h \neq h'$ e $k \neq k'$.

Para cada $t \in H \cap K$, tem-se $hk = (ht)(t^{-1}k)$, ou seja, cada elemento em HK é representado por pelo menos $|H \cap K|$ produtos em HK. Mas

$$\begin{aligned} hk = h'k' &\Rightarrow (h^{-1}h)(kk'^{-1}) = (h^{-1}h')(k'k'^{-1}) \\ &\Rightarrow kk'^{-1} = h^{-1}h' \end{aligned}$$

implica que $t = kk'^{-1} = h^{-1}h' \in H \cap K$, de modo que $h' = ht$ e $k' = t^{-1}k$. Assim, cada elemento em HK é representado por exatamente $|H \cap K|$ produtos e, portanto

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

□

Proposição 1.3.10. *Sejam H e K subgrupos de um grupo G. Então*

$$|G : H \cap K| \leq |G : H||G : K|,$$

valendo a igualdade se $|G : H|$ e $|G : K|$ são finitos e primos entre si.

Demonstração. Ver [9, Theorem **1.3.11**(ii), p. 14] □

Proposição 1.3.11. *Se G é um grupo e $G/Z(G)$ é cíclico, então G é um grupo abeliano. Em particular, $|G : Z(G)|$ nunca é um número primo.*

Demonstração. Como $G/Z(G)$ é cíclico, existe algum $yZ(G) \in G/Z(G)$ tal que $G/Z(G) = \langle yZ(G)\rangle$, onde $y \in G$.

Sejam $g_1, g_2 \in G$. Para cada $i \in \{1, 2\}$, como $g_iZ(G) \in G/Z(G) = \langle yZ(G)\rangle$, temos que existe $r_i \in \mathbb{Z}^+$ tal que $g_iZ(G) = (yZ(G))^{r_i} = y^{r_i}Z(G)$. Daí, existe $h_i \in Z(G)$ de modo que $g_i = y^{r_i} \cdot h_i,\ i = 1, 2$.

Note que,

$$\begin{aligned} g_1g_2 &= (y^{r_1}h_1)(y^{r_2}h_2) \\ &= y^{r_1}(h_1y^{r_2})h_2 \\ &= y^{r_1}(y^{r_2}h_1)h_2 \\ &= (y^{r_1}y^{r_2})(h_1h_2) \\ &= (y^{r_2}y^{r_1})(h_2h_1) \\ &= y^{r_2}(y^{r_1}h_2)h_1 \\ &= y^{r_2}(h_2y^{r_1})h_1 \\ &= (y^{r_2}h_2)(y^{r_1}h_1) \\ &= g_2g_1. \end{aligned}$$

Portanto, G é um grupo abeliano.

Para a segunda parte da proposição, suponhamos que $|G : Z(G)| = p$, com p primo. Assim, $|G/Z(G)| = p$ e pelo Corolário 1.3.5, $G/Z(G)$ é cíclico. Pelo o que já provamos, segue que G é um grupo abeliano. Consequentemente, $Z(G) = G$, o que implica, $G/Z(G)$ ser o grupo trivial. Portanto, $|G/Z(G)| = 1$, o que é um absurdo, pois 1 não é primo. Logo, $|G : Z(G)|$ não é um número primo. □

1.4 Homomorfismo de Grupos

Introduziremos agora uma família especial de funções, entre dois grupos, que preservam as operações binárias.

Definição 1.4.1. *Sejam $(G, \cdot)$ e $(G', \times)$ dois grupos.*

(i) Uma função $f : G \to G'$ tal que

$$f(a \cdot b) = f(a) \times f(b),$$

para todo $a, b \in G$, é chamada de homomorfismo de grupos ou simplesmente de homomorfismo.

(ii) Um homomorfismo bijetor f de um grupo G para um grupo G' é denominado isomorfismo de grupos. Nesse caso, dizemos que G e G' são isomórficos e denotamos por $G \approx G'$. Além disso, um isomorfismo de um grupo G sobre si mesmo é denominado de automorfismo de G.

Teorema 1.4.2. *Sejam G e G' grupos com identidades e e e', respectivamente, e $f : G \to G'$ um homomorfismo. Então,*

(i) *se f é sobrejetor, então $f(e) = e'$.*

(ii) *a **imagem** de f, $\mathrm{Im}(f) := \{f(g) \mid g \in G\}$, é um subgrupo de G'.*

(iii) *o **núcleo** de f, $\mathrm{Ker}(f) := \{g \in G \mid f(g) = e'\}$, é um subgrupo normal de G.*

(iv) *f é injetora se, e somente se, $\mathrm{Ker}(f) = \{e\}$.*

(v) $\dfrac{G}{\mathrm{Ker}(f)} \approx \mathrm{Im}(f)$.

Demonstração. (i) Seja $b \in G'$. Como f é sobrejetor, existe $a \in G$ tal que $f(a) = b$. Note que,

$$b \times f(e) = f(a) \times f(e) = f(a \cdot e) = f(a) = b$$

e

$$f(e) \times b = f(e) \times f(a) = f(e \cdot a) = f(a) = b.$$

Portanto, segue pela unicidade da identidade de um grupo que $f(e) = e'$.

(ii) Do item (i), temos que $e' \in \mathrm{Im}(f)$. Sejam $\alpha, \beta \in \mathrm{Im}(f)$. Então existem $a, b \in G$ tais que $\alpha = f(a)$ e $\beta = f(b)$. Note que,

$$\alpha \times \beta = f(a) \times f(b) = f(a \cdot b).$$

Portanto, $\alpha \times \beta \in \mathrm{Im}(f)$.

Agora, observe que

$$e' = f(e) = f(a \cdot a^{-1}) = f(a) \times f(a^{-1}) = \alpha \times f(a^{-1})$$

e

$$e' = f(e) = f(a^{-1} \cdot a) = f(a^{-1}) \times f(a) = f(a^{-1}) \times \alpha.$$

Pela Proposição 1.1.3(i), segue que $f(a^{-1}) = \alpha^{-1}$ e, portanto, $\alpha^{-1} \in \mathrm{Im}(f)$. Assim, pelo Teste de Subgrupo, $\mathrm{Im}(f) \leqslant G'$.

(iii) Do item (i), segue que $e' \in \mathrm{Ker}(f)$. Sejam $a, b \in \mathrm{Ker}(f)$. Então, $f(a) = e'$ e $f(b) = e'$. Note que,

$$f(a \cdot b) = f(a) \times f(b) = e' \times e' = e'.$$

Portanto, $a \cdot b \in \mathrm{Ker}(f)$.

Observe que

$$e' = f(e) = f(a \cdot a^{-1}) = f(a) \times f(a^{-1}) = e' \times f(a^{-1}) = f(a^{-1}).$$

Portanto, $a^{-1} \in \text{Ker}(f)$. Logo, pelo Teste de Subgrupo, $\text{Ker}(f) \leqslant G$.

Agora, sejam $a \in \text{Ker}(f)$ e $g \in G$. Então,

$$\begin{aligned} f(g \cdot a \cdot g^{-1}) &= f(g) \times f(a) \times f(g^{-1}) \\ &= f(g) \times e' \times f(g^{-1}) \\ &= f(g) \times f(g^{-1}) \\ &= f(g \cdot g^{-1}) \\ &= f(e) \\ &= e'. \end{aligned}$$

Portanto, pelo Teste de Subgrupo Normal, $\text{Ker}(f) \triangleleft G$.

(iv) ($\Rightarrow$) Assumindo que f é injetora. Se $a \in \text{Ker}(f)$, então $f(a) = e'$. Como $f : G \to \text{Im}(f)$ é sobrejetora, segue pelo item (i), segue que $f(e) = e'$. Daí, $f(a) = f(e)$. De f ser injetora, implica que $a = e$, donde concluímos que $\text{Ker}(f) = \{e\}$.

($\Leftarrow$) Sejam $a, b \in G$. Suponhamos que $f(a) = f(b)$. Então,

$$\begin{aligned} f(a) = f(b) &\Rightarrow f(a^{-1})f(a) = f(a^{-1})f(b) \\ &\Rightarrow f(a^{-1}a) = f(a^{-1}b) \\ &\Rightarrow f(e) = f(a^{-1}b) \\ &\Rightarrow e' = f(a^{-1}b). \end{aligned}$$

Assim, $a^{-1}b \in \text{Ker} = \{e\}$. Daí,

$$\begin{aligned} a^{-1}b = e &\Rightarrow a(a^{-1}b) = ae \\ &\Rightarrow (aa^{-1})b = a \\ &\Rightarrow eb = a \\ &\Rightarrow b = a. \end{aligned}$$

Portanto, f é injetora.

(v) Consideremos a função

$$\begin{aligned} \psi : \ G/\text{Ker}(f) &\to \text{Im}(f) \\ x\text{Ker}(f) &\mapsto f(x). \end{aligned}$$

Vamos mostrar que ψ é bem definida e é um homomorfismo bijetor.

Sejam $x\text{Ker}(f), y\text{Ker}(f) \in G/\text{Ker}(f)$. Assumimos que $x\text{Ker}(f) = y\text{Ker}(f)$. Assim, $y^{-1}x\text{Ker}(f) = \text{Ker}(f)$. Daí,

$$\begin{aligned} y^{-1}x \in \text{Ker}(f) &\Rightarrow f(y^{-1}x) = e' \\ &\Rightarrow f(y^{-1})f(x) = e' \\ &\Rightarrow (f(y)f(y^{-1}))f(x) = f(y)e' \\ &\Rightarrow f(yy^{-1})f(x) = f(y) \\ &\Rightarrow f(e)f(x) = f(y) \\ &\Rightarrow e'f(x) = f(y) \\ &\Rightarrow f(x) = f(y). \end{aligned}$$

Logo, ψ está bem definida.

Agora, sejam $x\text{Ker}(f), y\text{Ker}(f) \in G/\text{Ker}(f)$. Note que

$$\begin{aligned} \psi(x\text{Ker}(f)y\text{Ker}(f)) &= \psi(xy\text{Ker}(f)) \\ &= f(xy) \\ &= f(x)f(y) \\ &= \psi(x\text{Ker}(f))\psi(y\text{Ker}(f)). \end{aligned}$$

Portanto, ψ é um homomorfismo.

Agora, vamos mostrar que ψ é bijetor.

• ψ é injetor.

Para isso, vamos mostrar que $\text{Ker}(\psi) = \{\text{Ker}(f)\}$. É imediato que $\{\text{Ker}(f)\} \subseteq \text{Ker}(\psi)$. Seja $x\text{Ker}(f) \in \text{Ker}(\psi)$. Então,

$$\psi(x\text{Ker}(f)) = e' = f(x).$$

Logo, $x \in \text{Ker}(f)$. Portanto, $x\text{Ker}(f) = \text{Ker}(f)$ e, assim, $\text{Ker}(\psi) \subseteq \{\text{Ker}(f)\}$. Assim, $\text{Ker}(\psi) = \{\text{Ker}(f)\}$, e segue do item (iv) que ψ é injetora.

• ψ é sobrejetor.

A sobrejetividade é imediata.

Logo, ψ é um homomorfismo bijetor e, portanto, é um isomorfismo.

□

O item (v) do Teorema 1.4.2 é conhecido como o Primeiro Teorema de Isomorfismo.

Corolário 1.4.3. *Sejam G um grupo finito e $f : G \to G'$ um homomorfismo de grupos. Se $H \leqslant G$, então $|f(H)|$ divide $|H|$.*

Demonstração. Consideremos o homomorfismo restrito a H:

$$\begin{aligned} f|_H : \ H &\to f(H) \\ h &\mapsto f(h). \end{aligned}$$

Pelo item (v) do Teorema 1.4.2,

$$\frac{H}{\mathrm{Ker}(f|_H)} \approx f(H),$$

de modo que

$$\left|\frac{H}{\mathrm{Ker}(f|_H)}\right| = |f(H)|.$$

Pelo Teorema de Lagrange,

$$\left|\frac{H}{\mathrm{Ker}(f|_H)}\right| = \frac{|H|}{|\mathrm{Ker}(f|_H)|} = |f(H)| \ \Rightarrow \ |f(H)||\mathrm{Ker}(f|_H)| = |H|.$$

Portanto, $|f(H)|$ divide $|H|$.

□

Teorema 1.4.4 (Segundo Teorema de Isomorfismo)**.** *Sejam H e N subgrupos de um grupo G e $N \triangleleft G$. Então,*

$$\frac{H}{H \cap N} \approx \frac{HN}{N}.$$

Demonstração. Como $N \triangleleft G$, segue pelo Lema 1.2.8 que $HN \leqslant G$, além disso, $N \triangleleft G$ implica que $N \triangleleft HN$ e, portanto, podemos considerar o grupo quociente HN/N. Consideremos a função

$$\begin{aligned} \varphi : \ H &\to HN/N \\ h &\mapsto \ hN. \end{aligned}$$

Sejam $x, y \in H$. Note que,

$$\varphi(xy) = xyN = xNyN = \varphi(x)\varphi(y).$$

Portanto, φ é um homomorfismo. Além disso, observe que dado $xN \in HN/N$, existe $x \in H$ tal que $\varphi(x) = xN$ e, portanto, φ é sobrejetor. Agora, vamos calcular o $\mathrm{Ker}(\varphi)$:

$$\begin{aligned} \mathrm{Ker}(\varphi) &= \{h \in H \,|\, \varphi(h) = N\} \\ &= \{h \in H \,|\, hN = N\} \\ &= \{h \in H \,|\, h \in N\}. \end{aligned}$$

Assim, $\mathrm{Ker}(\varphi) = H \cap N$. Logo, pelo Teorema 1.4.2(v),

$$\frac{H}{H \cap N} \approx \frac{HN}{N}.$$

□

Proposição 1.4.5 (Terceiro Teorema de Isomorfismo)**.** *Sejam $K < H < G$ com $K \triangleleft G$ e $H \triangleleft G$. Então,*

$$\frac{G/K}{H/K} \approx \frac{G}{H}.$$

Demonstração. Considere o homomorfismo

$$\begin{aligned} \varphi: \ G/K &\to G/H \\ gK &\mapsto gH. \end{aligned}$$

A função φ é bem definida. De fato, $gK = g'K$ implica que $g = g'k$ para algum $k \in K$. Daí,

$$\varphi(gK) = gH = g'kH = g'H = \varphi(g'K).$$

Claramente, φ é sobrejetor. Note que,

$$\begin{aligned} \mathrm{Ker}(\varphi) &= \{gK \in G/K \,|\, \varphi(gK) = H\} \\ &= \{gK \in G/K \,|\, gH = H\} \\ &= \{gK \in G/K \,|\, g \in H\}. \end{aligned}$$

Assim, $\mathrm{Ker}(\varphi) = H/K$. Logo, pelo Teorema 1.4.2(v),

$$\frac{G/K}{H/K} \approx \frac{G}{H}.$$

□

Lema 1.4.6. *Sejam $H, K, N \leqslant G$. com $K, N \triangleleft G$. Se $N \leqslant K$, então*

$$\frac{H \cap K}{H \cap N} \ \text{ é isomorfo a um subgrupo de } \ \frac{K}{N}.$$

Demonstração. Considere a função

$$\begin{aligned} \varphi: \ H \cap K &\to K/N \\ x &\mapsto xN. \end{aligned}$$

É imediato que φ é um homomorfismo de grupos. Note que,

$$\begin{aligned}\mathrm{Ker}(\varphi) &= \{a \in H \cap K | \, \varphi(a) = N\} \\ &= \{a \in H \cap K | \, aN = N\} \\ &= \{a \in H \cap K | \, a \in N\}.\end{aligned}$$

Assim, $\mathrm{Ker}(\varphi) = H \cap N$. Logo, pelo item (v) Teorema 1.4.2,

$$\frac{H \cap K}{H \cap N} \approx \mathrm{Im}(\varphi).$$

Pelo item (ii) do Teorema 1.4.2, $\mathrm{Im}(\varphi) \leqslant K/N$.

□

A próxima definição é de suma importância no decorrer desse trabalho.

Definição 1.4.7. *Sejam H e K subgrupos de um grupo G. Dizemos que H e K são conjugados em G se existe um elemento $g \in G$ tal que $H = gKg^{-1}$.*

Lema 1.4.8. *Seja $f : G \to G'$ um homomorfismo sobrejetor de grupos.*

(i) Se $H \leqslant G'$, então $f^{-1}(H) := \{g \in G | f(g) \in H\}$ é subgrupo de G.

(ii) Se H e K são subgrupos conjugados de G', então a $f^{-1}(H)$ e $f^{-1}(K)$ são subgrupos conjugados de G.

Demonstração. Prova do item (i): Claramente, $e \in f^{-1}(H)$. Sejam $g_1, g_2 \in f^{-1}(H)$. Então $f(g_1), f(g_2) \in H$. Note que,

$$f(g_1)f(g_2) = f(g_1g_2) \in H.$$

Portanto, $g_1g_2 \in f^{-1}(H)$.

Agora, pela prova do Teorema 1.4.2 (ii),

$$f(g_1^{-1}) = f(g_1)^{-1} \in H.$$

Portanto, $g_1^{-1} \in f^{-1}(H)$. Assim, pelo Teste de Subgrupo, $f^{-1}(H) \leqslant G$.

Prova do item (ii): Como H e K são conjugados em G', existe $a \in G'$ tal que $aHa^{-1} = K$. Uma vez que f é sobrejetora, existe $g \in G$ tal que $f(g) = a$. Vamos mostrar que $gf^{-1}(H)g^{-1} = f^{-1}(K)$.

Seja $x \in gf^{-1}(H)g^{-1}$. Então, $x = gug^{-1}$ para algum $u \in f^{-1}(H)$. Note que,

$$f(x) = f(gug^{-1}) = f(g)f(u)f(g)^{-1} = af(u)a^{-1} \in K,$$

pois $f(u) \in H$. Logo, $x \in f^{-1}(K)$ e, portanto, $gf^{-1}(H)g^{-1} \subseteq f^{-1}(K)$.

Por outro lado, seja $x \in f^{-1}(K)$. Note que,

$$f(g^{-1}xg) = f(g)^{-1}f(x)f(g) = a^{-1}f(x)a \in a^{-1}Ka = a^{-1}(aHa^{-1})a = H.$$

Daí, $g^{-1}xg \in f^{-1}(H)$ e, assim, $x \in gf^{-1}(H)g^{-1}$. Logo,

$$f^{-1}(K) \subseteq gf^{-1}(H)g^{-1}.$$

Portanto, $gf^{-1}(H)g^{-1} = f^{-1}(K)$, donde concluímos que $f^{-1}(H)$ e $f^{-1}(K)$ são subgrupos conjugados de G. □

As duas proposições seguintes nos diz quando um grupo é isomorfo ao produto direto de grupos.

Proposição 1.4.9. *Sejam $G, G_1, \ldots, G_n$ grupos. Então o grupo é isomorfo ao grupo $G \times \cdots \times G_n$ se, somente se, o grupo G possui subgrupos $H_1 \approx G_1, \ldots, H_n \approx G_n$ tais que:*

(i) $G = H_1 \ldots H_n$.

(ii) $H_i \triangleleft G$, *para todo* $i = 1, \ldots, n$.

(iii) $H_i \cap (H_1 \ldots H_{i-1}H_{i+1} \ldots H_n) = \{e\}$, *para todo* $i = 1, \ldots, n$.

Demonstração. Ver [4, Teorema V.8.1 , p. 197]. □

Proposição 1.4.10. *Sejam G um grupo e $H_1, \ldots, H_n$ subgrupos de G. Então os itens $(i), (ii), (iii)$ da Proposição 1.4.9 são satisfeitos se, e somente se, os itens seguintes são satisfeitos:*

(i) Para cada $g \in G$, existem elementos unicamente determinados $x_1 \in H_1, \ldots, x_n \in H_n$ tais que $g = x_1 \ldots x_n$.

(ii) Para cada $i \neq j$, temos $xy = yx$, para todo $x \in H_i$ e $y \in H_j$.

Demonstração. Ver [4, Lema V.8.2 , p. 197-199]. □

Definição 1.4.11. *Um subgrupo H de um grupo G diz-se um subgrupo característico se $\varphi(H) = H$ para todo automorfismo $\varphi : G \to G$. Para indicar que H é um subgrupo característico de G escreveremos $H \operatorname{char} G$.*

Proposição 1.4.12. *O centro $Z(G)$ de um grupo G é um subgrupo característico de G.*

Demonstração. Considere o automorfismo $\varphi : G \to G$. Seja $z \in Z(G)$. Então,

$$zg = gz \quad \text{para todo} \ \ g \in G. \tag{1.2}$$

Aplicando o automorfismo φ nesta igualdade, temos que

$$\varphi(z)\varphi(g) = \varphi(zg) = \varphi(gz) = \varphi(g)\varphi(z).$$

Logo, $\varphi(z) \in Z(G)$, ou seja, $\varphi(Z(G)) \subseteq Z(G)$.

Por outro lado, como φ é bijetor, existe $\varphi^{-1}(z) = x \in G$, de modo que $z = \varphi(x)$. Além disso, cada $g \in G$ pode ser escrito como $g = \varphi(y)$, com $y \in G$. Substituindo esses valores na equação (1.2), obtemos

$$\varphi(xy) = \varphi(x)\varphi(y) = \varphi(y)\varphi(x) = \varphi(yx).$$

De φ ser injetora, concluímos que

$$xy = yx \quad \text{para todo } y \in G.$$

Logo, $x \in Z(G)$, o que implica $z = \varphi(Z(G))$ e, assim, $Z(G) \subseteq \varphi(Z(G))$.

Portanto, $\varphi(Z(G)) = Z(G)$, donde concluímos que o centro $Z(G)$ de um grupo G é um subgrupo característico de G. □

Em geral não vale a transitividade para subgrupos normais. Entretanto, vale o seguinte:

Proposição 1.4.13. *Sejam H, K subgrupos de um grupo G. Se $H \operatorname{char} K$ e $K \lhd G$, então $H \lhd G$.*

Demonstração. Para cada $g \in G$, é elementar verificar que a aplicação $\varphi_g : G \to G$ definida por $\varphi_g(x) = gxg^{-1}$ é um automorfismo de G. Como $K \lhd G$, temos que $\varphi_g(K) = K$ para cada $g \in G$. Logo, a restrição $(\varphi_g)_{|_K}$ de φ_g a K é um automorfismo de K. Uma vez que $H \operatorname{char} K$, segue que $(\varphi_g)_{|_K}(H) = H$ para cada $g \in G$. Portanto, $H \lhd G$. □

1.5 Ação de Grupos

Definição 1.5.1. *Sejam X um conjunto não vazio e G um grupo. Uma ação de G sobre X é uma função $\cdot : G \times X \to X$, denotada por $\cdot(g, x) = g \cdot x$, tal que*

(i) se e é a identidade de G, então $e \cdot x = x$, para cada $x \in X$,

(ii) $(g_1 g_2) \cdot x = g_1 \cdot (g_2 \cdot x)$, para todos $x \in X$ e $g_1, g_2 \in G$.

Exemplo 1.5.2. *Existe uma ação natural de um grupo $(G, *)$ nele mesmo, a saber:*

$$\begin{aligned} \cdot : \ G \times G &\to G \\ (g, x) &\mapsto g \cdot x := g * x. \end{aligned}$$

Exemplo 1.5.3. *Sejam V um espaço vetorial sobre o corpo K . Considerando o grupo multiplicativo $K^* := K - \{0\}$, temos que existe uma ação de K^* sobre V, dada por:*

$$\begin{array}{rccc} \cdot : & K^* \times V & \to & V \\ & (\alpha, v) & \mapsto & \alpha \cdot v := \alpha v. \end{array}$$

Se X é qualquer conjunto não vazio, denotaremos por S_X o grupo formado por todas as permutações de X.

Proposição 1.5.4. *Seja G um grupo que age sobre um conjunto não vazio X. Para cada $g \in G$, a função $\varphi_g : X \to X$ definida por $\varphi_g(x) = g \cdot x$ para $x \in X$ é uma permutação. Além disso, a função $\varphi : G \to S_X$ definida por $\varphi(g) = \varphi_g$ é um homomorfismo de grupos.*

Demonstração. Para mostrar que φ_g é uma permutação de X, devemos mostrar que φ_g é uma bijeção.

- φ_g é injetora.

  Sejam $x_1, x_2 \in X$. Suponhamos que $\varphi_g(x_1) = \varphi_g(x_2)$. Daí,

$$\begin{array}{rcl} g \cdot x_1 = g \cdot x_2 & \Leftrightarrow & g^{-1} \cdot (g \cdot x_1) = g^{-1} \cdot (g \cdot x_2) \\ & \Leftrightarrow & (g^{-1}g) \cdot x_1 = (g^{-1}g) \cdot x_2 \\ & \Leftrightarrow & e \cdot x_1 = e \cdot x_2 \\ & \Leftrightarrow & x_1 = x_2. \end{array}$$

  Portanto, φ_g é injetora.

- φ_g é sobrejetora.

  Seja $x \in X$. Tomemos $g^{-1} \in G$. Note que,

$$\begin{array}{rcl} \varphi_g(g^{-1}x) & = & g \cdot (g^{-1} \cdot x) \\ & = & (gg^{-1}) \cdot x \\ & = & e \cdot x \\ & = & x. \end{array}$$

  Logo, φ_g é sobrejetora.

  Assim, φ_g é uma bijeção e, portanto, uma permutação.

Agora vamos mostrar que $\varphi : G \to S_X$ definida por $\varphi(g) = \varphi_g$ é um homomorfismo. Para isso, devemos mostrar que $\varphi(g_1g_2) = \varphi(g_1)\varphi(g_2)$ para todos $g_1, g_2 \in G$. Note que,

$$\begin{aligned}
\varphi(g_1g_2)(x) &= \varphi_{g_1g_2}(x) \\
&= (g_1g_2) \cdot x \\
&= g_1 \cdot (g_2 \cdot x) \\
&= g_1 \cdot (\varphi_{g_2}(x)) \\
&= \varphi_{g_1}(\varphi_{g_2}(x)) \\
&= (\varphi_{g_1} \circ \varphi_{g_2}(x)) \\
&= (\varphi(g_1)\varphi(g_2))(x),
\end{aligned}$$

para $x \in X$. Logo, φ é um homomorfismo. □

Definição 1.5.5. *Seja G um grupo que age em um conjunto não vazio X. Para todo $x \in X$, o conjunto $Stab_G(x) = \{g \in G \mid g \cdot x = x\}$ é denominado de estabilizador de x em G.*

Proposição 1.5.6. *Seja G um grupo que age sobre um conjunto não vazio X. O conjunto $Stab_G(x)$ é um subgrupo de G para todo $x \in X$.*

Demonstração. Pelo item (i) da definição de ação de grupos, o elemento identidade de G, e, está em $Stab_G(x)$. Agora, sejam $x \in X$ e $g_1, g_2 \in Stab_G(x)$. Assim, $g_1 \cdot x = x$ e $g_2 \cdot x = x$. Consequentemente,

$$\begin{aligned}
(g_1g_2)x &= g_1 \cdot (g_2 \cdot x) \\
&= g_1 \cdot x \\
&= x.
\end{aligned}$$

Logo, $g_1g_2 \in Stab_G(x)$ e, portanto, $Stab_G(x)$ é fechado para a operação.

Agora, seja $g \in Stab_G(x)$. Daí,

$$\begin{aligned}
x &= e \cdot x \\
&= (g^{-1}g) \cdot x \\
&= g^{-1} \cdot (g \cdot x) \\
&= g^{-1} \cdot x.
\end{aligned}$$

Assim, $g^{-1} \in Stab_G(x)$. Portanto pela Proposição 1.1.8, $Stab_G(x)$ é um subgrupo de G. □

Seja G um grupo que age em um conjunto não vazio X. Definimos a relação $\sim$ em X

da seguinte maneira: sejam $x_1, x_2 \in X$,

$$x_1 \sim x_2 \text{ se, e somente se, existe } g \in G \text{ tal que } g \cdot x_1 = x_2. \tag{1.3}$$

Proposição 1.5.7. *A relação $\sim$ definida em (1.3) é uma relação de equivalência em X.*

Demonstração. Vamos mostrar que a relação $\sim$ é reflexiva, simétrica e transitiva.

- Sejam $x \in X$ e $e \in G$ o elemento identidade. Então, $e \cdot x = x$. Logo, $x \sim x$ e $\sim$ é reflexiva.
- Sejam $x_1, x_2 \in X$. Se $x_1 \sim x_2$, então $g \cdot x_1 = x_2$ para algum $g \in G$. Note que,

$$\begin{aligned} x_2 = g \cdot x_1 &\Rightarrow g^{-1} \cdot x_2 = g^{-1} \cdot (g \cdot x_1) \\ &\Rightarrow g^{-1} \cdot x_2 = (g^{-1}g) \cdot x_1 \\ &\Rightarrow g^{-1} \cdot x_2 = e \cdot x_1 \\ &\Rightarrow g^{-1} \cdot x_2 = x_1. \end{aligned}$$

  Logo, $x_2 \sim x_1$ e, assim, $\sim$ é simétrica.

- Sejam $x_1, x_2, x_3 \in X$. Se $x_1 \sim x_2$ e $x_2 \sim x_3$, então $g_1 \cdot x_1 = x_2$ e $g_2 \cdot x_2 = x_3$, para alguns $g_1, g_2 \in G$. Note que,

$$\begin{aligned} g_1 \cdot x_1 = x_2 &\Rightarrow g_2 \cdot (g_1 \cdot x_1) = g_2 \cdot x_2 \\ &\Rightarrow (g_2 g_1) \cdot x_1 = x_3. \end{aligned}$$

  Logo, $x_1 \sim x_3$ e, portanto, $\sim$ é transitiva.

Segue dos pontos anteriores que $\sim$ é uma relação de equivalência. □

A classe de equivalência que contém o elemento $x \in X$, será **chamada de órbita de** x e a denotaremos por

$$Orb_G(x) = \{g \cdot x \mid g \in G\}.$$

O próximo teorema será útil nas provas dos Teoremas de Sylow.

Teorema 1.5.8 (Teorema da órbita e do estabilizador)**.** *Seja G um grupo que age em um conjunto não vazio X. Então, $|Orb_G(x)| = |G : Stab_G(x)|$. Se $|G|$ é finito, então $|Orb_G(x)|$ é um divisor de $|G|$.*

Demonstração. Para provarmos esse teorema, devemos exibir uma bijeção entre o conjunto $G/Stab_G(x)$ e o conjunto $Orb_G(x)$. Assim, Consideremos a função

$$\begin{aligned} \psi : \ G/Stab_G(x) &\to Orb_G(x) \\ gStab_G(x) &\mapsto g \cdot x. \end{aligned}$$

Primeiramente, provaremos que ψ está bem definida. Sejam

$$gStab_G(x), hStab_G(x) \in G/Stab_G(x)$$

tais que $gStab_G(x) = hStab_G(x)$. Então, $g \in hStab_G(x)$, ou seja, existe $j \in Stab_G(x)$ tal que $g = hj$. Como j fixa o elemento x, temos que

$$\begin{aligned} \psi(gStab_G(x)) &= g \cdot x \\ &= (hj) \cdot x \\ &= h(j \cdot x) \\ &= h \cdot x \\ &= \psi(hStab_G(x)). \end{aligned}$$

Portanto, ψ está bem definida.

Mostraremos agora que ψ é injetora. Para isso, sejam

$$gStab_G(x), hStab_G(x) \in G/Stab_G(x)$$

tais que $\psi(gStab_G(x)) = \psi(hStab_G(x))$, ou seja, $g \cdot x = h \cdot x$. Daí

$$\begin{aligned} (h^{-1}g) \cdot x &= (h^{-1}h) \cdot x \\ &= e \cdot x \\ &= x. \end{aligned}$$

Logo, $h^{-1}g \in Stab_G(x)$, o que implica $gStab_G(x) = hStab_G(x)$. Portanto, ψ é injetora.

Mostraremos agora que ψ é sobrejetora. Para isso, seja $j \in Orb_G(x)$. Então $g \cdot x = j$ para algum $g \in G$. Claramente existe $gStab_G(x) \in G/Stab_G(x)$ tal que

$$\psi(gStab_G(x)) = g \cdot x = j.$$

Logo, ψ é sobrejetora. Portanto, ψ é uma bijeção.

Agora vamos provar a segunda parte do teorema, ou seja, se $|G|$ é finito, então $|Orb_G(x)|$ é um divisor de $|G|$. Pelo Teorema de Lagrange, tem-se

$$|G| = |G : Stab_G(x)||Stab_G(x)|.$$

Daí, segue da primeira parte do teorema que

$$|G| = |Orb_G(x)||Stab_G(x)|.$$

Assim, concluimos que $|Orb_G(x)|$ é um divisor de $|G|$.

□

Capítulo

2

Os Teoremas de Sylow

Neste capítulo, apresentaremos os três Teoremas de Sylow, resultados considerados centrais na Teoria dos Grupos Finitos. Iniciaremos o capítulo com uma seção dedicada a introdução dos p-grupos finitos. Posteriormente, enunciamos e provamos os três Teoremas de Sylow e finalizamos o capítulo com algumas aplicações destes teoremas.

2.1 p-Grupos Finitos

Definição 2.1.1. *Seja p um número primo. Um grupo finito G é chamado de p-grupo se sua ordem for uma potência de p.*

Pelo Teorema de Lagrange vemos que a ordem de cada elemento de um p-grupo finito é também uma potência de p.

Exemplo 2.1.2. *$\mathbb{Z}/8\mathbb{Z}, (\mathbb{Z}/4\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$ e $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$ são 2-grupos de ordem $8 = 2^3$.*

A seguinte proposição é um resultado fundamental sobre p-grupos.

Proposição 2.1.3. *O centro de um p-grupo finito não trivial, tem pelo menos p elementos.*

Demonstração. Considere a equação de classes

$$|G| = |Z(G)| + \sum_{a \notin Z(G)} |G : C(a)|.$$

Para elementos $a \notin Z(G)$, temos $|G : C(a)| > 1$. Pelo Teorema de Lagrange, $|G : C(a)|$ divide $|G|$, ou seja, divide p^n; assim, $|G : C(a)|$ é um múltiplo de p. De $\sum_{a \notin Z(G)} |G : C(a)|$ ser múltiplo de p, segue que

$$|Z(G)| = |G| - \sum_{a \notin Z(G)} |G : C(a)|$$

é um múltiplo de p. Uma vez que $e \in Z(G)$, temos que $|Z(G)| \neq 0$. Portanto, $Z(G)$ tem pelo menos p elementos.

□

Proposição 2.1.4. *Se G é um grupo finito de ordem p^2, então G é abeliano.*

Demonstração. Suponhamos que $|G| = p^2$. Uma vez que $Z(G)$ tem pelo menos p elementos, temos dois casos a considerar:

(i) $|Z(G)| = p$;

(ii) $|Z(G)| = p^2$.

No caso (i), temos $|G/Z(G)| = p$, de modo que $G/Z(G)$ é cíclico. Pela Proposição 1.3.11 segue que G é abeliano. Logo $G = Z(G)$, e, portanto, $G/Z(G)$ é trivial, o que é uma contradição, pois assumimos que $|G/Z(G)| = p$.

No caso (ii), como $Z(G)$ é subgrupo de G e $|G| = p^2 = |Z(G)|$, então $G = Z(G)$. Logo, G é abeliano. □

O próximo teorema nos dá um caso em que vale a recíproca do Teorema de Lagrange.

Teorema 2.1.5 (Teorema de Cauchy para grupos abelianos)**.** *Sejam G um grupo abeliano finito e p um número primo que divide a ordem de G. Então G tem um elemento de ordem p.*

Demonstração. Vamos prosseguir por indução sobre a ordem de G.

Se $|G| = 2$, a afirmação é verdadeira, pois G será cíclico e seu gerador terá ordem 2.

Assumimos que a afirmação é válida para todos os grupos abelianos finitos com ordem menor que a ordem de G e maior que 2. Vamos provar que a afirmação também vale para G. Certamente G possui elementos de ordem prima, pois se $x \in G$ tal que $|x| = m$ e $m = qn$, onde q é um primo, então $|x^n| = q$. Se $q = p$, terminamos. Suponhamos, então, que $q \neq p$. Consideremos o subgrupo $\langle x^n \rangle$ de G gerado por x^n. Como todo subgrupo de um grupo abeliano é normal, podemos construir o grupo quociente $\overline{G} = G/\langle x^n \rangle$. Assim, $\overline{G}$ é abeliano e p divide $|\overline{G}|$, uma vez que $|\overline{G}| = |G|/q$. Por hipótese de indução, existe $y\langle x^n \rangle \in \overline{G}$ tal que $|y\langle x^n \rangle| = p$. Desse modo, temos que

$$(y\langle x^n \rangle)^p = y^p \langle x^n \rangle = \langle x^n \rangle,$$

o que implica que $y^p \in \langle x^n \rangle$. Se $y^p = e_G$, terminamos. Caso contrário, $|y^p| = q$ e, assim, $|y^q| = p$. □

2.2 Os Teorema de Sylow

Como visto na Obseração 1.3.6 da Seção 1.3 deste trabalho, a recíproca do Teorema de Lagrange é falsa, ou seja, se G é um grupo de ordem m e n divide m, G não precisa ter um subgrupo de ordem n. O próximo teorema é uma recíproca parcial do Teorema de Lagrange. Ele foi provado pela primeira vez pelo matemático norueguês Ludwig Sylow $(1832 - 1918)$.

Teorema 2.2.1 (Primeiro Teorema de Sylow)**.** *Sejam G um grupo finito, p um número primo e k um inteiro não negativo. Se p^k divide $|G|$, então G tem pelo menos um subgrupo de ordem p^k.*

Demonstração. Inicialmente, notemos que a afirmação vale trivialmente se a ordem de G é igual a p^k. Por isso, para o que segue, assumiremos que $|G| \neq p^k$.

A prova do caso geral será por indução sobre $|G|$. Se $|G| = 1$, note que o grupo trivial é um subgrupo de ordem $p^0 = 1$. Logo, vale a base da indução.

Suponhamos agora que a afirmação vale para todos os grupos que possuem ordem menor que $|G|$. Provaremos que o mesmo vale para o grupo G. Observe que, para concluir a prova é suficiente provar que G possui um subgrupo próprio H tal que p^k divide $|H|$. De fato, se H é subgrupo próprio de G, então $|H|$ é estritamente menor que $|G|$, de modo que, pela nossa afirmação, H tem um subgrupo próprio de ordem p^k que, consequentemente, também será subgrupo próprio de G.

Provaremos agora que G possui um subgrupo próprio H de modo que p^k divide $|H|$. Para isso, procedemos por contradição, ou seja, suponhamos que p^k não divide a ordem de nenhum subgrupo próprio de G. O Teorema de Lagrange 1.3.2 aplicado para o centralizador $C(a)$ de um elemento a de G, nos dá que

$$|G| = |G : C(a)||C(a)|. \tag{2.1}$$

Pelas nossas hipóteses,

$$\begin{cases} p^k \text{ divide } |G| \\ p^k \text{ não divide } |C(a)|. \end{cases}$$

Logo, da relação (2.1) concluímos que p^k divide $|G : C(a)|$ e, consequentemente, p divide $|G : C(a)|$. Agora, da equação de classes

$$|G| = |Z(G)| + \sum_{a \notin Z(G)} |G : C(a)|, \tag{2.2}$$

concluímos que p divide $|Z(G)|$, uma vez que p divide $|G|$ e p divide $|G : C(a)|$ para cada $a \in G$. Pelo Teorema de Cauchy 2.1.5, existe $x \in Z(G)$ tal que $|\langle x \rangle| = p$. Como x comuta

com todos os elementos de G, temos que

$$\begin{aligned} gx^tg^{-1} &= g\underbrace{xx\cdots xx}_{t\,\text{vezes}}g^{-1} \\ &= xgx\cdots xxg^{-1} \\ &= xxg\cdots xxg^{-1} \\ &= xxx\cdots gxg^{-1} \\ &= xxx\cdots xgg^{-1} \\ &= xxx\cdots xe_G \\ &= x^t, \end{aligned}$$

para todo $g \in G$. Isso mostra que $\langle x\rangle \trianglelefteq G$. Logo, podemos considerar o grupo quociente $G/\langle x\rangle$. Note que p^{k-1} divide $|G/\langle x\rangle|$. Como $|G/\langle x\rangle| < |G|$, segue pela hipótese de indução que $G/\langle x\rangle$ tem pelo menos um subgrupo L de ordem p^{k-1}. Pelo Lema 1.2.16, existe um subgrupo H de G tal que $L = H/\langle x\rangle$. Pelo Teorema de Lagrange 1.3.2,

$$\begin{aligned} |H| &= |H : \langle x\rangle||\langle x\rangle| \\ &= p^{k-1}\cdot p \\ &= p^k. \end{aligned}$$

Uma vez que G não é um p-grupo, concluímos que H é um subgrupo próprio de G de ordem p^k. Dessa forma, dado um grupo finito G, um número p primo e k um inteiro não negativo, se p^k dividir $|G|$, então G terá pelo menos um subgrupo de ordem p^k. □

O Teorema 2.2.1 motiva a seguinte definição:

Definição 2.2.2. *Sejam G um grupo finito, p um número primo e k um inteiro não negativo. Se p^k divide $|G|$ e p^{k+1} não divide $|G|$, então qualquer subgrupo de G de ordem p^k será chamado de p-subgrupo de Sylow.*

O próximo lema será útil na prova do segundo Teorema de Sylow.

Lema 2.2.3. *Sejam G um grupo finito e K um p-subgrupo de Sylow de G. Então, os únicos elementos de $N_G(K)$ cuja as ordens são iguais a uma potência de p, são os elementos de K.*

Demonstração. Suponhamos que exista $x \in N_G(K)$ tal que $x \notin K$ e cuja a ordem é igual a uma potência de p. Consideremos $\langle x\rangle \leqslant N_G(K)$. Como $K \triangleleft N_G(K)$, temos que $K\langle x\rangle \leqslant N_G(K)$. Em particular, $K\langle x\rangle \leqslant G$. Pela Proposição 1.3.9 (ii)

$$|K\langle x\rangle| = \frac{|K||\langle x\rangle|}{|K \cap \langle x\rangle|}.$$

Como $K \cap \langle x \rangle \leqslant \langle x \rangle$ e $x \notin K$ implica que $|K \cap \langle x \rangle| < |\langle x \rangle|$. Desse modo, $|K\langle x \rangle| > |K|$ e $|K\langle x \rangle|$ é uma potência de p. Logo, temos uma contradição com o fato de K ser um p-subgrupo de Sylow de G. Portanto, não existe $x \in N_G(K)$ com $x \notin K$ tal que a ordem x é igual a uma potência de p. □

Teorema 2.2.4 (Segundo Teorema de Sylow)**.** *Se H é um subgrupo de um grupo finito G com ordem igual a uma potência de um primo p, então H está contido em algum p-subgrupo de Sylow de G.*

Demonstração. Seja K um p-subgrupo de Sylow de G e seja $C = \{K_1, K_2, \cdots, K_n\}$ o conjunto formado por todos os conjugados de K em G. Como a conjugação em G define um automorfismo de G, temos que cada elemento de C é um p-subgrupo de Sylow de G. Denotemos por S_c o conjunto de todas permutações de C. Agora, consideremos a aplicação $T : G \to S_c$ definida por

$$\begin{array}{rcl} T: \ G & \to & S_C \\ g & \mapsto & \varphi_g: \ C \to C \\ & & \qquad K_i \mapsto gK_ig^{-1} \end{array}$$

Afirmamos que T é um homomorfismo de grupos. De fato, para todos $g, h \in G$ temos que

$$\begin{aligned} \varphi_{gh}(K_i) &= (gh)K_i(gh)^{-1} \\ &= g(hK_ih^{-1})g^{-1} \\ &= g\varphi_h(K_i)g^{-1} \\ &= \varphi_g(\varphi_h(K_i)) \\ &= (\varphi_g \circ \varphi_h)(K_i). \end{aligned}$$

Assim,

$$T(gh) = \varphi_{gh} = \varphi_g \circ \varphi_h = T(g) \circ T(h).$$

Logo, $T : G \to S_C$ é um homomorfismo de grupos. Como $|H|$ é uma potência de p, segue pelo Corolário 1.4.3, que $|T(H)|$ também é. Agora, pelo Teorema da órbita e do estabilizador 1.5.8,

$$|T(H)| = |orb_{T(H)}(K_i)||stab_{T(H)}(K_i)|.$$

Daí, $|orb_{T(H)}(K_i)|$ divide $|T(H)|$ para cada $i \in \{1, \cdots, n\}$. Consequentemente, $|orb_{T(H)}(K_i)|$ é uma potência de p.

Para concluir a prova é suficiente mostrar que $|orb_{T(H)}(K_i)| = 1$ para algum $i \in \{1, \cdots, n\}$. Com efeito, $|orb_{T(H)}(K_i)| = 1$ se, e somente se,

$$\varphi_h(K_i) = hK_ih^{-1} = K_i \ \text{ para todo } \ h \in H,$$

ou seja, $|orb_{T(H)}(K_i)| = 1$ se, e somente se, $H \leq N_G(K_i)$. Pelo Lema 2.2.3, $|orb_{T(H)}(K_i)| = 1$ se, e semente se, $H \leq K_i$. Portanto, estará provado o Teorema.

Vamos mostrar que existe $i \in \{1, \cdots, n\}$ tal que $|orb_{T(H)}(K_i)| = 1$. Uma vez que, $|C| = |G : N_G(K_i)|$ e

$$|G : K_i| = |G : N_G(K_i)||N_G(K_i) : K_i|,$$

não é divisível por p, pelo fato de K_i ser um p-subgrupo de Sylow, concluímos que $|C|$ também não é divisível por p. Como as órbitas produzidas da ação de $T(H)$ sobre C geram uma partição do conjunto C, temos que

$$|C| = |orb_{T(H)}(K_1)| + |orb_{T(H)}(K_2)| + \cdots + |orb_{T(H)}(K_n)|.$$

De $|orb_{T(H)}(K_i)|$ ser uma potência de p e p não dividir $|C|$, concluímos que deve existir $i_0 \in \{1, \cdots, n\}$ de modo que $|orb_{T(H)}(K_{i_0})| = 1$, como queríamos. □

Corolário 2.2.5. *Se P é o único p-subgrupo de Sylow de um grupo finito G, então P é um subgrupo normal de G.*

Demonstração. Do teorema 2.2.4 segue que gPg^{-1} também é um p-subgrupo de Sylow de G para todo $g \in G$. Por hipótese, P é o único p-subgrupo de Sylow de G, logo

$$gPg^{-1} = P, \text{ para todo } g \in G.$$

Portanto, P é um subgrupo normal de G. □

O terceiro Teorema de Sylow nos dá informações em relação ao número de p-subgrupos de Sylow de um dado grupo finito.

Teorema 2.2.6 (Terceiro Teorema de Sylow)**.** *Sejam p um número primo e k, m inteiros de modo que k é não nulo. Seja G um grupo de ordem $p^k m$ com p não dividindo m. Se n_p é o número de p-subgrupos de Sylow de G, então vale as seguintes condições:*

(i) $n_p \equiv 1 (\text{mod } p)$*;*

(ii) n_p *divide* m*.*

Além disso, quaisquer dois p-subgrupos de Sylow de G são conjugados.

Demonstração. Seja K um p-subgrupo de Sylow de G e seja $C = \{K_1, K_2, \cdots, K_n\}$, com $K = K_1$, o conjunto de todos os conjugados de K em G. Como na prova do Teorema 2.2.4, consideremos o conjunto S_c formado por todas as permutações de C e o homomorfismo

$T : G \to S_c$ definido por

$$\begin{array}{rccccc} T: & G & \to & S_C & & \\ & g & \mapsto & \varphi_g: & C & \to & C \\ & & & & K_i & \mapsto & gK_ig^{-1}. \end{array}$$

Como $|K|$ é uma potência de p, segue pelo Corolário 1.4.3, que $|T(K)|$ também é. Agora, pelo Teorema da órbita e do estabilizador 1.5.8, temos,

$$|T(K)| = |orb_{T(K)}(K_i)||stab_{T(K)}(K_i)|.$$

Consequentemente, $|orb_{T(K)}(K_i)|$ divide $|T(K)|$ para cada $i \in \{1, \cdots, n\}$ e, assim, $|orb_{T(K)}(K_i)|$ é também uma potência de p. Como na prova do Teorema 2.2.4, $|orb_{T(K)}(K_i)| = 1$ se, e somente se, $K \leqslant K_i$. Como $K = K_1$, temos que $|orb_{T(K)}(K_1)| = 1$ e $|orb_{T(K)}(K_i)|$ é uma potência de p maior que 1, para todo $i \in \{2, \cdots, n\}$. Uma vez que o conjunto das órbitas da ação de $T(K)$ sobre C gera uma partição de C, temos que

$$\begin{aligned} |C| &= |orb_{T(K)}(K_1)| + |orb_{T(K)}(K_2)| + \cdots + |orb_{T(K)}(K_n)| \\ &= 1 + |orb_{T(K)}(K_2)| + \cdots + |orb_{T(K)}(K_n)|. \end{aligned}$$

Daí,

$$n - 1 = |orb_{T(K)}(K_2)| + \cdots + |orb_{T(K)}(K_n)|.$$

Como p divide $|orb_{T(K)}(K_i)$ para todo $i \in \{2, \cdots, n\}$, temos que $p|(n-1)$, assim, $n \equiv 1 (\text{mod } p)$.

Agora vamos mostrar que todo p-subgrupo de Sylow de G pertence a C. Para isso, suponhamos que H é um p-subgrupo de Sylow de G que não pertence a C. Notemos que, o conjunto das órbitas geradas pela ação de $T(H)$ sobre C também produz uma partição em C, assim

$$|C| = |orb_{T(H)}(K_1)| + |orb_{T(H)}(K_2)| + \cdots + |orb_{T(H)}(K_n)|.$$

Uma vez que $H \notin C$, temos que nenhuma órbita possui cardinalidade igual a 1. Portanto, $n \equiv 0 (\text{mod } p)$, pois $|orb_{T(H)}(K_i)|$ é divisível por p cada cada $i \in \{1, \cdots, n\}$. Logo, obtemos uma contradição com o que foi provado no parágrafo anterior. Logo, $H \in C$ e assim $n_p = n$.

Por fim, resta mostrar que n_p divide m. Da definição do conjunto C, segue que $n_p = |G : N_G(K)|$. De $K \leqslant N_G(K) \leqslant G$, vem da Proposição 1.3.9 (i) que

$$|G : K| = |G : N_G(K)||N_G(K) : K|.$$

Assim,

$$\begin{aligned} n_p \cdot |N(K) : K| &= |G : K| \\ &= \frac{|G|}{|K|} \\ &= \frac{p^k m}{p^k} \\ &= m. \end{aligned}$$

Portanto, n_p divide m. □

2.3 Aplicações dos Teoremas de Sylow

Os Teoremas de Sylow foram uma das principais ferramentas usadas na classificação dos grupos finitos simples.

Definição 2.3.1. *Um grupo G é dito simples, se seus únicos subgrupos normais são os triviais, isto é, $\{e_G\}$ e G.*

Proposição 2.3.2. *Todo grupo alternado A_n, com $n = 3$ ou $n \geq 5$, é simples.*

Demonstração. Ver [4, Teorema V.10.21 , p. 228-230]. □

Exemplo 2.3.3. *Todo grupo G de ordem 42 não é simples. De fato, vamos mostrar que esse grupo possui um subgrupo normal de ordem 7. Note que, ao fatorarmos a ordem de G, obtemos*

$$42 = 2 \cdot 3 \cdot 7.$$

Logo, pelo primeiro Teorema de Sylow (Teorema 2.2.1), existe pelo menos um subgrupo de ordem 7 que é um 7-subgrupo de Sylow.

Agora, vamos mostrar que este subgrupo é normal. Pelo terceiro Teorema de Sylow (Teorema 2.2.6), temos que

$$\begin{cases} n_7 \equiv 1 \pmod 7 \\ n_7 \text{ divide } 2 \cdot 3. \end{cases}$$

Logo, $n_7 = 1$, pois 1 é o único número que divide $2 \cdot 3$ e é congruente a 1 (mod 7), daí, pelo Corolário 2.2.5, segue que esse 7-subgrupo de Sylow é normal em G.

Proposição 2.3.4. *Todo p-grupo finito G não trivial, não é um grupo simples.*

Demonstração. Se G é abeliano, pelo primeiro Teorema de Sylow, existe um subgrupo de ordem p, que será normal em G.

Agora, se G não é abeliano, segue pela Proposição 2.1.3 que seu centro $Z(G)$ possui, pelo menos, p elementos. Como $Z(G) \neq G$, segue que $Z(G)$ é um subgrupo normal próprio de G. □

Exemplo 2.3.5. *Grupos de ordens* $8, 81$ *e* 3125 *não são simples. De fato, observe que*

$$8 = 2^3, \qquad 81 = 3^4, \qquad 3125 = 5^5.$$

Daí, pela Proposição 2.3.4 vemos que esses grupos não são simples.

Proposição 2.3.6. *Se* G *é um grupo tal que* $|G| = pq$*, com* p, q *números primos, então* G *não é um grupo simples.*

Demonstração. Se $p = q$, então $|G| = p^2$, e sabemos pela Proposição 2.1.4 que G é abeliano; pelo Teorema de Cauchy (Teorema 2.1.5) existe $g \in G$ de ordem p, donde temos $\langle g \rangle \triangleleft G$.

Suponhamos que $p > q$. Denotemos por n_p o número de p-subgrupos de Sylow de G. Do terceiro Teorema de Sylow (Teorema 2.2.6), temos que

$$\begin{cases} n_p \equiv 1 \pmod{p} \\ n_p \text{ divide } q. \end{cases}$$

Logo, $n_p = 1$, pois $p > q$. Assim, existe um único p-subgrupo de Sylow de G e pelo Corolário 2.2.5 ele é normal em G. □

Exemplo 2.3.7. *Todo grupo* G *de ordem 15 não é simples. De fato, ao fatorarmos a ordem de* G*, obtemos* $15 = 3 \cdot 5$*. Daí, segue pela Proposição 2.3.6 que* G *não é simples.*

Proposição 2.3.8. *Seja* G *um grupo tal que* $|G| = p^n q$*, com* p, q *números primos. Se* $p^n < q$*, então* G *possui um subgrupo normal de ordem* q*.*

Demonstração. Denotemos por n_q o número de q-subgrupos de Sylow de G. Pelo terceiro Teorema de Sylow (Teorema 2.2.6), temos que

$$\begin{cases} n_q \equiv 1 \pmod{q} \\ n_q \text{ divide } p^n. \end{cases}$$

Logo, $n_q \in \{1, p, p^2, \cdots, p^n\}$ e por $p^n < q$, tem-se que $n_q = 1$. Portanto, segue pelo Corolário 2.2.5 que o q-subgrupo de Sylow de G é normal em G. □

Exemplo 2.3.9. *Grupos de ordens* 20*,* 99 *e* 725 *não são simples. De fato, observe que*

$$20 = 2^2 \cdot 5, \qquad 99 = 3^2 \cdot 11, \qquad 725 = 5^2 \cdot 29.$$

Daí, segue pela Proposição 2.3.8 que esses grupos não são simples.

Algumas vezes, os Teoremas de Sylow não dão a resposta diretamente, mas dão a resposta após uma contagem, como será mostrado no exemplo a seguir.

Exemplo 2.3.10. *Não existe grupo G simples de ordem* 616. *De fato, uma vez que,*

$$616 = 2^3 \cdot 7 \cdot 11,$$

segue pelo primeiro Teorema de Sylow que G possui pelo menos um 7*-subgrupo de Sylow de ordem* 7 *e pelo menos um* 11*-subgrupo de Sylow de ordem* 11. *Daí, pelo terceiro Teorema de Sylow tem-se que,*

$$n_{11} \equiv 1 \ (mod\ 11) \ e\ n_{11}\ divide\ 2^3 \cdot 7$$

$$n_7 \equiv 1 \ (mod\ 7) \ e\ n_7\ divide\ 2^3 \cdot 11.$$

Assim, $n_{11} \in \{1, 56\}$ e $n_7 \in \{1, 8, 22\}$. Se $n_{11} = 1$ ou $n_7 = 1$, terminamos, pois pelo Corolário 2.2.5 teremos pelo menos um subgrupo normal em G que não é trivial. Então, suponhamos que $n_{11} = 56$ e $n_7 = 8$. Daí, faremos a contagem da quantidade de elementos diferentes da identidade do grupo G, ou seja, existem 10 *elementos diferentes da identidade em cada* 11*-subgrupo de Sylow de G e* 6 *elementos diferentes da identidade em cada* 7*-subgrupo de Sylow de G. Totalizando,*

$$10 \cdot 56 + 6 \cdot 8 = 608.$$

Neste caso, sobram $616 - 608 = 8$ elementos, que são elementos pertencentes ao único 2*-subgrupo de Sylow do grupo G, que pelo Corolário 2.2.5 é normal em G. Agora, suponhamos que $n_{11} = 56$ e $n_7 = 22$. Neste caso, teríamos $10 \cdot 56 + 6 \cdot 22 = 692$ elementos diferentes da identidade no grupo G, o que é um absurdo, pois G tem* 616 *elementos. Portanto, não existe um grupo G de ordem* 616 *simples.*

Capítulo

3

Uma Generalização para os Teoremas de Sylow

Neste capítulo, apresentaremos uma generalização para os Teoremas de Sylow em termos de grupos solúveis finitos, devido ao matemático Philip Hall. Para essa exposição, organizamos esse capítulo em três seções. A primeira trata sobre séries principais e de composições; a segunda sobre grupos solúveis finitos e na última seção enunciamos e provamos os Teoremas de Hall.

3.1 Séries Principais e Séries de Composição

Consideraremos uma cadeia de subgrupos de um grupo G,

$$G = A_0 \supset A_1 \supset A_2 \supset \cdots \supset A_n, \tag{3.1}$$

onde

$$A_i \triangleleft A_{i-1}, \quad i = 1, \ldots, n. \tag{3.2}$$

Estará associada à (3.1), a sequência de quocientes

$$A_{i-1}/A_i, \quad i = 1, \ldots, n, \tag{3.3}$$

onde cada quociente será chamado de **fator da série**.

Se cada A_i é um subgrupo normal de G, chamaremos a cadeia (3.1) de **série normal**. Se assumirmos apenas (3.2), chamaremos a cadeia de **série subnormal**.

Definição 3.1.1. *Uma série subnormal em que cada A_i é um subgrupo normal maximal* de A_{i-1} será chamada de série de composição.*

Definição 3.1.2. *Uma série normal em que cada grupo fator A_{i-1}/A_i é um subgrupo normal minimal não trivial de G/A_i é chamada de série principal. Equivalentemente, uma série normal será chamada de série principal se para cada $i = 1, \ldots, n$, não existe um subgrupo normal N de G, de modo que $A_i < N < A_{i-1}$.*

*Um subgrupo normal H de um grupo G é um subgrupo normal maximal de G se $H \neq \{1\}$ e não existe um subgrupo normal K de G tal que $\{1\} < H < K < G$.

Proposição 3.1.3. *Um grupo quociente G/N é simples se, e somente se, N for um subgrupo normal maximal do grupo G.*

Demonstração. ($\Rightarrow$) Suponhamos que N não é um subgrupo maximal de G. Daí, existe um subgrupo normal próprio H de G, que contém N propriamente, tal que

$$N \subsetneq H \subsetneq G.$$

Assim, H/N é um subgrupo normal de G/N não trivial. Portanto, G/N não é simples.

($\Leftarrow$) Suponhamos que G/N não seja simples. Então, existe $H/N \lhd G/N$ que é um subgrupo próprio não trivial. Daí pelo Lema 1.2.16, temos

$$N \lhd H \lhd G.$$

Logo, N não é subgrupo normal maximal de G.

Assim, concluímos que um grupo fator G/N é simples se, e somente se, N for subgrupo normal maximal de G. □

Proposição 3.1.4. *Todo grupo finito não trivial de G, admite uma série de composição.*

Demonstração. Inicialmente, afirmamos que existe um subgrupo G_1 de G que satisfaz

$$\begin{cases} G_1 \subsetneq G \\ G_1 \lhd G \end{cases}$$

e que é maximal para esta propriedade, isto é, tal que

$$\left.\begin{array}{l} G_1 \subseteq H \subsetneq G \\ H \lhd G \end{array}\right\} \Rightarrow G_1 = H.$$

De fato, o subgrupo $\{1\}$ está estritamente contido em G e é normal em G. Caso ele seja maximal para essa propriedade, podemos tomar $G_1 = \{1\}$; caso contrário, por definição mesmo, existe um subgrupo $H \supsetneq \{1\}$ que satisfaz $H \subsetneq G$ e $H \lhd G$. Caso H seja maximal para essa propriedade, podemos tomar $G_1 = H$; caso contrário, por definição mesmo, existe $H' \supsetneq H$ que satisfaz $H' \subsetneq G$ e $H' \lhd G$. Caso H' seja maximal para essa propriedade, podemos tomar $G_1 = H'$; caso contrário, continuamos o processo; este deve necessariamente parar, pois obtemos subgrupos $H, H', \ldots$ cada vez maiores, enquanto que o grupo G é finito.

Vamos mostrar agora que G possui uma série de composição. Pela afirmação, existe um subgrupo G_1 de G que satisfaz $G_1 \subsetneq G$ e $G_1 \lhd G$, e que é maximal para esta propriedade. Se $G_1 = \{1\}$, acabou:$\{1\} = G_1 \lhd G$ é uma série de composição. Se $G_1 \neq \{1\}$, pela

afirmação aplicada ao grupo G_1, obtemos a existência de de um subgrupo G_2 de G_1 que satisfaz $G_2 \subsetneq G_1$ e $G_2 \triangleleft G_1$, e que é maximal para esta propriedade. Se $G_2 = \{1\}$, acabou: $\{1\} = G_2 \triangleleft G_1 \triangleleft G$ é uma série de composição. Se $G_2 \neq \{1\}$, continuamos o processo aplicando a afirmação ao grupo G_2. Esse processo deve necessariamente acabar, pois obtemos subgrupos $G_1, G_2, \ldots$ cada vez menores, enquanto que o grupo G é finito.

□

O próximo resultado nos diz como as séries principais e as séries de composição se relacionam para um dado grupo.

Teorema 3.1.5. *Seja H um subgrupo normal de G tal que exista uma série de composição de G a H. Então, existe uma série principal de G a H,*

$$G = B_0 \supset B_1 \supset \cdots \supset B_n = H,$$

de modo que cada grupo quociente B_i/B_{i+1} é o produto direto de um número finito de grupos simples isomorfos. Reciprocamente, se tal série existe com B_i/B_{i+1} como produto direto de um número finito de grupos simples isomorfos, então existe uma série de composição de G a H.

Demonstração. Ver [6, Theorem 8.6.1, p. 131]. □

3.2 Grupos Solúveis

O conceito de grupo solúvel, um dos mais antigos na Teoria de Grupos, foi introduzido por Évariste Galois (1811-1832) quando estudava o problema de resolver equações algébricas por meio de radicais. Galois associava um grupo a cada equação e mostrou que a equação é solúvel por meio de radicais se, e somente se, o grupo correspondente é solúvel, da forma que definiremos abaixo.

Sem formalidades, um grupo é solúvel se ele é "quase abeliano". Por exemplo, um grupo G está "perto" de ser abeliano se ele contém um subgrupo normal H tal que tanto H quanto o quociente G/H são abelianos. Com uma generalização desta ideia, podemos elaborar a definição seguinte.

Definição 3.2.1. *Um grupo G diz-se solúvel se existe uma série subnormal*

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

tal que cada fator G_i/G_{i-1} é abeliano.

Exemplo 3.2.2.

1. *Todo grupo abeliano G é solúvel, uma vez que*

$$\{1\} \subset G$$

é uma série subnormal com as propriedades da Definição 3.2.1.

2. *Os grupos S_3 e S_4 são solúveis. De fato, para S_3,*

$$\{1\} \triangleleft A_3 \triangleleft S_3,$$

é uma série subnormal onde S_3/A_3 e $A_3/\{1\}$ são grupos abelianos, pois possuem ordem 2 e 3, respectivamente.

Para S_4,

$$\{1\} \triangleleft K_4 \triangleleft A_4 \triangleleft S_4,$$

onde K_4 é o grupo de Klein, é uma série subnormal onde S_4/A_4, A_4/K_4 e $K_4/\{1\}$ são grupos abelianos, pois possuem ordem 2, 3 e 4. respectivamente.

Uma definição muito importante no estudo dos grupos solúveis é a definição do comutador de dois elementos de um grupo G.

Definição 3.2.3. *Seja G um grupo. Dados $x, y \in G$, definimos o comutador de x e y como o elemento $x^{-1}y^{-1}xy \in G$, o qual será denotado por $[x, y]$. Mais geral, se H e K são dois subgrupos de um grupo G, definimos o subgrupo comutador de H e K por*

$$[H, K] := \langle h^{-1}k^{-1}hk | h \in H, k \in K \rangle.$$

Em particular, o grupo

$$G' := [G, G] = \langle x^{-1}y^{-1}xy | x, y \in G \rangle$$

será chamado de **subgrupo derivado** de G.

Utilizando essas noções, podemos definir indutivamente a seguinte sequência de subgrupos:

$$\begin{aligned} G^{(0)} &:= G \\ G^{(1)} &:= \left[G^{(0)}, G^{(0)}\right] = G' \\ G^{(2)} &:= \left[G^{(1)}, G^{(1)}\right] \\ &\vdots \quad \vdots \quad \vdots \\ G^{(n)} &:= \left[G^{(n-1)}, G^{(n-1)}\right]. \end{aligned}$$

O subgrupo $G^{(n)}$ será chamado de **n-ésimo subgrupo derivado** de G.

Proposição 3.2.4. *Sejam G um grupo e G' seu subgrupo derivado. Então,*

(i) $G' \triangleleft G$.

(ii) G/G' *é abeliano.*

(iii) G' *é o menor subgrupo normal de G com esta propriedade, isto é, se $H \triangleleft G$ é tal que G/H é abeliano, então $H \supseteq G'$.*

Demonstração. Para o item (i), sejam $g, x, y \in G$, vamos mostrar que $g[x,y]g^{-1} \in G'$. Note que,

$$\begin{aligned} g[x,y]g^{-1} = g(x^{-1}y^{-1})(xy)g^{-1} &\Rightarrow (gx^{-1})(g^{-1}g)(y^{-1}g^{-1})(gx)(g^{-1}g)(yg^{-1}) \\ &\Rightarrow (gx^{-1}g^{-1})(gy^{-1}g^{-1})(gxg^{-1})(gyg^{-1}). \end{aligned}$$

Uma vez que $gxg^{-1}, gyg^{-1} \in G$, temos que

$$g[x,y]g^{-1} = [gxg^{-1}, gyg^{-1}],$$

portanto, $g[x,y]g^{-1} \in G'$ e assim, $G' \triangleleft G$.

Para o item (ii), sejam $gG', hG' \in G/G'$. Note que

$$(hg)^{-1}(gh) = g^{-1}h^{-1}gh = [g,h] \in G'.$$

Daí,

$$\begin{aligned} ((hg)^{-1}G')((gh)G') = (hg)^{-1}(gh)G' = G' &\Rightarrow ((hg)(hg)^{-1})(gh)G' = (hg)G' \\ &\Rightarrow (gh)G' = (hg)G' \\ &\Rightarrow (gG')(hG') = (hG')(gG'). \end{aligned}$$

Portanto, G/G' é um grupo abeliano.

Para o item (iii), seja $H \triangleleft G$ tal que G/H é abeliano. Sejam $xH, yH \in G/H$. Note que,

$$\begin{aligned} xyH = yxH &\iff ((yx)^{-1}xy)H = H \\ &\iff (x^{-1}y^{-1}xy)H = H \\ &\iff [x,y] \in H. \end{aligned}$$

Logo, $G' \subseteq H$. □

Pela Proposição 3.2.4, a cadeia

$$G = G^{(0)} \supset G^{(1)} \supset \cdots \supset G^{(n)} \supset \cdots \tag{3.4}$$

é uma série subnormal em que cada grupo fator é abeliano. A cadeia (3.4) será chamada **série derivada** de G.

Proposição 3.2.5. *Seja G um grupo. As seguintes condições são equivalentes:*

(i) O grupo G é sóluvel.

(ii) Existe um inteiro n tal que $G^{(n)} = \{1\}$.

No caso de G ser finito, elas são também equivalentes a:

(iii) O grupo G possui uma série de composição cujos grupos fatores são abelianos (e portanto cíclicos de ordem prima).

Demonstração. $(i) \Rightarrow (ii)$. Como G é um grupo sóluvel, existe uma série subnormal

$$G = G_0 \triangleright G_1 \triangleright \cdots \triangleright G_r = \{1\}$$

tal que os fatores G_i/G_{i+1} são abelianos, para todo $i = 0, \ldots, r-1$. Sendo G_0/G_1 abeliano, sabemos pela Proposição 3.2.4 que $G_1 \supseteq (G_0)' = G^{(1)}$. Sendo G_1/G_2 abeliano, temos $G_2 \supseteq (G_1)' \supseteq (G^{(1)})' = G^{(2)}$. Sendo G_2/G_3 abeliano, temos $G_3 \supseteq (G_2)' \supseteq (G^{(2)})' = G^{(3)}$. Continuando desta maneira, obtemos que $G_i \supseteq G^{(i)}$, para todo $i = 0, \ldots, r$; portanto, obtemos que $G^{(r)} = \{1\}$.
$(ii) \Rightarrow (i)$. Pela Proposição 3.2.4, a série

$$G = G^{(0)} \triangleright G^{(1)} \triangleright G^2 \triangleright \cdots \triangleright G^{(n)} = \{1\},$$

é uma série subnormal cujos grupos fatores são abelianos.

Suponhamos agora que G é um grupo finito,
$(iii) \Rightarrow (i)$. É imediato.
$(i) \Rightarrow (iii)$. Como G é sóluvel, existe uma série subnormal

$$G = G_0 \triangleright G_1 \triangleright \cdots \triangleright G_r = \{1\}$$

tal que G_i/G_{i+1} abeliano, para todo $i = 0, \ldots, r-1$. Sendo G um grupo finito, então cada quociente G_i/G_{i+1} é um grupo finito abeliano. Podemos aplicar a Proposição 3.1.4 juntamente com o Teorema Fundamental dos Grupos Abelianos Finitos [3, Teorema 11.1] e Lema 1.2.16 a este grupo quociente para obter uma série de subgrupos entre G_i e G_{i+1} tal que cada grupo quociente desta série é cíclico de ordem prima. Fazendo isto para todo

índice $i = 0, \ldots, r-1$, obtemos uma série de composição de G cujos grupos quocientes são cíclicos de ordem prima.

□

Proposição 3.2.6. *Seja G um grupo solúvel. Então,*

(i) todo subgrupo de G é solúvel.

(ii) todo grupo quociente de G é solúvel.

Demonstração. (i) Seja G um grupo sóluvel e H um subgrupo de G. Então, por definição, $H' \subseteq G'$, uma vez que H' é gerado por todos os comutadores de elementos em H e G' por todos os comutadores em G. Logo, $(H')' \subseteq (G')'$, e assim sucessivamente, de modo que se $G^{(n)} = 1$, então $H^{(n)} = 1$ e, pela Proposição 3.2.5, H é solúvel. Aqui, $H^{(i)}$ pode ser a identidade para algum $i < n$.

(ii) Seja K um subgrupo normal. Então, $Q = G/K$ é um grupo fator de G. Considere o homomorfismo canônico $G \to Q$. Aqui, todo comutador em Q é a imagem de um comutador em G, de modo que $G' \to Q'$. Continuando, $G^{(n)} \to Q^{(n)}$, de onde $Q^{(n)} = 1$ se $G^{(n)} = 1$ e, assim, pela Proposição 3.2.5, Q é solúvel. Novamente, $Q^{(i)}$ pode ser a identidade para algum $i < n$. □

Definição 3.2.7. *Seja p um número primo. Um p-grupo abeliano finito que é isomorfo a $\mathbb{Z}_p \times \mathbb{Z}_p \times \cdots \times \mathbb{Z}_p$ é chamado de grupo abeliano elementar.*

Proposição 3.2.8. *Se G é um grupo solúvel finito, então todo subgrupo normal minimal de G é um grupo abeliano elementar.*

Demonstração. Ver [11, Theorem 5.24, p. 105-106]. □

Proposição 3.2.9. *Se G é um grupo solúvel, então G possui uma série de composição de modo que os grupos fatores são abelianos.*

Demonstração. Pela Proposição 3.2.4,

$$G \supset G^{(1)} \supset G^{(2)} \supset \cdots \supset G^{(n)} = \{1\},$$

é uma série subnormal em que cada grupo fator é abeliano. Assim, existirá um subgrupo normal maximal $A_1 \supseteq G^{(1)}$. Pela Proposição 3.1.3 G/A_1 é simples e, portanto, cíclico de ordem prima. Similarmente, como A_1 é solúvel, A_1 contém um subgrupo normal maximal A_2 tal que A_1/A_2 é cíclico de ordem prima. Continuando, temos

$$G = A_0 \supset A_1 \supset \cdots \supset A_r = \{1\},$$

onde cada A_{i-1}/A_i é cíclico de ordem prima. □

Teorema 3.2.10. *Todo grupo sóluvel finito G possui uma série principal,*

$$G = C_0 \supset C_1 \supset \cdots \supset C_s = \{1\},$$

de modo que os grupos fatores C_{i-1}/C_i, para $i = 1, \ldots, s$, são grupos abelianos elementares.

Demonstração. Pela Proposição 3.2.9, G possui uma série de composição de modo que os grupos fatores são abelianos. Segue do Teorema 3.1.5 que G possui uma série principal

$$G = C_0 \supset C_1 \supset \cdots \supset C_s = \{1\},$$

onde C_{i-1}/C_i é o produto direto de grupos simples isomorfos. Pela Proposição 3.2.6, esses grupos simples são solúveis e, portanto, cíclicos de ordem prima. Assim, C_{i-1}/C_i é o produto direto de grupos cíclicos de mesma ordem prima p e assim, cada C_{i-1}/C_i são grupos abelianos elementares. □

Proposição 3.2.11. *Seja G um grupo sóluvel finito e K um subgrupo normal de G. Então,*

(i) para um subgrupo H de G, as ordens dos fatores principais de H são divisores das ordens dos fatores principais de G.

(ii) as ordens dos fatores principais de G/K formam um subconjunto das ordens dos fatores principais de G.

Demonstração. (i) De G ser solúvel e finito, pelo Teorema 3.2.10, existe uma série principal

$$G = G_0 \supset G_1 \supset \cdots \supset G_s = \{1\}, \tag{3.5}$$

de modo que cada G_{i-1}/G_i é abeliano elementar. Agora, considere a seguinte série de subgrupos de H,

$$H \supseteq H \cap G_1 \supseteq H \cap G_2 \supseteq \cdots \supseteq H \cap G_s = \{1\}. \tag{3.6}$$

Note que, pela Proposição 1.2.9 a série (3.6) é uma série normal de H. Pelo Lema 1.4.6,

$$\frac{H \cap G_{i-1}}{H \cap G_i} \text{ é um subgrupo isomorfo de } \frac{G_{i-1}}{G_i}.$$

Pelo Teorema de Langrange,

$$\left|\frac{H \cap G_{i-1}}{H \cap G_i}\right| \text{ divide } \left|\frac{G_{i-1}}{G_i}\right|.$$

Se existe $i \in \{1, \ldots, n\}$ e $L \triangleleft H$ de modo que,

$$H \cap G_{i-1} \supseteq L \supseteq H \cap G_i.$$

Observe que pela Proposição 1.3.9,

$$|H \cap G_{i-1} : H \cap G_i| = |H \cap G_{i-1} : L||L : H \cap G_i|.$$

Consequentemente, $|H \cap G_{i-1} : L|$ e $|L : H \cap G_i|$ divide $|G_{i-1} : G_i|$, uma vez que $|H \cap G_{i-1} : H \cap G_i|$ divide $|G_{i-1} : G_i|$. Podemos repetir esse processo até obter uma série principal para H que, por construção, terá a propriedade do enunciado.

(ii) De G/K ser um grupo sóluvel, existe uma série principal

$$G/K = \overline{Q_0} \supseteq \overline{Q_1} \supseteq \cdots \supseteq \overline{Q_n} = \{1\}. \tag{3.7}$$

Pelo Lema 1.2.16, obtemos a seguinte série normal,

$$G = Q_0 \supseteq Q_1 \supseteq Q_2 \supseteq \cdots \supseteq K. \tag{3.8}$$

Usando a série normal em (3.5) para completar a série normal em (3.8) obtemos a seguinte série normal de G:

$$G = Q_0 \supseteq Q_1 \supseteq Q_2 \supseteq \cdots \supseteq K \supseteq K \cap G_1 \supseteq K \cap G_2 \supseteq \cdots \supseteq K \cap G_n = \{1\}. \tag{3.9}$$

Pelo Terceiro Teorema de Isomorfismo (Proposição 1.4.5),

$$\frac{Q_{i-1}}{Q_i} \approx \frac{\overline{Q}_{i-1}}{\overline{Q}_i} \quad \text{e} \quad \frac{\overline{Q}_0}{\overline{Q}_i} \approx \frac{G}{Q_i}.$$

Da série (3.7) ser principal, temos que Q_{i-1}/Q_i é normal e minimal em G/Q_i. Fazendo um processo análogo ao feito na prova do item (i) na série (3.9),a partir do subgrupo$K$, obteremos uma série principal de G com as propriedades desejadas.

□

3.3 Os Teoremas de Hall

Em setembro de 1927, o matemático inglês, Philip Hall, fez uma importante descoberta na Teoria dos Grupos ao demonstrar que os Teoremas de Sylow são generalizados para grupos solúveis finitos de ordem mn, em que m é relativamente primo em relação à n, sem a exigência de m ser uma potência de um número primo p.

Teorema 3.3.1 (Teoremas de Hall)**.** *Seja G um grupo solúvel finito e $|G| = mn$, com* $\mathrm{mdc}(m, n) = 1$*. Então,*

(i) G possui pelo menos um subgrupo de ordem m.

(ii) quaisquer dois subgrupos de ordem m são conjugados.

(iii) qualquer subgrupo cuja ordem m' divide m está contido em um subgrupo de ordem m.

(iv) o número h_m de subgrupos de ordem m pode ser expresso como um produto de fatores, em que cada um

(a) é congruente a 1 módulo algum fator primo de m;

(b) é uma potência de um número primo e divide a ordem de um dos fatores de uma série principal de G.

Demonstração. Note que se $m = p^k$, com p sendo um número primo, o item (i) é provado pelo Primeiro Teorema de Sylow (Teorema 2.2.1). O item (ii) é provado pelo Terceiro Teorema de Sylow (Teorema 2.2.6). O item (iii) é provado pelo Segundo Teorema de Sylow 2.2.4 e o item (iv) é uma declaração mais forte do Terceiro Teorema de Sylow (Teorema 2.2.6).

A prova será por indução sobre a ordem de G, sendo trivialmente verdadeira se a ordem de G for uma potência de um número primo. Além disso, a prova se baseará fortemente na estrutura de uma série principal de G e na estrutura dos grupos de fatores.

Dividiremos a demonstração em dois casos.

CASO 1: O grupo G tem um subgrupo normal próprio H de ordem m_1n_1, onde $m = m_1m_2$, $n = n_1n_2$ e $n_1 < n$.

Para o item (i), suponhamos que a afirmação do item (i) seja verdadeira para todos os grupos solúveis finitos com ordem menor que $|G|$. Pelo Teorema de Lagrange, temos que G/H tem ordem igual

$$\left|\frac{G}{H}\right| = \frac{mn}{m_1n_1} = \frac{m_1m_2n_1n_2}{m_1n_1} = m_2n_2.$$

Uma vez que $\mathrm{mdc}(m_2, n_2) = 1$ e $|G/H| < |G|$, segue pela hipótese de indução, que G/H tem um subgrupo $\overline{D}$ de ordem m_2. Pelo Lema 1.2.16, existe um subgrupo D de G que contém H, de modo que $\overline{D} = D/H$. Pelo Teorema de Lagrange,

$$|D| = |D : H||H| = m_2m_1n_1 = mn_1.$$

Note que, $\mathrm{mdc}(m, n_1) = 1$ e de $n_1 < n$ segue que $|D| < |G|$. Assim, novamente pela hipótese de indução, segue que D tem um subgrupo S de ordem m, consequentemente, $S \leqslant G$, uma vez que $D \leqslant G$.

Para o item (ii), sejam M e M' dois subgrupos de G ordem m. Como H é subgrupo normal em G, segue pelo Lema 1.2.8 que MH e $M'H$ são subgrupos de G. Afirmamos que $|MH|$ e $|M'H|$ divide $m_1m_2m_1n_1$. De fato, pelo segundo Teorema de isomorfismo (Teorema 1.4.4) temos que

$$\frac{MH}{H} \approx \frac{M}{M \cap H}. \tag{3.10}$$

Daí, pelo Teorema de Lagrange,

$$\begin{aligned} |MH| &= |MH : H||H| \\ &\overset{(3.10)}{=} |M : M \cap H||H| \\ &= \frac{m}{|M \cap H|} m_1 n_1 \\ &= \frac{m_1 m_2 m_1 n_1}{|M \cap H|}. \end{aligned}$$

Agora, note que,

$$\frac{m_1m_2m_1n_1}{|MH|} = \frac{m_1m_2m_1n_1}{\frac{m_1m_2m_1n_1}{|M\cap H|}} = m_1m_2m_1n_1\frac{|M \cap H|}{m_1m_2m_1n_1} = |M \cap H|.$$

Similarmente, mostra-se que $|M'H|$ divide $m_1m_2m_1n_1$.

Pelo Teorema de Lagrange, $|MH|$ e $|M'H|$ divide mn. Então, $|MH|$ e $|M'H|$ divide

$$\text{mdc}(m_1m_2m_1n_1, mn) = (m_1m_2m_1n_1, m_1m_2n_1n_2) = m_1m_2n_1 = mn_1.$$

Uma vez que $\text{mdc}(m, n_1) = 1$ e $|MH|$ e $|M'H|$ são múltiplos de m e n_1, segue que

$$|MH| = |M'H| = mn_1 = m_1m_2n_1.$$

Para concluir a prova do item (ii), procederemos agora por indução sobre $|G|$. Suponhamos que a afirmação do item (ii) seja verdadeira para todos os grupos solúveis finitos com ordem menor que $|G|$. Provaremos que a afirmação do item (ii) também vale para G. Pelo Teorema de Lagrange,

$$\left|\frac{MH}{H}\right| = \left|\frac{M'H}{H}\right| = \frac{mn_1}{m_1n_1} = \frac{m_1m_2n_1}{m_1n_1} = m_2.$$

Como

$$m_2n_2 = \left|\frac{G}{H}\right| < |G|,$$

e $\text{mdc}(m_2, n_2) = 1$, segue pela hipótese de indução, que os dois subgrupos $(MH)/H$ e $(M'H)/H$ são conjugados em G/H.

Consideremos o homomorfismo canônico

$$\begin{aligned} \pi : \ G &\to G/H \\ g &\mapsto gH. \end{aligned}$$

Pelo Lema 1.4.8,

$$\pi^{-1}\left(\frac{MH}{H}\right) = MH \text{ e } \pi^{-1}\left(\frac{M'H}{H}\right) = M'H$$

são subgrupos conjugados em G. Agora, note que $aM'a^{-1}$ e M são subgrupos de ordem m em MH, para algum $a \in G$. Como $|MH| = mn_1 < |G|$, pois $n_1 < n$, e $\text{mdc}(m, n_1) = 1$, segue novamente pela hipótese de indução que os subgrupos $aM'a^{-1}$ e M são conjugados em MH. Logo, existe $b \in MH$ tal que

$$M = b(aM'a^{-1})b^{-1} = baM'(ba)^{-1}.$$

Uma vez que $MH \leqslant G$, segue que M e M' são conjugados em G.

Para o item (iii), seja M_1 um subgrupo de G ordem m'. Suponhamos que m' seja um divisor de m. Como H é subgrupo normal em G, segue pelo Lema 1.2.8 que M_1H é subgrupo de G. Afirmamos que $|(M_1H)/H|$ divide m_2. De fato, note que,

$$\left|\frac{G}{H}\right| = \frac{mn}{m_1n_1} = \frac{m_1m_2n_1n_2}{m_1n_1} = m_2n_2.$$

Como $\text{mdc}(m, n) = 1$ e m' divide m, segue que $\text{mdc}(m', n) = 1$. Nesse caso, segue que qualquer divisor de m' é relativamente primo com n. Em particular, $|(M_1H)/H|$ é relativamente primo com n, consequentemente, $|(M_1H)/H|$ é relativamente primo com n_2, pois n_2 é divisor de n. Logo, pelo Teorema de Lagrange $|(M_1H)/H|$ divide $|G/H|$, donde concluimos que $|(M_1H)/H|$ divide m_2.

Para a indução, suponhamos que a afirmação do item (iii) seja verdadeira para todos os grupos solúveis finitos com ordem menor que $|G|$. Vamos mostrar que a afirmação também vale para G. Como

$$m_2n_2 = \left|\frac{G}{H}\right| < |G|,$$

e $\text{mdc}(m_2, n_2) = 1$, segue pela hipótese de indução, que $(M_1H)/H$ está contido em um subgrupo $\overline{D}$ de G/H de ordem m_2. Pelo Lema 1.2.16, existe um subgrupo D de G que contém H, de modo que $\overline{D} = D/H$ e, portanto, $M_1 \subset D$.

Pelo Teorema de Lagrange,

$$|D| = |D : H||H| = m_2m_1n_1 = mn_1.$$

Como $|D| < |G|$, pois $n_1 < n$, e $\text{mdc}(m, n_1) = 1$, segue pela hipótese de indução que

o subgrupo M_1 está contido em um subgrupo S de ordem m.

Para o item (iv), sabemos pelo item (ii) que para determinar o número de subgrupos de ordem m é suficiente calcular o número de conjugados para o dado subgrupo M de G.

Na prova do item (ii), concluimos que se $M \leqslant G$ de ordem m, então $(MH)/H \leqslant G/H$ de ordem m_2 e quaisquer subgrupos de G/H de ordem m_2 são conjugados. Vamos denotar por

$$\overline{D}_1, \overline{D}_2, \cdots, \overline{D}_{h_{m_2}},$$

todos os subgrupos de G/H de ordem m_2. Suponhamos que $\overline{D}_1 = (MH)/H$. Assim, a menos de uma permutação de índices, temos que

$$\overline{a}_i \overline{D}_1 \overline{a}_i^{-1} = \overline{D}_i, \text{ para algum } \overline{a}_i \in G/H, \ i = 2, \cdots, h_{m_2}.$$

Desse modo, as pré-imagens desses subgrupos via o homomorfismo canônico $\pi : G \longrightarrow G/H$ são conjugados em G, ou seja,

$$a_i(MH)a_i^{-1} = a_i D_1 a_i^{-1} = D_i, \ i = 2, \cdots h_{m_2}.$$

Aqui, $a_i = \pi^{-1}(\overline{a}_i)$. Desse modo, existem pelo menos h_{m_2} subgrupos de ordem m, a saber,

$$M, a_2 M a_2^{-1}, \cdots, a_{h_{m_2}} M a_{h_{m_2}}^{-1}.$$

Agora, sejam

$$M = M_1, M_2, \cdots, M_r$$

todos os subgrupos conjugados de M em MH. Então, todos os subgrupos de ordem m de G são:

$$\begin{array}{ccccc} M, & a_2 M a_2^{-1}, & \cdots, & a_{h_{m_2}} M a_{h_{m_2}}^{-1} \\ M_2, & a_2 M_2 a_2^{-1}, & \cdots, & a_{h_{m_2}} M_2 a_{h_{m_2}}^{-1} \\ \vdots & \vdots & & \vdots \\ M_r, & a_2 M_r a_2^{-1}, & \cdots, & a_{h_{m_2}} M_r a_{h_{m_2}}^{-1} \end{array}$$

Portanto, a quantidade de subgrupos de ordem m é $h_{m_2} r$.

Uma vez que $|G/H| < |G|$ e $|MH| < |G|$, segue por indução, que as condições do item (iv) são válidas para h_{m_2}, que representa o número de subgrupos de ordem m_2 de G/H, e para r, que representa o número de subgrupos de ordem m de MH. Pela Proposição 3.2.11, temos que as ordens dos fatores principais de G/H formam um subconjunto das ordens dos fatores principais de G e as ordens dos fatores principais de MH divide as ordens dos fatores principais de G. Logo, as condições do item (iv) vale para $h_m = h_{m_2} r$.

Se houver algum subgrupo normal próprio de G cuja ordem não seja divisível por n, então o teorema foi provado. Podemos, portanto, assumir que n divide $|H|$ para todo

subgrupo normal próprio H. Se H for um subgrupo normal minimal, no entanto, a Proposição 3.2.8 diz que H é um p-grupo abeliano elementar para algum número primo p. Pode-se, assim, assumir que $n = p^a$, de modo que H seja um p-subgrupo de Sylow de G. A normalidade de H força H a ser único, uma vez que todos os p-subgrupos de Sylow são conjugados. Desse modo, o problema agora foi reduzido ao caso seguinte.

CASO 2: $|G| = mp^a$, onde $p \nmid m$, G contém um p-subgrupo de Sylow normal abeliano K e K é o único subgrupo normal minimal em G.

Para o item (i), segue pela Proposição 3.2.6, que o grupo G/K é solúvel de ordem m. Seja L/K um subgrupo normal minimal de G/K. Pela Proposição 3.2.8 o grupo L/K é um q-grupo abeliano elementar, para algum número primo $q \neq p$. Agora, pelo Teorema de Lagrange,

$$|L| = |L : K||K| = q^b p^a, \text{ para algum inteiro positivo } b.$$

Seja Q um q-subgrupo de Sylow de L de ordem q^b e consideremos $N_G(Q)$ o normalizador de Q em G. Considere $N_G(Q) \cap K = T$. T é um subgrupo normal de $N_G(Q)$. De fato, sejam $t \in T$ e $a \in N_G(Q)$. Note que,

$$ata^{-1} \in K, \text{ pois } t \in K, \text{ e } K \lhd G;$$

e

$$ata^{-1} \in N_G(Q), \text{ pois } N_G(Q) \leqslant G \text{ e } t, a \in N_G(Q).$$

Logo, $ata^{-1} \in T = N_G(Q) \cap K$, e assim $aTa^{-1} \subseteq T$. Pelo teste de subgrupo normal, segue que $T \lhd N_G(Q)$. Como $T \leqslant K$, e K é abeliano, segue que T é abeliano.

Todo elemento de T permuta com todo elemento de Q. Com efeito, sejam $t \in T$ e $a \in Q$. Observe que,

$$[t, a] = t\underbrace{at^{-1}a^{-1}}_{\in T} \in T, \text{ pois } T \lhd N_G(Q);$$

e

$$[t, a] = \underbrace{tat^{-1}}_{\in Q}a^{-1} \in Q, \text{pois } T \leqslant N_G(Q).$$

Daí, $[t, a] \in T \cap Q$. Uma vez que T está contido em um p-subgrupo de Sylow, K, e Q é um q-subgrupo de Sylow, segue que $T \cap Q = 1$.

Afirmamos que T pertence ao centro $Z(L)$ de L. De fato, primeiro note que pela Proposição 1.3.9, temos que $|QK| = q^b p^a$, uma vez que $Q \cap K = 1$. Assim, $L = QK$.

Portanto, todo elemento $l \in L$ é da forma $l = xy$, com $x \in Q$ e $y \in K$. Note que,

$$\begin{aligned} tl &= t(xy) \\ &= (tx)y \\ &= (xt)y, \text{ pois os elementos de } T \text{ e } Q \text{ comutam} \\ &= x(ty) \\ &= x(yt) \text{ , pois } K \text{ é abeliano e } T \leqslant K \\ &= (xy)t \\ &= lt. \end{aligned}$$

Pela Proposição 1.4.12, $Z(L)$ char L, e como $L \triangleleft G$, então $Z(L) \triangleleft G$ (ver Proposição 1.4.13).

Se $Z(L) \neq 1$, então $K \leqslant Z(L)$, uma vez que K é o único subgrupo normal minimal de G. Desse fato, concluímos que cada elemento $l \in L = QK$ é escrito unicamente da forma $l = xy$, com $x \in Q$ e $y \in K$. De fato, suponhamos que l pode ser escrito de duas maneiras diferentes, $l = x_1y_1$ e $l = x_2y_2$, com $x_1, x_2 \in Q$ e $y_1, y_2 \in K$. Assim,

$$\begin{aligned} x_1y_1 = x_2y_2 &\Rightarrow x_2^{-1}(x_1y_1)y_1^{-1} = x_2^{-1}(x_2y_2)y_1^{-1} \\ &\Rightarrow x_2^{-1}x_1 = y_2y_1^{-1} \end{aligned}$$

Logo, $x_2^{-1}x_1, y_2y_1^{-1} \in Q \cap K = 1$. Daí, $x_1 = x_2$ e $y_1 = y_2$. Pela Proposição 1.4.10, segue que $Q \triangleleft G$ e, assim, $K \leqslant Q$, uma contradição. Portanto, $Z(L) = 1$. Daí, como $T = N_G(Q) \cap K \leqslant Z(L)$, segue que $T = 1$, portanto, $N_L(Q) = Q$. Assim, Q possui tantos conjugados em L, quanto seu índice em L, isto é, Q possui p^a conjugados em L. Qualquer conjugado de Q em G está em L, já que L é um subgrupo normal de G. Portanto, Q tem $n = p^a$ conjugados em G. Assim, $|G : N_G(Q)| = p^a$, pelo Teorema de Lagrange,

$$|N_G(Q)| = \frac{|G|}{|G : N_G(Q)|} = \frac{mp^a}{p^a} = m.$$

Uma vez que $N_G(Q) \leqslant G$, o item (i) está provado.

Para os itens (ii) e (iv), seja S um conjugado de Q em L. Pelo terceiro Teorema de Sylow (Teorema 2.2.6), S também é um q-subgrupo de Sylow de L. Pelo o que já foi provado no item (i) do Caso 2, S é distinto de Q e $N_L(S) = S$. Assim, os normalizadores dos p^a conjugados de Q em L são conjugados e distintos. Logo, temos p^a subgrupos conjugados de ordem m, uma vez que existem p^a q-subgrupos de Sylow distintos em L e o normalizador de cada um desses subgrupos em G, é um subgrupo de ordem m. Agora, se M' é qualquer subgrupo de ordem m, a ordem de $M'L$ é dada por

$$|M'L| = \frac{|M'||L|}{|M' \cap L|} = \frac{mq^bp^a}{|M' \cap L|} \overset{n=p^a}{=} \frac{mnq^b}{|M' \cap L|},$$

de onde vemos que mn divide a $|M'L|$. Logo, $G = M'L$. Pelo segundo Teorema de Isomorfismo, temos que

$$\frac{G}{L} \approx \frac{M'}{M' \cap L} \tag{3.11}$$

Vamos mostrar que $|M' \cap L| = q^b$. De fato, pelo Teorema de Lagrange,

$$\begin{aligned} |M'| &= |M' : M' \cap L||M' \cap L| \\ &\overset{(3.11)}{=} |G : L||M' \cap L| \\ &= \frac{m}{q^b}|M' \cap L|. \end{aligned}$$

Assim,

$$|M' \cap L| = m\frac{q^b}{m} = q^b.$$

De $|M' \cap L| = q^b$, segue que $M' \cap L$ é um conjugado de Q. Além disso, $M' \cap L$ é normal em M', pois para qualquer $x \in M' \cap L$ e $m \in M'$, temos que $mxm^{-1} \in M'$ e $mxm^{-1} \in L$, já que L é normal em G (Lema 1.2.16). Logo, $M' \leqslant N_G(M' \cap L)$, pela prova do item (i) do Caso 2, $|N_G(M' \cap L)| = m$, donde concluímos que $M' = N_G(M' \cap L)$. Assim, os p^a subgrupos conjugados de ordem m já constituem todos os subgrupos de ordem m. Isso prova o item (ii).

Uma vez que existem p^a q-subgrupos de Sylow em L, segue pelo terceiro Teorema de Sylow que

$$p^a \equiv 1 \pmod{q}.$$

Foi provado no parágrafo anterior que existem exatamente p^a subgrupos de ordem m. Como K é um p-subgrupo de Sylow abeliano normal e minimal em G, segue que existe uma série principal de G onde K figura entre os termos na seguinte posição

$$G \supseteq \cdots \supseteq K \supseteq \{1\}.$$

Logo, como p^a divide $|K : \{1\}| = p^a$ o item (iv) está provado.

Para o item (iii), sejam M' um subgrupo de G de ordem m', um divisor de m, e M um subgrupo de G de ordem m. Consideremos o $M^* = M \cap (M'K)$. Vamos mostrar que $|M^*| = m'$. Como m' divide m, existe $d \in \mathbb{Z}$ tal que $m = m'd$. Note que,

$$\left|\frac{G}{M}\right| = \frac{mp^a}{m} = p^a$$

e

$$\left|\frac{G}{M'K}\right| = \frac{mp^a}{m'p^a} = \frac{m'dp^a}{m'p^a} = d,$$

uma vez que pela Proposição 1.3.9,

$$|M'K| = \frac{|M'||K|}{|M' \cap K|} = \frac{m'p^a}{|M' \cap K|},$$

e de $\mathrm{mdc}(m', p^a) = 1$, vemos que $M' \cap K$ é trivial. Como $\mathrm{mdc}(p^a, d) = 1$, segue pela Proposição 1.3.10 que

$$\left|\frac{G}{M \cap (M'K)}\right| = \left|\frac{G}{M}\right| \left|\frac{G}{M'K}\right| = p^a d.$$

Então,

$$|M \cap (M'K)| = \frac{|G|}{p^a d} = \frac{mp^a}{p^a d} = \frac{m'dp^a}{p^a d} = m'.$$

Aplicando o resultado do item (ii) para $M'K$, temos que M^* é conjugado a M' (aqui estamos aplicando a hipótese de indução). Uma vez que $M^* \leqslant M$, segue que M' está contido em um conjugado de M de ordem m. □

Note que os Teoremas de Hall (Teorema 3.3.1) garantem a existência de subgrupos de ordens que não são assegurados apenas com o uso dos Teoremas de Sylow.

Exemplo 3.3.2. *Seja G um grupo sóluvel finito de ordem 60. Então,*

(i) G possui pelo menos um subgrupo de ordem 12;

(ii) G possui pelo menos um subgrupo de ordem 15;

(iii) G possui pelo menos um subgrupo de ordem 20.

Com efeito, ao fatorarmos o número 60, obtemos

$$60 = 2^2 \cdot 3 \cdot 5.$$

Daí, para o item (i), consideramos $m = 2^2 \cdot 3 = 12$ e $n = 5$. Uma vez que $\mathrm{mdc}(12, 5) = 1$, segue pelo item (i) do Teorema 3.3.1 que existe um subgrupo H de G de ordem 12. Para o item (ii), consideramos $m = 3 \cdot 5 = 15$ e $n = 2^2 = 4$. Uma vez que $\mathrm{mdc}(15, 4) = 1$, segue pelo item (i) do Teorema 3.3.1 que existe um subgrupo K de G de ordem 15. Para o item (iii), consideramos $m = 2^2 \cdot 5 = 20$ e $n = 3$. Uma vez que $\mathrm{mdc}(20, 3) = 1$, segue pelo item (i) do Teorema 3.3.1 que existe um subgrupo L de G de ordem 20.

Capítulo

4

Considerações Finais

Neste trabalho, apresentamos alguns resultados centrais da Teoria de Grupos Finitos; começando pelo Teorema de Lagrange e culminando nos Teoremas de Hall, que generalizam os Teoremas de Sylow em termos de grupos solúveis finitos.

Embora tenhamos focado em uma generalização para grupos solúveis finitos, é importante mencionar que há diversas outras generalizações para os Teoremas de Sylow. Por exemplo, existem generalizações para grupos localmente finitos [8] e para table algebras, fusion rule algebras, and hypergroups [1]. Além disso, existe uma generalização particular para o Terceiro Teorema de Sylow [2]. Essa generalização diz que,

Teorema 4.0.1. *Seja c o número de potências de p que são cone points de D. Então $v_D(H, G)$ é divisível por p^c. Se G é p-perfeito módulo H, então $v_D(H, G)$ é divisível por p^w, onde w é o número de potências de p que são cone points fracos de D.*

A demonstração e corolários decorrentes deste teorema podem ser consultados em [2].

Referências Bibliográficas

[1] BLAU, H. I.; ZIESCHANG, Paul-Hermann. ***Sylow theory for table algebras, fusion rule algebras, and hypergroups***. Journal of Algebra, vol. 273, n° 2, p. 551–570, 2004. DOI: 10.1016/j.jalgebra.2003.09.041. Disponível em: `https://core.ac.uk/display/82065934`. Acesso em: 20 nov. 2024.

[2] BROWN, K. S.; THÉVENAZ, J., ***A Generalization of Sylow's Third Theorem***, Journal of Algebra, vol. 115, p. 414–430, 1988. Disponível em: `https://core.ac.uk/download/pdf/82386925.pdf`. Acesso em: 20 nov. 2024.

[3] GALLIAN, J. A. ***Contemporary Abstract Algebra***. 8th Edition. Boston: Brooks/Cole, 2013.

[4] GARCIA, A. LEQUAIN, Y. ***Elementos de álgebra***. Rio de Janeiro: IMPA, 2002.

[5] GORENSTEIN, D. ***Finite Simple Groups:*** *An Introduction to Their Classification*. 1st Edition. New York: Springer Science+Business Media, 1982.

[6] HALL JR, M. ***The Theory of Groups***. 4th Edition. New York: The Macmillan Company, 1963.

[7] HALL, P. ***A Note on Soluble Groups***. Journal of the London Mathematical Society, vol. 3, n° 1, p. 98-105, 1928.

[8] HARTLEY, B. ***Sylow theory in locally finite groups***. Compositio Mathematica, vol. 25, n° 3, p. 263-280, 1972. Disponível em: `http://www.numdam.org/item/CM_1972__25_3_263_0`. Acesso em: 20 nov. 2024.

[9] ROBINSON, D. J. S. ***A Course in the Theory of Groups***. 2th Edition. New York: Springer, 1996.

[10] ROTH, R. L. ***A History of Lagrange's Theorem on Groups***. Mathematics Magazine, vol. 74, n° 2, p. 99-108, 2001.

[11] ROTMAN, J. J. ***An Introduction to the Theory of Groups***. 4th Edition. New York: Springer, 1995.