UNIVERSIDADE ESTADUAL DA PARAÍBA
CAMPUS VI - POETA PINTO DO MONTEIRO
CENTRO DE CIÊNCIAS HUMANAS E EXATAS
CURSO DE LICENCIATURA PLENA EM MATEMÁTICA

IZAMARA RAFAELA RAMOS

RECÍPROCAS PARA O TEOREMA DE LAGRANGE

MONTEIRO
2017

IZAMARA RAFAELA RAMOS

RECÍPROCAS PARA O TEOREMA DE LAGRANGE

Trabalho de Conclusão do Curso apresentado à coordenação do curso de Licenciatura em Matemática do Centro de Ciências Humanas e Exatas da Universidade Estadual da Paraíba, em cumprimento às exigências legais para a obtenção do título de Graduado no Curso de Licenciatura Plena em Matemática.

Área de concentração: Álgebra

Orientador: Prof. Me. Marciel Medeiros de Oliveira

MONTEIRO
2017

R175r Ramos, Izamara Rafaela.
Recíprocas para o teorema de Lagrange [manuscrito] : / Izamara Rafaela Ramos. - 2017.
43 p.

Digitado.
Trabalho de Conclusão de Curso (Graduação em Matemática) - Universidade Estadual da Paraíba, Centro de Ciências Humanas e Exatas, 2017.
"Orientação : Prof. Me. Marciel Medeiros de Oliveira, Coordenação do Curso de Matemática - CCHE."

1. Teorema de Lagrange. 2. Grupos cíclicos. 3. Teoria de grupos. 4. Teorema de Sylow.

21. ed. CDD 512.2

IZAMARA RAFAELA RAMOS

RECÍPROCAS PARA O TEOREMA DE LAGRANGE

Trabalho de Conclusão do Curso apresentado à coordenação do curso de Licenciatura em Matemática do Centro de Ciências Humanas e Exatas da Universidade Estadual da Paraíba, em cumprimento às exigências legais para a obtenção do título de Graduado no Curso de Licenciatura Plena em Matemática.

Área de concentração: Álgebra

Aprovada em: 12/12/2017.

BANCA EXAMINADORA

Marciel Medeiros de Oliveira

Prof. Me. Marciel Medeiros de Oliveira
Orientador

Luciano dos Santos Ferreira

Prof. Me. Luciano dos Santos Ferreira
Examinador interno (CCHE/UEPB)

Luiz Lima de Oliveira Junior

Prof. Me. Luiz Lima de Oliveira Junior
Examinador interno (CCHE/UEPB)

Dedico aos meus pais, Maria das Neves e José Ramos, a minha irmã Amara Isabel, ao meu noivo Verinaldo Aneas e a todos que de forma direta e indireta contribuiram com esse trabalho.

AGRADECIMENTOS

Agradeço primeiramente a Deus, que permitiu que esse ciclo fosse concluído, me dando saúde e coragem para sempre seguir em frente ao longo da minha vida, e não somente nestes cinco anos como universitária, mas que em todos os momentos é o maior mestre que alguém pode conhecer.

Ao meu noivo, Verinaldo Aneas de França, que durante esse tempo se dedicou de forma integral a minha caminhada na vida acadêmica, que sem medir esfoços fez tudo que estava ao seu alcance para torna possível cada momento, e sem sua ajuda, não teria conseguindo aqui chegar, só nos sabemos o quanto complicado foi. Meus sinceros agradecimentos.

A minha mãe Maria das Neves Ramos, que de forma sabia sempre me encorajou a buscar vôos cada vez mais altos e procurar na educação uma forma de buscar um futuro que me proporciona-se ser alguém que eu podesse me orgulhar. E sempre serei grata por tudo que abriu mão para permitir que esse curso fosse concluído.

Ao meu pai José Ramos Sobrinho, que quando pensei em desistir de estudar com apenas 4 anos, me ensinou com ações que a escola era a única chance de me levar a um lugar diferente de onde ele veio, e sem dúvidas aquele momento me fez ter coragem de ultrapassar cada obstáculo encontrado pelo caminho e sempre me superar diante das dificuldades.

A minha irmã Amara Isabel, que mesmo longe durante quase todo curso, sempre esteve ao meu lado, me proporcionando suavidade para nunca desistir diante de uma dificuldade.

A Patrícia Núbia, que desde 2013 se tornou uma irmã mais velha, permitindo que a caminhada acadêmica torna-se mais suave com sua presença, fazendo com que nunca vinhesse a desiste das coisas que desejo alcançar. Agradeço ainda, a Wanderley e Edielso que foram verdadeiros amigos durante todo o curso, sempre estando do meu lado.

Ao meu Orientador Marciel Medeiros, pelas horas dedicadas e por todos os ensinamentos durante o curso, e que mesmo passando por momentos difícies, na reta final deste trabalho, nunca deixou de orientar com todo carinho possível, me sinto grata por ter sido sua orientada, meus sinceros agradecimentos pelo belissimo professor que és.

Aos professores, Ana Emília, Brauner Coutinho e Robson Batista, que de forma simples me ensinaram mais que conceitos Matemáticos, sempre serei grata por cada palavra a me dirigida. Meus sinceros agradecimentos.

Agradeço ainda a banca examinadora, nas pessoas de, Luciano dos Santos e Luiz

Lima de Oliveira, que desde o início do curso sempre se fizeram presentes, e principalmente agradeço pelo carinho com este trabalho e pelas palavras a me proferidas, meus sinceros agradecimentos.

Em fim, agradeço a todos os funcionários da Universidade, em especial Gilmaria, da coordenação de Matemática, pelo carinho e por sempre torcer por nós, e aos demais que de forma direta ou indireta fizeram parte desta jornada.

E agora compreendo que os momentos de dificuldades foram necessários, mas vencemos e com o fim só nos restará saudades.

"A matemática do tempo é simples. Você tem menos do que pensa e precisa mais do que acha."
(Kevin Ashton)

RESUMO

O estudo acerca da estrutura de Grupos, se desenvolveu a partir da tentativa de verificar se as equações de grau maior ou igual a 3, eram resolúvel por radicais. E dentre os pesquisadores que se dedicaram a essa questão, *Joseph Louis Lagrange*(1736-1813) teve um grande destaque, principalmente com seu Teorema. Dessa forma, o objetivo deste trabalho é a formulação e demonstração de algumas recíprocas deste Teorema. Pra isso, inicialmente apresentamos conceitos preliminares sobre Grupo, como *Subgrupos, Grupos ciclícos, Subgrupo Normal e Grupo Quociente, Homomorfismo e Isomorfismo de grupos*, e de forma detalhada apresentamos o *Teorema de Lagrange* e sua demonstração. Mais adiante, expomos conteúdos mais aprofundados sobre a Teoria de Grupos para fornecer embasamento teórico para a obtenção das recíprocas, como por exemplo, o Primeiro Teorema de Sylow, p-subgrupos, Grupos Abelianos, Solúveis e Nilpotentes, e dessa forma apresentaremos quatro recíprocas, correspondentes a *p-grupos, Grupos Abelianos, Grupos Solúveis e Grupos Nilpotentes.*

Palavras-chave: Grupos. Teorema de Lagrange. Recíprocas do Teorema de Lagrange.

ABSTRACT

The study about the structure of Groups was developed from the attempt to verify if the equations of degree higher or equal to 3 were solvable by radicals. Among the researchers who devoted themselves to this issue, *Joseph Louis Lagrange* (1736-1813) had a great prominence, mainly due to his Theorem. Therefore, the aim of this work is to formulate and to demonstrate some reciprocals of this Theorem. To do so, we firstly present preliminary concepts about Group, such as *Subgroups, Cyclic Groups, Normal Subgroup and Quotient Group, Homomorphism and Isomorphism of groups*, and in a detailed way we present the *Lagrange's Theorem* and its demonstration. Further on, we present more in-depth content about Group Theory to provide theoretical background to obtain the reciprocals, such as Sylow's First Theorem, p-subgroups, Abelian Groups, soluble and nilpotent and, therefore, we will present four reciprocals, which correspond to *p-groups, Abelian Groups, Soluble Groups and Nilpotent Groups.*

Key-words: Groups. Lagrange's Theorem. Reciprocals of Lagrange's Theorem.

LISTA DE ILUSTRAÇÕES

SUMÁRIO

1 INTRODUÇÃO

A Teoria dos Grupos constitui um dos mais importantes instrumentos para a organização e o estudo de diversas partes da matemática e de outras áreas. Em nível mais elementar, pode-se citar a teoria das simetrias geométricas, que essencialmente associa cada figura a um grupo e este por sua vez retrata a simetria da figura.

Seguindo essa linha, um resultado muito importante na Teoria de Grupos finitos é o *Teorema de Lagrange*, o qual garante que em um grupo G de ordem finita a ordem de todos os subgrupos H de G, divide a ordem de G. Esse Teorema proporcionou o aprofundamento e importantes resultados nos estudos matemáticos, como por exemplo, no estudo dos grupos comutativos, o qual garante que todos os grupos com ordem até cinco é comutativo.

Porém, há uma questão importante acerca desse teorema, que diz respeito a validade de sua recíproca, ou seja, em qualquer grupo finito G, para cada divisor de sua ordem existirá um subgrupo H de G, cuja ordem será esse divisor? Esse questionamento em geral é falso, porém sob certas condições e para alguns grupos específicos essa recíproca é verdadeira.

Assim, neste trabalho o nosso objetivo é realizar a apresentação de algumas recíprocas para o *Teorema de Lagrange*, sendo uma recíproca fraca para Grupos Solúveis e três recíprocas fortes para p-grupo, Grupos Abelianos e Grupos Nilpotentes. As denominamos dessa forma por questão de organização, no qual chamamos de "fraca" a recíproca que não possui um caráter geral e de "forte" as recíprocas que possui.

Para alcançar nosso objetivo, utilizamos algumas referências, em especial, Garcia e Lequain (2012) e Vieira (2015), que desde o início foram as bases norteadores deste trabalho. Utilizamos ainda, Milies (2003), Fazzio e Watari (2009), Bhattacharia, Jain e Nagpaul (1995) e Silveira (2010).

O referido trabalho se encontra organizado em três capítulos, obedecendo a seguinte organização: No primeiro é apresentado alguns resultados preliminar da Teoria de Grupos, e de forma especial, é apresentado e demonstrado o *Teorema de Lagrange*. No segundo capítulo nos dedicamos a um estudo mais aprofundado sobre Grupos, no qual é apresentado o Primeiro Teorema de Sylow, a definição de p-subgrupos, de Grupos Solúveis e Nilpotentes, sendo ainda mostrado resultados sobre os grupos apresentados, e para finalizar, no último capítulo é apresentado a demonstração das recíprocas do *Teorema de Lagrange*.

2 CONCEITOS PRELIMINARES

Apresentaremos a seguir, definições e resultados sobre a Teoria de Grupos. Tal Teoria nasceu como resultado de pesquisas realizadas sobre a resolubilidade por radicais [1] de equações de grau maior que 3, recebendo, influência de diversos pesquisadores matemáticos, dentre estes podemos citar *Joseph-Louis Lagrange* (1736 - 1813) e *Evariste Galois* (1811 - 1832), que se dedicaram durante décadas a resolver tal questão.

2.1 Grupos

Definição 2.1. Um conjunto G não vazio munido de uma operação $*$

$$\begin{array}{ccc} G \times G & \longrightarrow & G \\ (a,b) & \longmapsto & a*b \end{array}$$

é um **grupo** quando as propriedades abaixo são satisfeitas:

G_1: A operação $*$ é associativa, ou seja, $a*(b*c) = (a*b)*c, \forall\ a,b,c \in G$.

G_2: Existe o elemento neutro para a operação, e é único, ou seja, $\exists\ e \in G$ tal que $a*e = e*a = a$, $\forall a \in G$.

G_3: Todo elemento em G é invertível em relação a operação $*$ dada, e cada elemento possui um único inverso, ou seja, $\exists\ a' \in G$ tal que $a*a' = a'*a = e$, $\forall a \in G$.

Satisfeito as condições acima, indicaremos o grupo por $(G,*)$. Quando não houver dúvidas sobre a operação utilizada, o indicaremos apenas por G. A operação do grupo irá mudar de acordo com o grupo considerado. Em geral, quando a operação for um **produto**, chama-se o grupo G de **multiplicativo**, e usamos ab ao invés de $a*b$.

De forma similar, quando a operação for **adição**, o grupo G é chamado de **grupo aditivo**. Assim, como forma de padronização, adotaremos em nosso trabalho a notação multiplicativa. Vale salientar ainda, que os resultados aqui mostrados também valem para a notação aditiva, com as devidas alterações.

Definição 2.2. Um grupo $(G,*\ )$ é dito **comutativo** ou **abeliano** quando $a*b = b*a$, $\forall a,b \in G$.

Os grupos comutativos recebem o nome *abelianos*, em homenagem ao matemático norueguês *Niels Henrik Abel*(1802-1829), que deixou diversas contribuições para a Mate-

[1] Uma equação é resolúvel por radical quando todas as suas raízes podem ser expressas através de uma fórmula escrita apenas com operações aritméticas e de radiciação.

mática, na qual a contribuição para à Álgebra abstrata é a mais notória, onde demonstrou de forma rigorosa a impossibilidade de resolver equações de quinto grau usando radicais.

Apresentaremos a seguir, algumas propriedades resultantes da definição de Grupos, nas quais algumas serão aceitas sem demonstração, podendo as mesmas serem encontradas em Vieira (2015). Esses resultados serão utilizados mais adiante, para o estudo de conceitos mais aprofundados que são de suma importância para o desenvolvimento desse trabalho.

Proposição 2.1. *Seja $(G, \cdot)$ um grupo. Assim as leis de cancelamento à direita e à esquerda são valídas em G, isto é, dados $a, b, c \in G$, teremos*

$$a \cdot b = a \cdot c \;\Rightarrow\; b = c \quad e \quad b \cdot a = c \cdot a \;\Rightarrow\; b = c.$$

Demonstração. Ver Vieira(2015, p. 176). ■

Proposição 2.2. *Seja $(G,\cdot)$ um grupo. Dados $a, b \in G$, as equações lineares*

$$a \cdot x = b \quad e \quad x \cdot a = b$$

tem soluções únicas em G.

Demonstração. Ver Vieira(2015, p. 176). ■

O elemento neutro da operação " $\cdot$ " em G é denominado de identidade de G. Além disso, se $\{G_i\}_{i\in A}$ é uma família de grupos, então e_i indicará a identidade de cada grupo G_i. Quanto ao elemento inverso, "a'" de a, o denotaremos de acordo com a operação do grupo. Ou seja, se o grupo for multiplicativo, o inverso é denotado por a^{-1}, caso seja aditivo o escreveremos por $-a$.

Proposição 2.3. *Em um grupo multiplicativo G, valem as seguintes condições:*

(1) $(a^{-1})^{-1} = a$, $\forall a \in G$.

(2) $(ab)^{-1} = b^{-1}a^{-1}$, $\forall a, b \in G$.

Demonstração. Ver Vieira(2015, p. 178). ■

O resultado do item (2) pode ser generalizado para mais de dois termos, ou seja, dados $a_1, a_2, ..., a_n \in G$,teremos:

$$(a_1 \cdot a_2 \cdot ... \cdot a_n)^{-1} = (a_n)^{-1} \cdot (a_{n-1})^{-1} \cdot ... \cdot (a_1)^{-1}$$

que é possível ser demonstrado por meio de indução matemática.

Um conceito importante ao nosso trabalho é o de ordem de um Grupo, o qual é atribuído ao matemático alemão *Georg Cantor*(1845-1918), que revolucionou a Teoria dos Conjuntos. Uma vez que com essa definição provou que os conjuntos $\mathbb{Z}$ e $\mathbb{R}$ apesar de

serem infinitos, não possuem a mesma cardinalidade[2], pois não existe nenhuma bijeção entre $\mathbb{Z}$ e $\mathbb{R}$.

Definição 2.3. Definimos a **ordem** de um grupo G como sendo a quantidade de elementos do conjunto G.

O grupo G é dito finito quando o conjunto G possui uma quantidade finita n de elementos e nesse caso escrevemos $|G| = n$, caso contrário G é dito grupo infinito.

Exemplo 2.1. Considere os grupos $(G_1, \cdot)$, $(G_2, \cdot)$,..., $(G_n, \cdot)$. Então o produto cartesiano

$$G_1 \times G_2 \times ... \times G_n = \{(x_1, x_2, ..., x_n) \ : \ x_i \in G_i, \ i = 1, 2, ..., n\}$$

com a operação

$$(x_1, x_2, ..., x_n) \cdot (y_1, y_2, ..., y_n) = (x_1 \cdot y_1, x_2 \cdot y_2, ..., x_n \cdot y_n)$$

é um grupo chamado de **Grupo de Produto Direto**.

Vale chamar a atenção que o grupo $G_1 \times G_2 \times ... \times G_n$ é abeliano se, e somente se, G_i é abeliano para cada $i = 1, 2, ..., n$.

Exemplo 2.2. Seja G um conjunto não vazio e S_G o conjunto de todas as permutações de G, isto é,

$$S_G = \{f : G \to G \text{ tal que } f \text{ é bijetora } \}.$$

É possivel verificar que $(S_G, \circ)$ é um grupo em que " $\circ$ " é a composição de funções e é chamado de **grupo das permutações sobre** G. Quando o conjunto $G = \{1, 2, ..., n\}$, então S_G será denotado por S_n e chamado de *grupo das permutações* de n elementos, sendo que a ordem de S_n será $n!$. Além disso, vale chamar atenção que S_n será abeliano somente quando $G = \{1\}$ ou $G = \{1, 2\}$.

2.2 Subgrupo

Às vezes é conveniente estudar um subconjunto H de um grupo G, com quantidades menores de elementos, sobre o qual o estudo do grupo G, em alguns casos, se torna realizável, de certa forma, quando utilizamos resultados obtidos sobre H de modo a obter informações importantes de G.

Mas, para que as propriedades de H seja refletida no grupo G, é necessário que H seja uma estrutura algébrica, uma vez que o conjunto G é. Nesse contexto, apresentamos a seguinte definição.

[2] Dois Conjuntos A e B tem a mesma Cardinalidade se, e somente se, existir uma Função Bijetora (Injetora e Sobrejetora) $f : A \to B$.

Definição 2.4. Seja G um grupo. Um subconjunto não vazio H de G é um **subgrupo** de G, $H < G$, quando H com a operação de G, também for um grupo.

Como forma de simplificar a verificação de que um dado subconjunto H de G é um subgrupo de G, estabelecemos o seguinte Teorema:

Teorema 2.1. *Seja H um subconjunto não vazio de G. Então, H é um subgrupo de G se, e somente se, uma das condições a seguir for satisfeita:*

(1) $h_1h_2 \in H$ *e* $h^{-1} \in H$, $\forall h_1, h_2 \in H$.

(2) $h_1h_2^{-1} \in H$, $\forall h_1, h_2 \in H$.

Demonstração. Considere inicialmente que H é um subgrupo de G, então pela Definição 2.4, H será um grupo, e assim as condições (1) e (2) são satisfeitas.

Reciprocamente, suponha que H satisfaz a condição (1). Ou seja, dados $h_1,\ h_2 \in H$, teremos que $h_1h_2 \in H$ e $h^{-1} \in H$. Assim, $e = hh^{-1} \in H$, sendo assim $H < G$. Considere por fim, que H satisfaz a condição (2), então dados $h_1, h_2 \in H$, temos que

$$e = h_2h_2^{-1} \in H.$$

Operando pela direita com h_2^{-1}, teremos

$$h_2^{-1} = eh_2^{-1} \in H.$$

Com isso,

$$h_1h_2 = h_1(h_2^{-1})^{-1} \in H.$$

Portanto, H é subgrupo de G. ■

Como $H \subset G$, temos que o elemento neutro e_H e o inverso de h em H é necessariamente igual ao elemento neutro e de G e igual ao inverso de h em G, respectivamente. Por definição temos que um subgrupo qualquer é necessariamente um grupo, em que os dois itens apresentados no Teorema 2.1 se tornam válidos. Porém, quando H for um subconjunto finito podemos simplificar o processo, de acordo com o seguinte Teorema:

Teorema 2.2. *Sejam G um grupo e H um subconjunto finito não vazio de G. Então*

$$H < G \ \Leftrightarrow\ h_1h_2 \in H, \quad \forall h_1, h_2 \in H.$$

Demonstração. Seja H um subgrupo de G, assim pelo Teorema 2.1, $h_1h_2 \in H$, para quaisquer $h_1, h_2 \in H$. De forma recíproca por meio do mesmo Teorema, se $h_1, h_2 \in H$, basta mostrar que $h^{-1} \in H$, $\forall h \in H$.

Assim, suponhamos que H contenha n elementos, então por hipótese, dado $h \in H$, os elementos $h, h^2, h^3, ..., h^{n+1}$ pertencem a H, em que pelo menos dois serão iguais, pois caso contrário, H não teria n elementos. Por isso, existem $i, j \in \{1, 2, ..., n, n+1\}$, com $i < j$, tais que

$$h^j = h^i.$$

Multiplicando ambos os membros por h^{-i},teremos

$$h^j h^{-i} = h^i h^{-i} \Rightarrow h^{j-i} = e \in H.$$

Operando com h^{-1}, obtemos:

$$eh^{-1} = h^{j-i}h^{-1} \Rightarrow h^{-1} = h^{j-i-1} \in H \ .$$

Portanto, H é subgrupo de G. ■

Observação 2.1. Temos que G e $\{e\}$ são sempre subgrupos de G, chamados de *subgrupos triviais*, os demais subgrupos H, no qual $H \neq \{e\}$ e $H \neq G$ são chamados de *subgrupos próprios ou não triviais.*

Um exemplo importante de subgrupo é o centro de G, o qual apresentamos a seguir.

Exemplo 2.3. Considere um grupo G qualquer e $Z(G)$ um subconjunto de G, cujos elementos comutam com todo elemento de G, ou seja,

$$Z(G) = \{a \in G : xa = ax, \forall x \in G\}.$$

É possível verificar que esse conjunto definido dessa forma é um subgrupo de G, chamado de *centro* de G, além disso $Z(G)$ é um grupo abeliano de G.

De forma particular alguns subgrupos podem ser formados a partir de outros subconjuntos, que não são necessariamente subgrupos. Então como forma de facilitar a verificação nesses casos, estabeleceremos as seguintes proposições.

Proposição 2.4. *Se H_1 e H_2 são subgrupos de G. Então $H_1 \cap H_2$ é um subgrupo de G.*

Demonstração. Ver Vieira (2015, p. 195) ■

Se H e K são subconjuntos de G, de forma particular subgrupos. O conjunto $\{hg : h \in H \text{ e } k \in K\}$ será denotado por HK. De forma geral, esse conjunto não é um subgrupo de G. Porém, em alguns casos particulares isso se torna verdadeiro, onde apresentaremos a seguir alguns desses casos.

Proposição 2.5. *Sejam H e K subconjuntos não vazios de um grupo G. Então HK é um subgrupo de G se, e somente se, $HK = KH$.*

Demonstração. Ver Vieira (2015, 196). ■

Como consequência da proposição temos,

Corolário 2.1. Se H e K são subgrupos de um grupo abeliano G, então HK é um subgrupo de G.

2.3 Grupos Cíclicos

Sejam G um grupo e $a \in G$. Consideremos H o conjunto de todas as potências de a,

$$H = \{a^n : n \in \mathbb{Z}\}. \tag{2.1}$$

Mostraremos que $H < G$. Note que $H \neq \phi$, pois $a^0 = e \in H$. Considere $h_1, h_2 \in H$, em que $h_1 = a^{n_1}$ e $h_2 = a^{n_2}$, com $n_1, n_2 \in \mathbb{Z}$, pelo Teorema 2.1, verificaremos se o item (2) é satisfeito. Temos:

$$h_1 h_2^{-1} = a^{n_1} a^{-n_2} = a^{n_1 - n_2} \in H, \text{ pois } n_1 - n_2 \in \mathbb{Z}.$$

Portanto, H é um subgrupo de G, chamado **subgrupo cíclico gerado por** a, o qual denotaremos por,

$$H = \langle a \rangle$$

e dizemos que a é um **gerador** de H.

Definição 2.5. Um grupo G é dito **cíclico** se existir $a \in G$ tal que

$$G = \langle a \rangle.$$

Observação 2.2. Para um grupo cíclico $G = \langle a \rangle$ há duas possibilidades:

(a) $a^n = e$ para algum $n \in \mathbb{N}$. Neste caso, G tem ordem finita.

(b) $a^n \neq e$ para todo $n \in \mathbb{N}$. Neste caso, todas as potências de a são distintas e G tem ordem infinita.

Proposição 2.6. *Todo grupo cíclico é abeliano.*

Demonstração. De acordo com a Definição 2.2, para que o grupo G seja abeliano, teremos que mostrar que dados $x_1, x_2 \in G$, temos $x_1 x_2 = x_2 x_1$. Sendo assim, considere G um grupo e $a \in G$ tal que,

$$G = \langle a \rangle = \{a^n : n \in \mathbb{Z}\}.$$

Dados $x_1, x_2 \in G$, da forma $x_1 = a^{n_1}$ e $x_2 = a^{n_2}$,

$$x_1 x_2 = a^{n_1} a^{n_2} = a^{n_1+n_2} = a^{n_2+n_1} = a^{n_2} a^{n_1} = x_2 x_1.$$

Logo, G é abeliano. ■

Definição 2.6. Sejam G um grupo e $a \in G$. Se existir $n \in \mathbb{N}$ tal que $a^n = e$, dizemos que o elemento a tem **ordem finita**. Neste caso, o menor inteiro positivo m tal que $a^m = e$ será a **ordem** de a, a qual denotaremos por O(a). Caso não exista nenhum $n \in \mathbb{N}$ satisfazendo tal propriedade, então o elemento a é dito ser de **ordem infinita**.

Teorema 2.3. *Sejam G um grupo e $a \in G$.*

(1) Se $a^n = e$ para algum $n \in \mathbb{N}$, então $O(a)$ divide n.

(2) Se $O(a)=m$, então para qualquer $k \in \mathbb{Z}$, $a^k = a^r$, sendo r o resto da divisão de k por m.

(3) $O(a)=m$ se, e somente se, $\langle a \rangle$ tem ordem m.

Demonstração. Provando os itens acima temos:

(1) Como $a^n = e$, pela Definição 2.6, a tem ordem finita. Então considere $O(a) = m$. Pelo algoritmo da divisão é garantido a existência de $q, r \in \mathbb{Z}$ tais que $n = mq + r$, com $0 \leq r < m$. Logo

$$e = a^n = a^{mq+r} = a^{mq} a^r = (a^m)^q a^r = e^q a^r \Rightarrow a^r = e.$$

Como $O(a) = m$, então m é o menor inteiro, sendo assim $r = 0$ e portanto $n = mq$, dividindo então a ordem de a.

(2) Bastar verificar o caso provado no item anterior, onde para cada $k \in \mathbb{Z}$, $k = mq + r$, com $q, r \in \mathbb{Z}$ e $0 \leq r < m$, o que levará a $a^k = a^r$.

(3) Se $O(a) = m$, segue que os elementos $e, a, a^2, ..., a^{m-1}$ são todos distintos. Pois caso contrário, se $a^i = a^j$ para $0 \leq i < j \leq m-1$, então $a^i a^{-j} = a^j a^{-j} = a^{j-j} = a^0 = e \Rightarrow a^{i-j} = e$ e $j - i < m$, o que é uma contradição uma vez que $O(a) = m$.

Agora seja $H = \langle a \rangle$. Pelo item (2), temos que dado $k \in \mathbb{Z}, a^k = a^r$, sendo $r \in \{0, 1, ..., m-1\}$. Assim,

$$H = \langle a \rangle = \{a^k : k \in \mathbb{Z}\} = \{a^r : r = 0, 1, ..., m-1\}$$

onde $H = \langle a \rangle$ tem ordem m.

De forma recíproca, suponhamos que $H = \langle a \rangle$ tem ordem finita. Isso nos diz que as potências $a^i \in \mathbb{Z}$, não podem ser todas distintas. Assim, existem $i, j \in \mathbb{Z}$, com $i < j$, de maneira que $a^i = a^j$, como já mencionamos $a^{i-j} = e$. Mas, isso implica que a tem ordem finita, digamos $O(a) = m$. Desde que, os elementos $e, a, a^2, ..., a^{m-1}$ são todos distintos, temos que,

$$H = \langle a \rangle = \{a^k : k \in \mathbb{Z}\} = \{a^r : r = 0, 1, ..., m-1\}$$

ou seja, $O(H) = m$.

■

2.4 Classes Laterais

Sejam G um grupo e H um subgrupo de G. Sobre G, vamos considerar a relação " $\equiv_E (modH)$" dada, para quaisquer $a, b, \in G$, por

$$a \equiv_E b(modH) \;\Rightarrow\; a^{-1}b \in H.$$

As vezes, indicaremos a relação apenas por " $\equiv_E$ " quando não houver dúvidas quanto ao subgrupo H utilizado. Podemos verificar ainda, que a relação $\equiv_E (modH)$ é de equivalência. Além disso, a classe de equivalência de um elemento $g \in G$, relativa a esta relação, é dada por $\{gh : h \in H\}$. De forma bem sugestiva, vamos denotar a classe $\overline{g}$ de um elemento $g \in G$ segundo a relação $\equiv_E (modH)$ por gH, a qual chamaremos de forma especial de **classe lateral de g à esquerda**. Assim,

$$gH = \{gh : h \in H\}.$$

De forma análoga, temos que a relação $\equiv_D (modH)$ sobre G, dada para quaisquer $a, b \in G$, por

$$a \equiv_D b(modH) \Rightarrow ab^{-1} \in H$$

é de equivalência. E ainda, para cada $g \in G$, a classe de equivalência de g segundo a relação é $\overline{g} = \{hg : h \in H\}$, a qual denotaremos por:

$$Hg = \{hg : h \in H\}$$

e chamaremos de **classe lateral de g à direita**.

Como essas classes são de equivalência, decorre que o grupo G é formado pela união de todas as suas classes laterais, ou seja,

$$G = \bigcup_{g \in G} gH \tag{2.2}$$

e ainda podemos observar que para $x, y \in G$, teremos que suas classes laterais são iguais ou disjuntas, ou seja,

$$xH = yH \quad \text{ou} \quad xH \cap yH = \phi.$$

Desse modo, denotaremos por H_E o conjunto de todas as classes laterais à esquerda de H,

$$H_E = \{gH : g \in G\} = G/\equiv_E.$$

Com modificações convenientes, temos que $H_D = \{Hg : g \in G\} = G/\equiv_D$. E ainda, H_E e H_D são partição de G.

Observação 2.3. E importante ressaltar que:

(a) Se G é um grupo abeliano, então para cada $g \in G$, temos

$$gH = \{gh : h \in H\} = \{hg : h \in H\} = Hg.$$

Dessa forma, o conjunto das classe lateral à direita, H_D, de g coincide com a classe lateral à esquerda, H_E. Para grupos não abelianos não podemos mais afirmar que as classes laterais coincidem, pois em geral teremos $H_E \neq H_D$.
(b) O subgrupo H é ele próprio uma classe lateral de H tanto à esquerda quanto à direita, pois

$$eH = \{eh : h \in H\} = H = \{he : h \in H\} = He.$$

(c) Para $g \in G$,

$$gH = H \Leftrightarrow gH = eH \Leftrightarrow g \equiv_E e \Leftrightarrow g^{-1}e \in H \Leftrightarrow g \in H.$$

Similarmente,

$$Hg = H \Leftrightarrow g \in H.$$

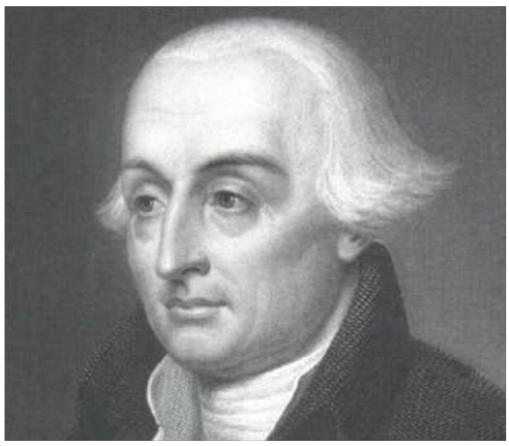
Definição 2.7. Sejam G um grupo e H um subgrupo de G. A cardinalidade do conjunto H_E(a mesma de H_D) chama-se **índice** de H em G, o qual será indicado por $(G : H)$.

O índice $(G : H)$ pode ser finito ou infinito. Se o grupo G for finito, então o índice claramente é finito, pois os elementos da classe são subconjuntos de G. Ainda podemos ter, um grupo G infinito no qual possua um subgrupo $H \neq G$, onde o índice será finito, também pode ocorrer que nesse grupo tenha um subgrupo $K \neq G$, de maneira que o índice seja infinito.

2.5 Teorema de Lagrange

Joseph Louis Lagrange(1736-1813) foi um matemático e físico-matemático italiano, que juntamente com *Leonhard Euler*(1707-1783), foi um dos grandes matemáticos do Século XVIII. Seu objetivo principal na Matemática não era apenas adicionar mais aplicações do cálculo de *Newton* e *Leibniz* a lista já existente. Mas sim, revisar seus fundamentos e oferecer uma explicação mais rigorosa do " por quê " e de como o cálculo funciona. *Lagrange* acreditava que explicações conceituais ou intuitivas não tinham lugar em uma demonstração rigorosa, dai o esforço de reduzir os fundamentos de cálculo à álgebra.

Figura 1 – *Joseph Louis Lagrange*



Fonte: Google

Um resultado desse pensamento, é um dos mais importantes Teoremas existentes na Teoria de Grupos, o *Teorema de Lagrange*. Esse teorema é fruto de décadas de pesquisas dedicadas a obter resposta ao que o matemático italiano *Scipione del Ferro* lançou aos algebristas entre os anos de 1500 e 1515, que consistia em provar se as equações de grau maior ou igual a 3 eram resolúvel por radicais. *Lagrange* desenvolveu as primeiras ideias acerca dessa questão, porém foi *Abel* que conseguiu pela primeira vez provar que de forma geral, essas equações não podem ser resolvidas por radicais. O teorema seguir é a base da teoria dos grupos finitos.

Teorema 2.4. *(**Teorema de Lagrange**) Sejam G um grupo finito e H um subgrupo de G. Então, a ordem de H divide a ordem de G. Especificamente,*

$$|G| = |H| \cdot (G : H)$$

Demonstração. Por G ser finito, temos que $(G : H)$ também será. Suponha que $(G : H) = r$. Considere $H_E = \{a_1H, a_2H, ..., a_rH\}$. Como H_E é um partição de G,

$$G = a_1H \cup a_2H \cup ... \cup a_rH,$$

e ainda, $a_iH \cap a_jH = \phi$ para $i \neq j$. Desse modo, considerando o fato de que a cardinalidade de cada classe H_E é igual a ordem de H, obtemos

$$|G| = |H| + |H| + ... + |H| = |H| \cdot r.$$

em que $|H|$ se repeti r vezes. Logo, $|G| = |H| \cdot (G : H)$. ■

Em posse deste Teorema, podemos verificar facilmente se um dado subconjunto de G é um subgrupo. Por exemplo, dado o subconjunto $K = \{\bar{0}, \bar{2}, \bar{4}\}$ de $G = \mathbb{Z}_8$, com ordem igual a 3, teremos segundo o *Teorema de Lagrange* que K não é um subgrupo de G, pois 3 não divide 8. Porém, será que para todo divisor m da ordem de G, é garantido a existência de um subgrupo de ordem m ?

Em geral a resposta é não. Como é o caso do grupo das permutações pares A_5[3], que possui ordem igual a 60, pois $|A_5| = \frac{n!}{2} = \frac{5!}{2} = \frac{120}{2} = 60$. Porém não possui nenhum subgrupo com ordem $15, 20$ ou 30. Mas de certa forma, determinados grupos estabelecem condições nas quais se torna possível estabelecer essa recíproca, como veremos um pouco mais adiante.

De forma preliminar, estabeleceremos algumas aplicações elementares desse Teorema, que de forma geral facilita a análise da estrutura dos grupos.

Corolário 2.2. Sejam G um grupo finito e $g \in G$. Então, a $O(g)$ divide $|G|$. Em particular

$$g^{|G|} = e.$$

Demonstração. Ver Vieira(2015, p. 238). ■

Corolário 2.3. Todo grupo G de ordem prima é ciclíco. Em particular, G é abeliano.

Demonstração. Ver Vieira(2015, p. 238). ■

2.6 Subgrupos Normais e Grupos Quocientes

Como vimos na Seção 2.4, dado um grupo G não abeliano, temos que suas classes laterais serão diferentes, ou seja, $H_E \neq H_D$. Como podemos perceber nas classes do grupo

[3] Sobre este grupo daremos mais detalhes no próximo capítulo.

S_3. Sendo assim, nessa seção buscaremos estabelecer condições de forma a possibilitar a igualdade entre as classes laterais de um determinado grupo.

Proposição 2.7. *Seja H um subgrupo de G. As afirmações seguintes são equivalentes:*

(1) a operação definida sobre as classes laterais á esquerda de H em G é bem definida.

(2) $gHg^{-1} \subseteq H, \quad \forall g \in G$

(3) $gHg^{-1} = H, \quad \forall g \in G$

(4) $gH = Hg, \quad \forall g \in G$

Demonstração. Mostraremos apenas a equivalência entre os itens (1) e (2). Dada a operação

$$(xH, yH) \vdash xyH$$

verificaremos, inicialmente, se ela está bem definida. Assim, dados $x, y \in G$ e $h, k \in H$ quaisquer, então x e xh são representantes da mesma classe xH, como também y e yk são representantes da mesma classe yH. Assim, a operação induzida sobre as classes laterais à esquerda é bem definida se, e só se

$$xyH = xhykH, \quad \forall x, y \in G, \quad \forall h, k \in H$$

se, e somente se

$$y^{-1}x^{-1}xyH = y^{-1}x^{-1}xhykH$$

ou seja,

$$H = y^{-1}hyH, \quad \forall y \in G, \quad \forall h \in H$$

e portanto se, e somente se,

$$ghg^{-1} \in H, \quad \forall g \in G, \quad \forall h \in H.$$

■

Definição 2.8. Um subgrupo H é um **subgrupo normal** em G, $H \triangleleft G$, se ele satisfaz as afirmações equivalentes da proposição acima. Neste caso, as classes laterais à esquerda da H são iguais às classes laterais à direita de H.

Sendo assim, quando H for um subgrupo normal de G, representaremos os conjuntos das classes laterais(H_E ou H_D) por G/H, isto é,

$$G/H = \{gH : g \in G\}.$$

Como vimos na Seção 2.2, existe uma condição para se verificar se dados dois subgrupos, operados ou multiplicados entre si, o resultado ainda é um subgrupo. Com a definição de subgrupo normal, essa verificação se torna mais acessível, e podemos estabelecer a seguinte proposição.

Proposição 2.8. *Sejam H e K subgrupos de um grupo G. Se H ou K for normal em G, então HK é um subgrupo de G.*

Demonstração. Ver Vieira(2015, p.246). ■

Proposição 2.9. *Se H é um subgrupo de um grupo G tal que $(G : H) = 2$, então $H \triangleleft G$.*

Demonstração. Ver Vieira(2015, p. 248). ■

A proposição acima é uma boa ferramenta quando se deseja determinar subgrupos normais de um grupo finito, mesmo considerando o fato de ser um resultado um tanto quanto restrito.

Teorema 2.5. *Seja G um grupo e seja H um subgrupo normal de G. Então o conjunto das classes laterais, com a operação induzida de G, é um grupo.*

Demonstração. Ver Garcia e Lequain(2012, p. 155). ■

Definição 2.9. Sejam G um grupo e H um subgrupo normal de G. O grupo de suas classes laterais, com a operação induzida de G, é chamado de **grupo quociente** de G por H e será denotado por G/H.

Observação 2.4. Dados o grupo G e o subgrupo H de G, podemos estabeler uma relação entre a ordem de H e a ordem do grupo quociente G/H. No qual pelas Definições 2.7 e 2.9, temos que $|G/H| = (G : H)$, sendo assim a ordem de G, é dada por $|G| = |H|.(G : H)$.

Agora apresentaremos resultados que caracterizem esse grupo, facilitando as análises.

Proposição 2.10. *Sejam G um grupo e $H \triangleleft G$.*

(1) Se G é abeliano, então G/H é abeliano.

(2) Se G é cíclico, então G/H é cíclico.

Demonstração. Ver Vieira(2015, p. 254). ■

Vimos que dado um grupo G qualquer o centro de G, o qual denotamos por $Z(G)$ é um subgrupo de G. E é muito mais do que isso, $Z(G)$ é um sugrupo normal de G. Assim, podemos estabelecer a proposição seguinte.

Proposição 2.11. *Seja G um grupo e seja $Z(G)$ seu centro. Se o quociente $G/Z(G)$ é cíclico, então $Z(G) = G$. Em particular, o índice de $Z(G)$ em G nunca é igual a um número primo.*

Demonstração. Ver Garcia e Lequain(2012, p. 155). ■

2.7 Homomorfismo de Grupos

Definição 2.10. Sejam $(G_1, \cdot)$ e $(G_2, \times)$ dois grupos. Uma função $f : G_1 \to G_2$ é um **homomorfismo** se ela é compatível com as estruturas dos grupos, isto é, se

$$f(a \cdot b) = f(a) \times f(b), \forall a, b \in G_1. \tag{2.3}$$

A definição de homomorfismo de grupos, vem facilitar o estudo de certos grupos, pois, em alguns casos esse estudo se torna complicado devido sua estrutura, e quando definimos um homomorfismo entre o grupo e outro já conhecido, facilita o estudo do mesmo. Assim, se torna necessário apresentar algumas observações sobre homomorfismo de grupos.

Proposição 2.12. *Seja $f : G_1 \to G_2$ um homomorfismo de grupos. Então:*

(1) $f(e_{G_1}) = e_{G_2}$.

(2) $f(x^{-1}) = f(x)^{-1}, \forall\ x \in G_1$.

*(3) $kerf := \{x \in G_1 : f(x) = e_{G_2}\}$ é um subgrupo normal de G_1 chamado **núcleo** do homomorfismo f.*

*(4) $Im(f) := \{y \in G_2 : y = f(g)$ para algum $g \in G_1\}$ é um subgrupo de G_2, chamado de **imagem** de f.*

(5) $kerf = \{e_{G_1}\} \Leftrightarrow f$ é injetiva.

Demonstração. Aqui demonstraremos apenas os itens (3) e (5), as demais podem ser encontrados em Vieira(2015, p. 262).

(3) Inicialmente analisaremos se $kerf < G_1$. De fato, dados $x, y \in kerf$, sendo f um homomorfismo temos:

$$f(x \cdot y) = f(x) \times f(y) = e_{G_2} \times e_{G_2} = e_{G_2} \quad \text{e} \quad f(x^{-1}) = f(x)^{-1} = {e_{G_2}}^{-1} = e_{G_2}$$

Logo, $kerf < G_1$. Agora, só nos falta mostrar que $kerf \triangleleft G_1$, para isso provaremos que

$$gxg^{-1} \in kerf, \quad \forall g \in G_1 \quad \text{e} \quad \forall x \in kerf.$$

De fato,

$$f(gxg^{-1}) = f(g) \times f(x) \times f(g^{-1}) = f(g) \times e_{G_2} \times f(g^{-1}) = f(g) \times f(g^{-1}) = e_{G_2}$$

Portanto, $kerf$ é um subgrupo normal de G_1.

(5) Consideremos inicialmente que $kerf = \{e_{G_1}\}$, e sejam $x_1, x_2 \in G_1$. Assim,

$$\begin{array}{rcll} f(x_1) = f(x_2) & \Rightarrow & f(x_1) \times f(x_2)^{-1} & = e_{G_2} \\ & \Rightarrow & f(x_1) \times f({x_2}^{-1}) & = e_{G_2} \\ & \Rightarrow & f(x_1 {x_2}^{-1}) & = e_{G_2}. \end{array}$$

Porém, como $f(x_1{x_2}^{-1}) = e_{G_2}$, implica que $x_1{x_2}^{-1} \in kerf = \{e_{G_1}\}$, assim $x_1{x_2}^{-1} = e_{G_1}$, ou seja, $x_1 = x_2$, e portanto f é injetiva. De forma recíproca, dado $x \in G_1$, temos que

$$x \in kerf \Leftrightarrow f(x) = e_{G_2} = f(e_{G_1}).$$

Por hipótese, temos que f é injetiva, assim $f(x) = f(e_{G_1})$ nos diz que $x = e_{G_1}$, e por consequência, $kerf = \{e_{G_1}\}$. Como queriamos provar. ■

Um tipo especial de homomorfismo é o chamado *homomorfismo canônico*, onde dado $H \triangleleft G$ e $f : G \to G/H$ temos $f(g) = gH$.

Definição 2.11. Um homomorfismo de grupos $f : G_1 \to G_2$ bijetivo recebe o nome de **isomorfismo**. Em particular, um isomorfismo $f : G \to G$ denomina-se **automorfismo** de G.

Quando existe um isomorfismo entre dois grupos G_1 e G_2, dizemos que são isomorfos e denotamos por $G_1 \simeq G_2$. Para um grupo G qualquer, indicaremos por $Aut(G)$ o conjunto formado por todos os automorfismo de G, onde será um grupo com a operação composição de funções, isto é,

$$Aut(G) = \{f : G \to \text{G tal que } f \text{ é automorfismo}\}.$$

De forma particular, um automorfismo induzido de um elemento fixo g do grupo G através de uma conjugação, no qual,

$$\begin{array}{rcll} T_g : G & \Rightarrow & G & \\ x & \Rightarrow & T_g(x) & = x^g = g^{-1}xg \end{array}$$

é comumente chamado de *automorfismo interno induzido por g*. E será indicado por $In(G)$ no qual é um subgrupo normal de $Aut(G)$.

$$In(G) = \{T_g : g \in G\}$$

Proposição 2.13. *Sejam $f : G_1 \to G_2$ um homomorfismo de grupos e $g \in G_1$. Suponhamos que $O(g)$ é finita. Então, $O(f(g))$ divide $O(g)$. Em particular, sendo f injetora, tem-se que $O(g) = O(f(g))$.*

De acordo com que foi apresentado até aqui, um homomorfismo de grupos $f : G_1 \to G_2$ conduz a um grupo quociente natural, $G_1/kerf$, isso porque pelo item (3) da Proposição 2.12, $kerf$ é um subgrupo normal de G_1.

3 GRUPOS DE PERMUTAÇÕES

Arthur Cayley, matemático Inglês, desenvolveu pesquisas em várias partes da Álgebra, e uma das suas principais contribuições está no Teorema que leva seu nome. O mesmo afirma que todo grupo G é isomorfo a um grupo de permutações, especificamente, é isomorfo a um subgrupo de S_G.

Embora seu resultado não nos permita classificar todos os grupos, ele nos aponta o ambiente em que as informações dos grupos a princípio devem ser estudadas. O mesmo também evidência a importância dos grupos de permutações.

Lema 3.0.1. *Seja G um grupo. Para cada $g \in G$, a função $f_g : G \to G$ dada por $f_g(x) = gx, \forall x \in G$, é uma permutação de G, isto é, f_g[1] $\in S_G$.*

Demonstração. Ver Vieira(2015, p. 275). ■

Teorema 3.1 (***Teorema de Cayley***)**.** *Todo grupo G é isomorfo a um grupo de permutações.*

Demonstração. Consideremos S_G o grupo das permutações de G e a aplicação

$$\begin{array}{ccccc} F : G & \longrightarrow & S_G & & \\ g & \longmapsto & F(g) = & f_g = & gx. \end{array} \tag{3.1}$$

Utilizando o Lema 3.0.1, notemos inicialmente que para $a, b \in G$,

$$f_{ab}(x) = abx = f_a(bx) = f_a(f_b(x)) = (f_{ab})(x),$$

de maneira que $f_{ab} = f_a f_b$. Portanto,

$$F(ab) = f_{ab} = f_a f_b = F(a)F(b),$$

isso nos diz que F é um homomorfismo de grupo. Agora,

$$F(a) = F(b) \;\Rightarrow\; f_a = f_b \;\Rightarrow\; ax = bx, \;\; \forall x \in G.$$

Mas, em G, a igualdade $ax = bx$ implica em $a = b$, isto é, F é injetora. Por conseguinte $F_1 : G \to F(G)$ dada por $F_1(g) = F(g)$ para todo $g \in G$, é um homomorfismo injetivo. Naturalmente, F_1 é sobrejetora e assim, é bijetora. Logo, F_1 é um isomorfismo, e como $F_1(G) = F(G)$, segue que $G \simeq F(G) < S_G$. ■

[1] denominamos de *translação à esquerda definida por g.*

Definição 3.1. Uma permutação $\alpha \in S_n$ é denominado de **r-ciclo** ou **ciclo de comprimento** r quando existem elementos distintos $a_1, a_2, ..., a_r \in I_n$ tais que

$$\alpha(a_1) = a_2, \alpha(a_2) = a_3, ..., \alpha(a_{r-1}) = a_r, \alpha(a_r) = a_1$$
$$\alpha(i) = i, \forall i \in I_n - \{a_1, a_2, ..., a_r\}$$

Em particular, os 2-ciclos são também chamados de **transposição**.

E comum representar uma permutação $\alpha \in S_n$ por

$$\alpha = \begin{pmatrix} 1 & 2 & ... & n \\ \alpha(1) & \alpha(2) & ... & \alpha(n) \end{pmatrix}. \tag{3.2}$$

Definição 3.2. Se $\alpha \in S_n$, e $i \in I_n$, diz-se que α **move** i quando $\alpha(i) \neq i$, e dizemos que α **fixa** i quando $\alpha(i) = i$.

Se $\alpha \in S_n$ for um ciclo, o cálculo de sua ordem é realizado de forma direta, pois ela é igual ao comprimento do ciclo. Sendo assim, dado um *r-ciclo* em S_n, temos que sua ordem é r.

Definição 3.3. Seja $\alpha \in S_n$ um r-ciclo e seja $\beta \in S_n$ um s-ciclo. As permutações α e β são ditas **disjuntas** se nenhum elemento de $\{1, 2, ..., n\}$ é movido por ambas, isto é, $\forall a \in \{1, 2, ..., n\}$, temos que $\alpha(a) = a$ ou $\beta(a) = a$.

De forma equivalente, dados $\alpha = \{a_1, a_2, ..., a_n\}$ e $\beta = \{b_1, b_2, ..., b_n\}$, dizemos que α e β são disjuntos se $\{a_1, a_2, ..., a_n\} \cap \{b_1, b_2, ..., b_n\} = \phi$. Quando for dito que $\alpha_1, \alpha_2, ..., \alpha_n$ são ciclos disjuntos, significa dizer que eles são disjuntos aos pares.

E como veremos a seguir, todas as permutações $\alpha \in S_n - \{e\}$ pode ser escrita como produto de ciclos disjuntos. Assim segue o seguinte Teorema:

Teorema 3.2. *Toda permutação $\alpha \in S_n$ pode ser escrita como um produto de ciclos disjuntos aos pares. Além disso, esta fatoração é única, a menos da ordem dos fatores.*

Demonstração. Ver Vieira(2015, p. 297). ■

De forma particular, a partir desse teorema podemos também garantir o seguinte corolário.

Corolário 3.1. Toda permutação $\alpha \in S_n$ pode ser escrita como produto de transposições.

Definição 3.4. Uma permutação $\alpha \in S_n$ é **par** se α pode ser escrita como um produto de um número par de transposições, caso α for **ímpar** significa que α pode ser escrita como um produto de um número ímpar de transposições.

Assim, denotaremos por A_n o conjunto de todas as permutações pares de S_n. Se $\alpha, \beta \in A_n$, então é imediato que $\alpha\beta$ também está em A_n, desde que A_n seja um subconjunto finito e fechado sobre S_n. Então pelo Teorema 2.2, tem-se que $A_n < S_n$, o qual possui ordem $|A_n| = \frac{n!}{2}$. E chamaremos A_n de **grupo alternado de grau** n ou **grupo das permutações pares de grau** n.

Definição 3.5. Seja G um grupo finito. Definimos em G a relação R abaixo:

$$\forall x, y \in G, xRy \Leftrightarrow \exists g \in G \text{ tal que } y = gxg^{-1}.$$

A relação R, é chamada de **relação de conjugação** e a mesma é de equivalência em G. Essas classes de equivalência são chamadas de **classes de conjugação** de G, e dessa forma se $x \in G$, a classe de conjugação que contém x é o conjunto

$$C\ell(x) := \{gxg^{-1} : g \in G\}.$$

De acordo com a definição, note que dois elementos de S_n são conjugados em S_n se, e somente se, eles tem o mesmo tipo de decomposição, e de forma particular os conjuntos das transposições e dos 3-ciclos são classes de conjugação de S_n.

Adotaremos a seguir, uma nova maneira de estudar a estrutura de grupos, para a qual dados dois grupos G_1 e G_2 e se $f : G_1 \to G_2$ é um homomorfismo, é esperado que algumas propriedades de G_1 possam ser transportadas para G_2 via o homomorfismo f. E o mesmo poderá ocorrer, caso G_2 seja um grupo de permutações ou de matrizes invertíveis, onde algumas de suas propriedades poderá ser trazida de volta para o grupo G_1.

3.1 Representação de Grupos por Permutação

A ideia é a de se estudar um grupo G_1 *via um outro grupo* G_2 e um homomorfismo f. Ou seja, dado um grupo G_1, uma *representação* de G_1 é um homomorfismo f de G_1 em algum grupo G_2. Estudaremos aqui apenas as representações de um grupo G por permutações de um conjunto. E dessa forma, tentaremos descobrir o máximo de sua estrutura, seguindo alguns tópicos específicos, como: *Existência de subgrupos de uma ordem dada, a quantidade de tais subgrupos e a relação entre eles.*

Definição 3.6. Sejam G um grupo, C um conjunto e $P(C)$ o grupo de permutações de C. Uma **representação** de G **no grupo das permutações de** C é um homomorfismo $f : G \to P(C)$, isto é, uma função tal que $f(g_1g_2) = f(g_1) \circ f(g_2)$. Diz-se também que o grupo G opera sobre o conjunto C.

Com base na definição, considere um grupo G, um conjunto C e um homomorfismo $f : G \to P(C)$, no qual é uma representação de G. Sobre C definimos uma relação de equivalência $\sim$ da seguinte maneira:

$$\forall x, y \in G, \quad x \sim y \Leftrightarrow \exists\ g \in G \text{ tal que } f(g)(x) = y$$

A seguir vamos definir Órbita e Estabilizado de um dado elemento.

Definição 3.7. Sejam G um grupo e $x \in C$. Definimos a **órbita** de x como o conjunto definido por,

$$\tau(x) := \{y \in C : y \sim x\} = \{f(g)(x) = y : g \in G\}.$$

O **estabilizador** de x, por sua vez, é o conjunto dos elementos de G que deixam o elemento x fixo, isto é,

$$E(x) := \{g \in G : f(g)(x) = x\}.$$

É possível verificar ainda, que o conjunto $E(x)$ é um subgrupo de G. Da definição, podemos estabelecer a seguinte relação:

Teorema 3.3. *Seja $f : G \to P(C)$ uma representação do grupo G no grupo de permutações do conjunto C. Seja $x \in C$, então a aplicação ψ abaixo é uma bijeção:*

$\psi : \tau(x) \to \{$ *Classes laterais à esquerda de $E(x)$ em G*$\}$

$f(g)(x) \mapsto gE(x)$

Em particular, no caso de G ser um grupo finito, temos que $|\tau(x)| = (G : E(x))$ e que $|\tau(x)|$ divide $|G|$.

Demonstração. Ver Garcia e Lequain(2012, p. 255). ■

Exemplo 3.1. Sejam G um grupo e C um conjunto. Considere a aplicação

$$\begin{array}{ccccccc} f : G & \longrightarrow & P(C) & & & & \\ g & \longmapsto & f_g : & C & \longrightarrow & C \\ & & & x & \longmapsto & gxg^{-1} \end{array}$$

Seja $x \in C$. A órbita $\tau(x) = \{f_g : g \in G\} = \{gxg^{-1} : g \in G\}$ de um elemento $x \in C$. Observe que temos $C\ell(x) = \{x\} \Leftrightarrow gxg^{-1} = x$, $\forall g \in G \Leftrightarrow x \in Z(G)$.

O estabilizador, definido por:

$$E(x) = \{g \in G : f_g(x) = x\} = \{g \in G : gxg^{-1} = x\} = \{g \in G : g \text{ comuta com } x\}$$

de um elemento $x \in C$, que nesta representação por conjugação se chama o *centralizador de* x, e se denota por $Z(x)$, ou seja, $Z(x) = \{g \in G : gx = xg\}$.

Segundo o Teorema 3.3, temos,

$$|C\ell(x)| = \#^2\{ \text{ conjugados de } x \text{ em } G\} = (G : Z(x)).$$

Naturalmente, o conjunto C é igual à união, disjunta, das classes de conjugação. Em cada classe de conjugação escolhemos um representante x_α. Então, temos $|G| = \sum_\alpha |C\ell(x_\alpha)|$, logo

$$|G| = |Z(G)| + \sum_{x_\alpha \notin Z(G)} |C\ell(x_\alpha)|. \tag{3.3}$$

No qual $Z(x_\alpha) \subset G$. Da equação (3.2), podemos estabeler algumas consequências interessantes, que são apresentadas a seguir.

Proposição 3.1. *Seja p um número primo e seja G um grupo de ordem p^n com $n \geq 1$. Então $Z(G)$ tem pelo menos p elementos.*

Demonstração. Ver Garcia e Lequain(2012, p. 256). ■

Proposição 3.2. *Seja p um número primo. Então todo grupo G de ordem p^2 é abeliano.*

Demonstração. Ver Garcia e Lequain(2012, p. 256). ■

3.2 Teorema de Sylow

Como já debatemos no final do Capítulo 2, sabemos que a recíproca do *Teorema de Lagrange* não é valida, em geral. E um dos caminhos para a obtenção da validade dessa recíproca, para alguns casos, parte do estudo do 1º Teorema de Sylow, que nos fornecerá embasamento para a sua obtenção.

Peter Ludwig Mejdell Sylow (1832 – 1918) foi um matemático norueguês, que publicou trabalhos de grande importância sobre Teoria dos Grupos. Onde em 1872, o mesmo provou uma série de Teoremas que foi a pedra angular da Teoria de Grupos finitos.

Dessa forma, faremos a apresentação do 1º Teorema de Sylow e alguns resultados derivados dele, principalmente a definição de p-grupos.

[2] Representação de Cardinalidade de um conjunto

Figura 2 – *Peter Ludwig Mejdell Sylow*

Fonte: Google

Lema 3.3.1. ***(Cauchy)*** *Seja G um grupo abeliano finito. Seja p um número primo que divide $|G|$. Então existe $x \in G$ de ordem p.*

Demonstração. Para verificar esse lema, faremos uma indução sobre $|G|$. Sendo assim temos:

Se $|G| = 1$, não tem o que ser feito.

Se $|G| > 1$, suponha por hipótese de indução, que o Lema é válido para todos os grupos abelianos de ordem menor que $|G|$, e provaremos que o Lema também vale para o grupo G.

Se $p = |G|$, então pelos Corolário 2.2 e 2.3, podemos garantir que G é cíclico e qualquer gerador de G tem ordem p. Provando o que queriamos.

Caso $p \neq |G|$, afirmaremos inicialmente que existe um subgrupo H tal que $1 < |H| < |G|$. De fato, tome $y \in G, y \neq e$; se $\langle y \rangle \neq G$ então $H = \langle y \rangle$ serve, se $\langle y \rangle = G$, então $y^p \neq e$ e $H = \langle y^p \rangle$ serve, no qual $|H| = O(y^p) = |G|/p < |G|$.

Agora, se p divide $|H|$ então, pela hipótese de indução, existe elementos $x \in H \subseteq G$ de ordem p, finalizando o que queriamos provar. Caso p não divida $|H|$ então, pela igualdade $|G| = |H||G/H|$ onde $H \triangleleft G$, assim temos que p divide $|G/H|$ e $|G/H| < |G|$; logo, pela hipótese, existe $\bar{z} \in G/H$ de ordem p. Considere o homomorfismo canônico:

$$\begin{array}{ccc} f : G & \longrightarrow & G/H \\ z & \longmapsto & f(z) = \bar{z} \end{array} \tag{3.4}$$

Seja r a ordem deste elemento z, onde $z^r = e$, logo $f(z^r) = f(e)$, ou seja, $\bar{z}^r = \bar{e}$ e,

portanto, r é um múltiplo da ordem de $\bar{z}$, ou seja, r é múltiplo de p, onde $r = kp$ com $k \geq 1$. Então z^k é um elemento de G de ordem p. ■

Como generalização do Lema de Cauchy, temos:

Corolário 3.2. Sejam G um grupo finito e p um número primo que divide $|G|$. Então existe um elemento $x \in G$ de ordem p.

Dessa forma, podemos apresentar o 1º Teorema de Sylow.

Teorema 3.4. ***(1º Teorema de Sylow)*** *Sejam p um número primo e G um grupo de ordem $p^m b$ com $mdc(p, b) = 1$. Então, para cada n, com $0 \leq n \leq m$, existe um subgrupo H de G tal que $|H| = p^n$.*

Demonstração. De forma similar com a demonstração do Lema de Cauchy, faremos uma indução sobre $|G|$.

Se $|G| = 1$, não teremos o que mostrar.

Se $|G| \neq 1$, iremos supor, como hipótese de indução, que o Teorema vale para todos os grupos de ordem menor que $|G|$, e assim provaremos que também vale para para o grupo G.

Seja n um inteiro positivo tal que p^n divide $|G|$. Assim iremos considerar dois casos, a saber,

CASO 1: Se existe um subgrupo próprio H de G tal que p^n divida sua ordem. Neste caso, pela hipótese de indução, como H é um subgrupo não trivial, temos que G possui um subgrupo de ordem p^n.

CASO 2: Se não existe um subgrupo próprio H de G tal que p^n divide sua ordem, consideraremos a equação 3.2, assim

$$|G| = |Z(G)| + \sum_{x_\alpha \notin Z(G)} |C\ell(x_\alpha)| = |Z(G)| + \sum_{x_\alpha \notin Z(G)} (G : Z(x_\alpha)). \tag{3.5}$$

Para $x_\alpha \notin Z(G)$, temos que $Z(x_\alpha) \subset G$, sendo distintos, logo por hipótese, p^n não divide $|Z(x_\alpha)|$, e portanto p divide $(G : Z(x_\alpha))$. Como p divide $|G|$, então obtemos que p divide $|Z(G)|$. Como $Z(G)$ é um grupo abeliano, existe pelo Lema de Cauchy, um elemento $y \in Z(G)$ de ordem p. Como $y \in Z(G)$, é possível perceber que $\langle y \rangle \triangleleft G$, de modo que podemos considerar o grupo quociente $G/\langle y \rangle$. Naturalmente, $|G/\langle y \rangle| < |G|$ e p^{n-1} divide $|G/\langle y \rangle|$. Da indução, o grupo $G/\langle y \rangle$ possui um subgrupo K' de ordem p^{n-1}.

Assim, considere o homomorfismo canônico $f : G \to G/\langle y \rangle$, e tome $K = f^{-1}(K')$. Então K é um subgrupo de G com $|K| = |kerf||K'| = |\langle y \rangle||K'| = p^n$. Como queriamos provar!

■

Em posse deste Teorema, você pode garantir a existência de determinados subgrupos em um dado grupo. E de forma particular, com o corolário a seguir, você garante de forma bem precisa a existência de um determinado subgrupo, que mais adiante veremos que recebe um nome especial.

Corolário 3.3. Sejam G um grupo finito e p um número primo. Seja p^m a maior potência de p que divide $|G|$. Então existe um subgrupo de G de ordem p^m.

Definição 3.8. Sejam G um grupo finito, p um primo e p^m a maior potência de p que divide $|G|$. Os subgrupos de G que tem ordem p^m são chamados de **p-subgrupos de Sylow** de G, ou **subgrupos de Sylow de** G.

O 1º Teorema de Sylow garante que há ao menos um p-subgrupo de Sylow, para cada primo "p" que aparece na decomposição em fatores primos da ordem de G. Sendo então a primeira garantia para a existência das recíprocas do *Teorema de Lagrange*.

Corolário 3.4. Sejam G um grupo finito e p um número primo. Então $|G|$ é igual a uma potência de p se e só se cada elemento do grupo G tem sua ordem igual a uma potência de p.

A partir desse corolário, definimos portanto, p-grupo.

Definição 3.9. Seja p um número primo. Um grupo G, não necessáriamente finito, no qual todo elemento tem sua ordem igual a uma potência de p é chamado de **p-grupo**.

3.3 Grupos Solúveis e Grupos Nilpotentes

O conceito de grupo solúvel é um dos mais antigos na Teoria de Grupos, que foi introduzido pro *Ernest Galois* quando estudava o problema de resolver equaçõe algébricas mediante radicais. Ele associou um grupo a cada equação e mostrou que a equação é resolúvel mediante radicais se, e somente se, o grupo correspondente é solúvel.

Pode-se pensar nos grupos solúveis como "aproximadamente abelianos". Por exemplo, podemos considerar que 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, e esse grupo é chamado de *metabeliano*.

Definição 3.10. Um grupo G diz-se **solúvel** se contém uma cadeia de subgrupos:

$$\{e\} = G_0 \subseteq G_1 \subseteq ... \subseteq G_n = G$$

tal que cada subgrupo G_{i-1} é normal em G_i e o grupo quociente G_i/G_{i-1}, com $1 \leq i \leq n$ é abeliano.

Uma cadeia de subgrupos de G com está propriedade chama-se uma *série subnormal abeliana de* G e os quocientes respectivos chamam-se *fatores da série.*

Teorema 3.5. *Seja G um grupo. Assim,*

(1) Seja H um subgrupo de G. Se G é solúvel, então H é solúvel.

(2) Seja H um subgrupo normal de G. Então, o grupo G é solúvel se, e somente, se os grupos H e G/H são solúvel.

Demonstração. Ver Garcia e Lequain(2012, p. 302). ■

Definição 3.11. Dados dois elementos x, y de um grupo G, o **comutador** de x e y é o elemento

$$[x, y] := x^{-1}y^{-1}xy \in G.$$

Dessa forma, dados dois subconjuntos H e K de um grupo G, denotaremos por $[H, K]$ o subgrupo de G gerado pelo conjunto:

$$\{[h, k] | h \in H, k \in K\}.$$

Em particular, o grupo $G' = [G, G]$ chama-se *subgrupo comutador* ou *subgrupo derivado* de G.

Indutivamente, podemos definir agora uma sequência de subgrupos da seguinte forma:

$$G^{(0)} = G$$
$$G^{(1)} = G'$$
$$\vdots$$
$$G^{(n)} = (G^{(n-1)})$$

O subgrupo $G^{(n)}$ acima chama-se o n-ésimo grupo derivado de G e a sequência

$$G = G^{(0)} \supseteq G^{(1)} \supseteq ... \supseteq G^{(n)} \supseteq ...$$

chama-se a *sequência derivada* de G.

Exemplo 3.2. Temos que se $n \geq 5$, então S_n não é solúvel. De fato, pois se S_n fosse solúvel, o subgrupo das permutações pares A_n também seria, mas sabemos que A_n é simples (para $n \neq 4$) e $A'_n \lhd A_n \Rightarrow A'_n = A_n$, pois A_n é não abeliano. Consequentemente, $A_n = {A_n}^k$, para todo $k \in \mathbb{Z}$, o que é uma contradição pois A_n so é solúvel se, e somente se, ${A_n}^k = 1$.

Estudaremos agora, uma classe de grupos que, de certa forma, está entre a classe dos grupos abelianos e a classe dos grupos solúveis e é possível obter resultados fortes sobre sua estrutura.

Definição 3.12. Um grupo G diz-se **nilpotente** se ele contém uma série de subgrupos

$$\{e\} = G_0 \subset G_1 \subset ... \subset G_n = G$$

tal que cada subgrupo G_{i-1} é normal em G e cada quociente G_i/G_{i-1} está contido no centro de G/G_{i-1}, $1 \leq i \leq n$. Uma tal série de subgrupos de G diz-se **série central** de G.

Note que a definição de nilpotência e estremamente mais restritiva em relação a definição de solubilidade, logo temos as seguintes inclusões: grupos ciclícos $\subset$ grupos abelianos $\subset$ grupos nilpotentes $\subset$ grupos solúveis $\subset$ todos os grupos.

Definiremos duas novas séries de subgrupos indutivamente,

$$\gamma_1(G) = G,\ \gamma_2(G) = G' \text{ e } \gamma_i(G) = (\gamma_{i-1}(G), G).$$

O outro subgrupo será apoiado no conceito de *centro* de um grupo:

$$\text{Denotamos } \zeta_0(G) = \{e\},\ \zeta_1(G) = Z(G)$$

e definimos indutivamente $\zeta_i(G)$ como sendo o único subgrupo de G tal que $\zeta_i(G)/\zeta_{i-1}(G) = Z(G/\zeta_{i-1}(G))$. Onde esse subgrupo recebe o nome de **i-ésimo centro** de G.

Proposição 3.3. *Todo p-grupo finito é nilpotente.*

Demonstração. Ver Bhattacharya (1995, p. 126) ■

Proposição 3.4. *Produto direto de grupos nilpotente é nilpotente.*

Demonstração. Ver Bhattacharya (1995, p. 128)

■

Teorema 3.6. *Um grupo fnito é nilpotente se, e somente se, ele for o produto direto de seus subgrupos de Sylow.*

Demonstração. Ver Silveira (2010, p. 13-14)

■

4 RECÍPROCAS PARA O TEOREMA DE LAGRANGE

Com o auxílio do exposto nas seções anteriores, temos condições de aprofundar os estudos sobre o *Teorema de Lagrange*, mas precisamente sobre algumas recíprocas deste.

Ficaria incompleto esse trabalho, se não mecionar o *Lema de Cauchy* e o *1º Teorema de Sylow* e apresentá-los como sendo recíprocas gene do *Teorema de Lagrange*.

Sendo assim o *Lema de Cauchy* nos diz que dados G um grupo abeliano finito e p um número primo que divide $|G|$. Então existe $x \in G$ de ordem p. Portanto, usando o fato que $O(x) = | < x > |$ temos a consequência.

Já o *1º Teorema de Sylow* nos diz que se p um número primo e G um grupo de ordem $p^m b$ com $mdc(p, b) = 1$. Então, para cada n, com $0 \leq n \leq m$, existe um subgrupo H de G tal que $|H| = p^n$. Portanto, como se pode perceber todos os grupos finitos que satisfazem às condições do teorema possui subgrupo com quantidade de elementos divisor da ordem de G.

Ademais, apresentamos uma recíproca envolvendo Grupos Solúveis que a chamaremos de recíproca fraca por não ter um caráter geral e três recíprocas envolvendo p-grupos, Grupos abelianos finitos e Grupos nilpotentes, as quais chamaremos de recíprocas fortes por possuírem um caráter geral.

4.1 Recíproca para Grupos Abelianos finitos

Proposição 4.1. *Sejam G um grupo abeliano finito e m um inteiro que divide $|G|$. Então existe um subgrupo K de G tal que $|K| = m$.*

Demonstração. Sendo m um inteiro que divide $|G|$, assim podemos decompor m em fatores primos, ou seja,

$$m = {p_1}^{\alpha_1} ... {p_l}^{\alpha_l}.$$

Pelo Teorema 3.4 temos que existem subgrupos N_i de G com ordem ${p_i}^{\alpha_i}$, para $1 \leq i \leq l$. Sendo G abeliano, então como consequência pela Definição 2.8, N_i é normal em G para cada i. Então pela Proposição 2.8 temos que $N_1 ... N_i$ é um subgrupo de G, para cada $i = 1, ..., l$. Considere N_j como sendo um dos subgrupos qualquer de G, temos que

$$x \in N_j \cap (N_1 ... N_{j-1} N_{j+1} ... N_l) \text{ temos que } O(x) \mid p_j \text{ e } O(x) \mid p_i$$

para algum $i = 1, ..., j-1, j+1, ..., l$. Como $p_i \neq p_j$ para $i \neq j$, temos que $O(x) = 1$, isto é $x = e$. Logo,

$$N_j \cap (N_1 ... N_{j-1} N_{j+1} ... N_l) = \{e\}.$$

Sendo assim $K = N_1 ... N_l$ é um subgrupo de G com ordem m. Como queriamos provar. ■

4.2 Recíproca para p-grupos

Proposição 4.2. *Se G é um grupo de ordem p^m, então G contém subgrupos de ordem p^k, para todo inteiro positivo $k \leq m$.*

Demonstração. Partindo do 1º Teorema de Sylow, ele expõem que dado um grupo de ordem $p^m b$, existirá um subgrupo de ordem p^n, com $0 \leq n \leq m$. De forma particular seja $b = 1$, assim temos que $|G| = p^m$, que é o caso aqui expresso, e sendo assim podemos concluir que existe subgrupos de ordem p^k, para $k \leq m$. ■

4.3 Recíproca para Grupos Solúveis

Teorema 4.1. *(P. Hall, 1928) Seja G um grupo solúvel finito de ordem mn com $mdc(m, n) = 1$. Então existe um subgrupo de G de ordem m.*

Demonstração. Realizaremos a demonstração por indução em $|G|$.
Se $|G| = m = 1$, não temos o que fazer, no qual $m = n = 1$ e G terá somente um subgrupo trivial, da mesma ordem que G.
Se $|G| \neq 1$, por hipotese o Teorema vale para os grupos de ordem menor que $|G|$, e assim provaremos que também vale para o grupo G.
Considere que G contém um subgrupo normal H de G de ordem $m'n'$, no qual $m'|m$ e $n'|n$, com $n' < n$. Verificaremos, a existência desse subgrupo. Neste caso, o grupo G/H é um grupo solúvel pelo Teorema 3.6 e pelo *Teorema de Lagrange*, terá ordem igual a $(m/m')(n/n')$. Então, $(m/m')(n/n') < mn$. Ademais, (m/m') e (n/n') são primos, uma vez que m e n são. Por hipótese indutiva, G/H tem um subgrupo A/H com ordem m/m'. Agora pelo *Teorema de Lagrange*, A tem ordem $(m/m')|H| = mn' < mn$. Sendo A subgrupo de G, assim o mesmo é solúvel pelo Teorema 3.6, e por hipótese, tem um subgrupo de ordem m. Como queriamos provar!

■

4.4 Recíproca para Grupos Nilpotentes

Proposição 4.3. *Se G for um grupo nilpotente e m divide $|G|$, então G possui um subgrupo de ordem m.*

Demonstração. Podemos escrever a ordem de G, como um produto de potências de primos distintos, assim

$$|G| = {p_1}^{n_1}...{p_i}^{n_i} \text{ com } n_i > 0, \text{ assim } m = {p_1}^{m_1}...{p_i}^{m_i}, \text{ com } 0 \leq m_i \leq n_i.$$

Pelo Teorema 3.4, podemos garantir a existência de H_i, um subgrupo de G, cuja ordem é ${p_i}^{m_i}$ para todo i. Portanto o produto direto $H = H_1 \times H_2 \times ... \times H_i$ é o subgrupo de ordem m. ■

REFERÊNCIAS

BHATTACHARIA, P.; JAIN, S.; NAGPAUL, S. **Basic Abstract Algebra**. 2. ed. New York, EUA: Cambridge University Press, 1995. Citado na página 12.

FAZZIO, A.; WATARI, K. **Introdução à Teoria de Grupos aplicada em moléculas e sólidos**. 2. ed. Santa Maria, RS: UFSM, 2009. Citado na página 12.

GARCIA, A.; LEQUAIN, Y. **Elementos de Álgebra**. 6. ed. Rio de Janeiro, RJ: IMPA, 2012. Citado na página 12.

MILIES, C. P. Grupos Nilpotentes: Uma Introdução. **Matemática Universitária**, n. 34, p. 55 – 100, 2003. Citado na página 12.

SILVEIRA, D. S. Grupos solúveis e nilpotentes. UFMG, 2010. Citado na página 12.

VIEIRA, V. L. **Álgebra Abstrata para Licenciatura**. 2. ed. Campina Grande, PB: EDUEPB, 2015. Citado nas páginas 12 e 14.