UNIVERSIDADE FEDERAL DO NORTE DO TOCANTINS
CENTRO DE CIÊNCIAS INTEGRADAS
CURSO DE LICENCIATURA EM MATEMÁTICA

GUSTAVO SANTOS XAVIER

TEOREMA DE LAGRANGE: EXEMPLOS E APLICAÇÕES DA TEORIA DE GRUPOS

Araguaína / TO

2022

GUSTAVO SANTOS XAVIER

TEOREMA DE LAGRANGE: EXEMPLOS E APLICAÇÕES DA TEORIA DE GRUPOS

Monografia apresentada ao Curso de Licenciatura em Matemática, da Universidade Federal do Norte do Tocantins - UFNT, Centro de Ciências Integradas, como requisito parcial para a obtenção do título de Licenciado em Matemática.

Orientadora: Profª. Drª. Renata Alves da Silva

Araguaína / TO

2022

Dados Internacionais de Catalogação na Publicação (CIP)
Sistema de Bibliotecas da Universidade Federal do Tocantins

X3t Xavier, Gustavo Santos.

Teorema de Lagrange: exemplos e aplicações da Teoria de Grupos . / Gustavo Santos Xavier. – Araguaína, TO, 2022.

43 f.

Monografia Graduação - Universidade Federal do Tocantins – Câmpus Universitário de Araguaína - Curso de Matemática, 2022. Orientadora : Renata Alves da Silva

1. Teoria de Grupos. 2. Teorema de Lagrange. 3. Teorema de Fermat. 4. Álgebra Abstrata. I. Título

CDD 510

Elaborado pelo sistema de geração automática de ficha catalográfica da UFT com os dados fornecidos pelo(a) autor(a).

GUSTAVO SANTOS XAVIER

TEOREMA DE LAGRANGE: EXEMPLOS E APLICAÇÕES DA TEORIA DE GRUPOS

Monografia apresentada ao Curso de Licenciatura em Matemática, da Universidade Federal do Norte do Tocantins - UFNT, Centro de Ciências Integradas – CCI/Cimba, como requisito parcial para a obtenção do título de Licenciado em Matemática.

Aprovada em 08 de dezembro de 2022.

Banca examinadora

Profª. Drª. Renata Alves da Silva
Orientadora/UFNT

Prof. Dr. José Carlos de Oliveira Junior
Examinador/UFNT

Prof. Dr. Alvaro Julio Yucra Hancco
Examinador/UFNT

Araguaína / TO

2022

Dedicado aos senhores João Batista Xavier e Maria de Fátima dos Santos Xavier, meus pais, e a Hartur Batista Xavier Oliveira, meu afilhado.

AGRADECIMENTOS

Agradeço em primeira instância aos meus pais, João Batista Xavier e Maria de Fátima dos Santos Xavier, e a minha família por todo o esforço e incentivo para com meus estudos e para com minha formação.

Agradeço a Universidade Federal do Norte do Tocantins, Campus Araguaína Cimba e a todo colegiado do curso em Licenciatura em Matemática pela oportunidade de estudo e pelo trabalho e empenho na formação superior, em especial à Profª. Drª. Renata Alves da Silva por ter aceitado a orientação deste trabalho.

Agradeço também à Coordenação de Aperfeiçoamento de Pessoal de Nível Superior – CAPES, pelo período de fomento durante o Programa Institucional de Bolsa a Iniciação à Docência – PIBID, assim como os professores coordenadores e supervisores.

Por fim, agradeço aos amigos e colegas que conheci, dentro e fora da universidade, durante esse ciclo por todo o apoio, auxílio e incentivo em continuar no curso, além das muitas histórias que construímos e vivemos.

RESUMO

A Teoria de Grupos teve seu início em 1830 com a então descoberta do francês Évariste Galois sobre resolubilidade de equações algébricas. Esse marco foi reflexo de séculos de estudos e esforços de grandes matemáticos que, assim como Galois buscavam encontrar um método geral de resolver as equações polinomiais de grau maior que cinco. Dentre tantos nomes que antecederam e contribuíram fortemente com o desenvolvimento da teoria destaca-se o de Joseph Louis Lagrange. A teoria de Grupos perpassou por diversos estudiosos ao longo da história, chegando na forma como é conhecida em seus enunciados e notações moderna. Nesse sentido, no presente trabalho pautamo-nos em apresentar e exemplificar conceitos e resultados chaves da Teoria de Grupos para demonstrar o Teorema de Lagrange, o qual trata de uma relação da ordem de um grupo com a ordem do seu subgrupo e propor algumas aplicações em relação a grupos finitos e na Teoria dos Números, através da demonstração do Pequeno Teorema de Fermat sobre divisibilidade por números primos.

Palavras-chave: Grupos. Subgrupo. Classes Laterais. Classe. Números Primos.

ABSTRACT

Group Theory began in 1830 with Évariste Galois' discovery about the solvability of algebraic equations. This milestone was a reflection of centuries of studies and efforts of great mathematicians who, like Galois, sought to find a general method of solving polynomial equations of degree greater than five. Among many names that preceded and strongly contributed to the development of the theory is Joseph Louis Lagrange. The theory of groups has passed through several scholars throughout history, arriving in the way it is known in its modern statements and notations. In this sense, this paper is based on presenting and exemplifying key concepts and results of Group Theory to demonstrate the Lagrange Theorem, which deals with a relationship of the order of a group with the order of its subgroup and propose some applications in finite groups and in Number Theory, through the demonstration of Fermat's Little Theorem about divisibility by prime numbers.

Keywords: Groups. Subgroup. Side Classes. Class. Prime numbers.

SUMÁRIO

INTRODUÇÃO

A Teoria de Grupos se iniciou com a obra de Évariste Galois (1811-1832) mais especificamente, no ano de 1830, em seu artigo no qual deu uma caracterização matemática para a resolubilidade de equações polinomiais de grau maior ou igual a cinco, associando a cada equação um grupo de permutações de suas raízes, munindo-o a uma operação que permita a relação entre os elementos do conjunto e condicionando-a à resolubilidade por radicais através de suas propriedades. Por exemplo, a existência de um elemento neutro da operação presente no conjunto, a equação $a * x = b$ possuir conjunto solução unitário constituído por $a' * b$, onde a' é o elemento simétrico de a.

Contudo, a problemática da resolubilidade das equações de quinto grau ou superior se iniciou logo após a descoberta de uma forma geral para a resolução de equações de terceiro grau utilizando radicais desenvolvida por Del Ferro (1456-1526), entre os anos de 1500 e 1515. Esta descoberta indagou a comunidade matemática acerca da possibilidade das equações de grau maior que quatro tivessem a resolubilidade por radicais através de fórmulas matemáticas, assim como para as equações quadráticas, no Brasil conhecida como fórmula de Bhaskara, e as cúbicas descobertas por Del Ferro.

O movimento de procura destas resolubilidades provocou ainda no século XVI a descoberta da fórmula de resolução de equações de quarto grau, dada por Ludovico Ferrari (1522-1560), um dos alunos de Cardano, o qual a publicou em continuidade à solução de grau três em 1545 (SCHUVAAB, 2013), que foi reescrita por Ferrari posteriormente de maneira mais simplificada. Dois séculos após, no ano de 1770-1771, destaca-se na problemática das quínticas o nome de Joseph Louis Lagrange, o qual traz em sua obra publicada neste mesmo ano, alguns deslumbres que embasariam Galois no desenvolvimento da teoria de grupos séculos mais tarde. Lagrange foi o responsável por enunciar um dos teoremas presentes nos estudos de grupos antes mesmo desta teoria ser consolidada.

Neste sentido, a busca pela resolutividade das equações de graus maiores que quatro não parou e quase um século mais tarde, no ano de 1824, Niels Henrik Abel provara que não existe resolubilidade por radicais para certas equações de grau maior ou igual a cinco. Porém, mesmo com esta demonstração, o questionamento acerca da resolubilidade das quínticas se perdurou até o ano de 1830, data de publicação da obra de Galois que tratava da resolubilidade destes polinômios.

A Teoria de Grupos desenvolvida pelo jovem francês, do qual a batizou por este mesmo nome em sua obra, se tornou objeto de estudo para notáveis matemáticos ao decorrer da história,

se tornando elemento de grande importância dentro da Álgebra e de outras áreas da ciência, como na Física na solução da equação de Schrödinger referente a evolução de ondas associadas a partículas de forma temporal e espacial, na Biologia com a modelagem de códigos genéticos (códon), entre outras.

Desse modo, o presente trabalho se atenta em fazer um estudo acerca de alguns tópicos pertencentes à Teoria de Grupos, dando ênfase nos grupos de classes residuais e sua relação na teoria de congruência envolvendo números primos. Além de pautar-se em descobrir qual a relação entre a quantidade de classes laterais e a quantidade de elementos de um grupo qualquer e ainda, sobre quais condições a teoria de Grupos atua no estudo dos números primos.

Sendo assim, tem-se como objetivo principal, perpassar pelo Teorema de Lagrange, que diz que a ordem de um grupo G é dada pelo produto da ordem do subgrupo H de G pelo índice de G por H. Trazendo, sempre que possível, demonstrações, exemplos e aplicações, sendo uma delas o Pequeno Teorema de Fermat, um importante teorema quando se trata de congruência envolvendo números primos, ou seja, $a \equiv b\ (mod\ p)$, onde a e b são inteiros quaisquer e p um número primo, usualmente utilizado quando se deseja encontrar restos da divisão de números inteiros muito grandes por números primos.

Dessa maneira, a organização deste trabalho se encontra da seguinte forma: o primeiro capítulo traz algumas notas históricas acerca da Teoria de Grupos, tomando por valer uma breve construção do que influenciou no desenvolvimento histórico desta teoria.

Em seguida, no capítulo dois, trabalha-se o estudo de alguns pontos chaves da teoria, dando ênfase nos grupos das classes residuais, classes laterais e subgrupos, sendo estes pontos cruciais da teoria para compreender o resultado principal neste trabalho, o Teorema de Lagrange.

Por fim, no terceiro capítulo, trabalha-se com a demonstração, exemplos e aplicações do Teorema de Lagrange, sendo uma destas aplicações a prova do pequeno Teorema de Fermat, um forte resultado quando se trata de congruência envolvendo números primos.

1 NOTAS HISTÓRICAS SOBRE A TEORIA DE GRUPOS

Analisando qualquer material relacionado à História da Matemática, nota-se que o desenvolvimento das primeiras civilizações se deu pelo desenvolvimento da linguagem oral, escrita e com esta a linguagem numérica, dando espaço para uma interpretação quantitativa das situações do cotidiano, como em medições de terrenos e no comércio, fazendo com que a Matemática deixasse, gradativamente, de ser apenas uma ferramenta e começasse a se tornar como se mostra hoje.

Nesse sentido, as equações quadráticas possuem seu registro mais antigo (EVES, 2011) no período do antigo Egito com o Papiro de Berlim, o qual remota por volta do ano de 1950 a.C. e, atualmente se encontra exposto no museu Staatliche (Berlim). Um outro registro deste povo é o Papiro de Kahun de 1800 a.C., que traz em suas escrituras alguns problemas envolvendo equações de primeiro e segundo grau cuja solução utiliza o método de falsa posição, o qual envolve um sistema de equações compostas por uma equação de grau dois e outra afim. De maneira geral, os egípcios trabalhavam com problemas com fins práticos, mas ainda assim aritméticos (BOYER, 2012, p.12), ou seja, não se baseavam apenas em objetos concretos ou apenas em números conhecidos, mas se valiam também de soluções de equações lineares utilizando as *aha*, conhecidas hoje como incógnitas.

Já os babilônicos, povo que vivia na região mesopotâmica entre os rios Tigres e Eufrates, são conhecidos pelo seu grande desenvolvimento matemático simultâneo ao dos egípcios, mas ao que se sabe, possuíam estratégias para resolver equações de segundo grau por volta de 1700 a.C., data posterior aos Papiros de Berlim e Kahun. Por não possuírem notações algébricas, seus problemas eram enunciados em vocábulos, tal qual suas respostas, dando assim uma aparência de "receitas matemáticas" (BOYER, 2012) para as resoluções das equações.

É com os antigos gregos que se inicia um formalismo matemático baseado na ordenação lógica de ideias para demonstrá-las, passando assim de fins práticos e para abstrações e até um caráter filosófico, influenciando assim em avanços consideráveis para a Matemática. Principalmente após a obra *Os Elementos* de Euclides, levou os gregos a desenvolverem tratamentos geométricos para diversos problemas, entre eles a equação quadrática.

Ao falar da Matemática hindu voltada a resolver equações de segundo grau, destaca-se nomes como Aryabhata (séc. VI), Brahmagupta (séc. VII), Sridhara (séc. XI) e Bhaskara (séc. XII). Por ser precedido por vários matemáticos habilidosos, Bhaskara trata de problemas que haviam sido trabalhados anteriormente. Em seu livro *Lilavati* ele se dedica, entre outros assuntos, a resolver várias questões de equações de segundo grau, que já haviam sido abordadas

por Brahmagupta (que propôs soluções gerais encontrando duas raízes, inclusive com valores negativos), Sridhara e outros matemáticos. Complementou o trabalho de seus antecessores, preencheu algumas lacunas que haviam sido deixadas, e fez suas próprias contribuições, dando a solução geral da equação $x^2 = 1 + py^2$ e de muitas outras equações diofantinas.

Já os árabes, famosos principalmente pela conservação, tradução e disseminação da Matemática hindu e ocidental, construindo grandes centros científicos que ficaram conhecidos como *Bait al-hikma* ou Casa da Sabedoria, o que influenciou o surgimento de grandes nomes dentro da Matemática, entre eles o de Mohammed ibn al-Khowarizmi (780-850), célebre por seus tratados de álgebra como o *Ciência das Equações*, em tradução, no qual descreve, de maneira retórica, soluções de equações de primeiro e segundo grau e, no século IX descobriu um método de comprovação geométrica para raízes positivas, iniciando o que é conhecida hoje como Álgebra Geométrica (GUELLI, 1995).

Na Europa, a partir do século XII, se iniciou um movimento de propagação da Matemática graças a diversas obras traduzidas do hindu, árabe e grego, dando início a não apenas a padronização da escrita matemática, mas também pelo desenvolvimento de métodos de resolução das quadráticas no qual destaca-se nomes como François Viète (1540-1603) e René Descartes (1596-1650) (OLIVEIRA, 2018).

Contudo, ao especificar os estudos históricos para a teoria de grupos nota-se que os primeiros relances desta se iniciaram por volta do ano de 1500-1515, quando o italiano Scipione del Ferro (1456-1526) anunciou o descobrimento de uma fórmula de resolução por radicais para as equações de terceiro grau, possibilitando encontrar as raízes cúbicas através de

$$x = \sqrt[3]{\frac{q}{2} + \sqrt{\left(\frac{q}{2}\right)^2 - \left(\frac{p}{3}\right)^3}} - \sqrt[3]{\frac{q}{2} + \sqrt{\left(\frac{q}{2}\right)^2 - \left(\frac{p}{3}\right)^3}}.$$

O trabalho de del Ferro, assim como a resolubilidade das equações quadradas, conhecida no Brasil como fórmula de Bhaskara, da qual possui uma vasta história, desafiou outros matemáticos, principalmente algebristas, a descobrir se toda equação algébrica é resolúvel por radicais. Del Ferro não costumava registrar suas descobertas de forma escrita, apenas comunicava-as para algumas pessoas, geralmente seus alunos, nesta ocasião se tratava de Antônio Maria Fior.

Em 1535, o matemático Nicola Fontana de Brescia, mais conhecido como Tartaglia ou "Tartamudo" devido a sua condição física que dificultava sua fala, inteirou que havia descoberto a resolução algébrica das equações cúbicas (EVES, 2011) sem conhecimento do método de del Ferro. Incitado pela curiosidade, Fior acreditando, também, que se tratava de um

blefe de Tartaglia, o propôs um desafio, que na época consistia em resolver problemas propostos pelo outro.

O tartamudo aceitou o desafio, pois não dava muita credibilidade a Fior (SCHUVAAB, 2013) e, utilizando de seus métodos de resolução das cúbicas desenvolvidas por volta de 1535, ganhou o desafio de Fior, resolvendo todos os problemas propostos por ele.

Tartaglia que também não tinha costume de publicar os métodos de suas descobertas, apenas os resultados, contou após muita insistência o método de resolução das cúbicas para seu amigo Gerolamo Cardano (1501-1576), que a priori, concordou sob juramento solene em manter segredo. Mas ao tomar conhecimento de que ele não havia sido o primeiro a descobrir o método destas equações, Cardano publicou em 1845 o livro *Ars Magna*, marcando um grande rompimento aos estudos de matemática da época, já que trouxe consigo não apenas os resultados das equações, mas também os métodos de resolução das equações cúbicas e também as quárticas.

Seguindo um caminho paralelo, mas tendo quase o mesmo fim, temos ainda no século XVI, motivado pelos rumores da descoberta de del Ferro, Ludovico Ferrai (1522-1560) descobriu a fórmula de resolubilidade para as equações de grau igual a quatro utilizando método de transformação, o qual também foi publicada por Cardano, seu professor, em 1545 (SCHUVAAB, 2013). Estes fatos incitaram ainda mais a comunidade a matemática a procurar fórmulas de resolução por radicais para as equações de graus maiores que quatro, levantando diversos impasses que impediam o desenvolvimento destes resultados. Tal desafio frustrou muitos destes por séculos e contribuíram para a criação do conceito, do que futuramente, viria a ser chamado de “grupo”, como visto em Domingues e Iezzi (2003, p. 137).

Foi apenas em 1770-1771 que a questão começou a ser esclarecida com o ítalo-francês Joseph Louis Lagrange (1736-1813), na obra *Réflexions sur la résolution algébrique des équations* (Reflexões sobre a resolução algébrica de equações, 1770-1771), sendo este, em dois séculos, o primeiro matemático a perceber com lucidez (DOMINGOS e IEZZI, 2003) a dimensão do caminho necessário para solucionar o problema das resoluções das equações de graus maiores ou iguais a cinco, conseguindo notar a importância da Teoria das Permutações, referenciando-as como raízes da equação.

Lagrange, assim como o matemático Leonhard Euler (1707-1783) em 1750, tentaram aplicar o método de redução de Ferrari nas equações de grau cinco, mas ambos falharam neste feito. Em contrapartida entre os anos de 1803 e 1813, o médico italiano Paolo Ruffini (1725-1822) tentou provar que as raízes das quínticas não poderiam ser expressas por meio de seus

radicais, mas Ruffini, apesar de seus esforços, nunca conseguira provar de maneira suficiente os seus estudos.

Mesmo com vislumbre dado por Lagrange e Ruffini, foi em 1824 que o matemático Niels Henrik Abel (1802-1829), conseguira provar que não há nenhuma fórmula geral por meio de radicais para as equações de grau maior ou igual a 5, ou seja, não são resolúveis por radicais. Tal resultado é conhecido hoje como teorema de Abel-Ruffini (ou Ruffini-Abel), em homenagem a estes estudiosos.

O teorema provado por Abel não deu fim à procura de uma resposta para a solução das quínticas. Nesse processo, surge o jovem francês Évariste Galois (1811-1832), que em 1830 delineou o conceito de grupo, intitulando-o por esse mesmo nome. A ideia de Galois foi, em resumo, "associar a cada equação um grupo formado por permutações de suas raízes" (DOMINGUES e IEZZI, 2003, p. 138) condicionando-as a resolubilidade por radicais por propriedade do grupo, ressaltando o que foi dito por Lagrange em 1700-1701.

Évariste Galois, nascido em uma pequena comuna das redondezas da França conhecida como Bourg-la-Reine, em 1811. Aflorou um talento extraordinário para a matemática aos seus 15 anos (EVEES, 2011), mas apesar disto, foi recusado por duas vezes na Escola Politécnica por despreparo às exigências formais, até por confundir alguns professores com seus raciocínios rápidos, além de sua fama de arrogante. Galois, apesar da pouca idade, possuía uma grande facilidade para dominar as obras renomadas da Matemática como as de Lagrange, Gauss e Abel (D'AMBROSIO, 2021). Assim, pôde aprofundar seus estudos após ingressar na Escola Normal. Aos 17 anos de idade, tendo alcançado grandes resultados e os encaminhados para a Academia de Ciências, estas produções se extraviaram, o que aumentou ainda mais sua frustração. Em 1830, além da publicação do artigo que instaurou o verdadeiro início da Teoria de Grupos, o jovem francês se viu envolvido pela agitação dos movimentos democráticos da Revolução, no qual resultara a Galois a perda de sua vaga na escola, além de ter ficado meses recluso, sendo liberto em 1832, ano de sua morte.

Em sua obra, Eves (2011) traz algumas anedotas sobre Galois, inclusive sobre sua morte. Galois morreu precocemente aos 21 anos em um duelo motivado por uma relação amorosa. Sabendo que iria morrer, deixou em testamento científico em forma de carta a um amigo, Auguste Chevalier. Neste se abordava algumas de suas descobertas não-publicadas a serem aprofundadas, o que ocorreria futuramente graças a talentosos matemáticos presentes na história.

D'Ambrosio (2021) traz algumas versões diferentes sobre a causa real que motivou o duelo que matou Galois. Em uma delas é citado que o jovem francês haveria se voluntariado a

ser parte de um plano de revolução contra o retorno do governo dos Bourbons, no qual consistia na morte de um republicano conhecido o suficiente para incitar o povo contra os apoiadores dos contra partidário, os quais seriam atribuídos a culpa. O que não contavam era que a morte de um bonapartista ofuscaria a de Galois, fazendo com que sua morte se caracterizasse em suicídio, podendo dizer que “sua morte foi em vão” (D’AMBROSIO, 2021, p. 127).

O reconhecimento de Galois acerca destes estudos se deu, substancialmente após sua morte precoce e imprudente, quando Chevalier publicou suas descobertas na obra *Revue Encyclopédique* (SOUZA, 2020) e, por outros nomes que divulgaram suas memórias e manuscritos, tais como Joseph Liouville (1809-1882) e Camille Jordan (1838-1902).

Estes trabalhos foram de suma importância para a propagação da teoria de Galois, na qual os estudos foram sucessivamente levados por muitos outros grandes nomes na história da matemática como Augustin-Louis Cauchy (1789-1857), do qual fora sucedido por estudos de casos particulares. Arthur Cayley (1821-1899) considerado um dos precursores dos estudos dos grupos de forma abstrata. Cayley e outros grandes nomes foram responsáveis pela concretização da ideia de grupos e sua definição moderna como sendo um conjunto não vazio munido de uma operação binária que satisfaça as propriedades associativas e existência tanto do elemento neutro quanto dos elementos inversos.

Com o tempo se verificou a importância desta ideia dentro de muitos campos da matemática, como na Topologia Algébrica (SOUZA, 2020), na Análise Combinatória nos grupos de permutação e outras áreas da ciência, como na Física para dar embasamento matemático aos conceitos de simetria de cristais fundamentais na Espectroscopia e Cristalografia.

2 TEORIA DE GRUPOS

Este capítulo volta-se o olhar para a Teoria de Grupos como é trabalhada hoje, utilizando as definições e notações modernas desenvolvidas por Cayley e tantos outros matemáticos ao longo da história. Aqui estão os principais conceitos dentro da teoria, dando ênfase naqueles que se mostram mais necessários para o desdobramento do próximo capítulo.

2.1 Grupos

Um grupo é um conjunto não vazio munido de uma operação $*$ de tal modo que satisfaça algumas propriedades em relação a operação $*$. Nesse sentido, a definição formal é dada por:

Definição 2.1: Seja G um conjunto não vazio munido de uma operação qualquer $*$. $(G,*)$ é chamado de grupo se G for fechado para a operação $*$, ou seja, $\forall\, a, b \in G, a * b \in G$ de tal modo que satisfaça as seguintes propriedades:

i) Associativa;

$(a * b) * c = a * (b * c)$, para quaisquer $a, b, c \in G$.

ii) Existência de elemento neutro (e) da operação;

Existe um elemento $e \in G$ de tal modo que $a * e = e * a = a, \forall\, a \in G$.

iii) Existência de elemento simétrico;

Para todo $a \in G$ existe um a' de tal modo que $a * a' = a' * a = e$.

Satisfazendo estas condições, o conjunto $G \neq \emptyset$ munido da operação $*$ é chamado de Grupo.

Observação: Se o grupo ainda atender a propriedade comutativa em relação a operação de modo que ao tomar $a, b \in G$ tal que $a * b = b * a \in G$, o grupo é chamado de grupo Abeliano ou grupo comutativo.

Um grupo será denotado por $(G,*)$, sendo $*$ uma operação, ou apenas por G para melhor notação.

Exemplo 2.2: Um dos exemplos clássicos de grupo é o conjunto dos números Reais ($\mathbb{R}$) com a operação de adição, ou seja, $(\mathbb{R}, +)$ satisfaz:

i) Associatividade, pois sendo $a, b, c \in \mathbb{R}$ é válido que $(a + b) + c = a + (b + c)$;

ii) Existência do elemento neutro, tal que $a + 0 = 0 + a = a, \forall\, a \in R$;

iii) Existência do elemento simétrico, também chamado de elemento oposto $-a \in \mathbb{R}$ de modo que $a + (-a) = -a + a = 0, \forall\, a \in \mathbb{R}$.

É válido também a comutatividade da soma, uma vez que $a + b = b + a, \forall\, a, b \in \mathbb{R}$, logo $(\mathbb{R}, +)$ é um grupo Abeliano. ■

Outros conjuntos numéricos conhecidos também satisfazem a definição de grupo com determinadas operações, tais como $(\mathbb{R}^*, \cdot)$; $(\mathbb{Z}, +)$; $(\mathbb{Q}^*, \cdot)$, entre outros. Utiliza-se * para denotar que tomamos todos os elementos não nulos do conjunto.

Exemplo 2.3: O conjunto das matrizes quadradas reais denotado por $M_n(\mathbb{R})$ é um exemplo de grupo aditivo Abeliano, uma vez que a operação de adição de matrizes satisfaz a associatividade, a existência de elemento neutro, dada pela matriz nula, a matriz oposta representa o elemento simétrico da operação e, como as entradas das matrizes são números reais, é válida a comutatividade. Veja por exemplo as matrizes quadradas de ordem 2.

Sejam $M_2(\mathbb{R})$ o conjunto das matrizes quadradas 2 por 2 e $A, B, C \in M_2(\mathbb{R})$, de modo que

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}, B = \begin{bmatrix} f & g \\ h & i \end{bmatrix}, C = \begin{bmatrix} j & k \\ l & m \end{bmatrix}, \text{ onde } a, b, c, d, f, g, h, i, j, k, l, m \in \mathbb{R}.$$

Têm-se que $A + (B + C) = (A + B) + C$. De fato, pois

$$A + (B + C) = \begin{bmatrix} a & b \\ c & d \end{bmatrix} + \left(\begin{bmatrix} f & g \\ h & i \end{bmatrix} + \begin{bmatrix} j & k \\ l & m \end{bmatrix} \right)$$

$$= \begin{bmatrix} a & b \\ c & d \end{bmatrix} + \begin{bmatrix} f + j & g + k \\ h + l & i + m \end{bmatrix} = \begin{bmatrix} a + (f + i) & b + (g + k) \\ c + (h + l) & d + (i + m) \end{bmatrix}.$$

Dado que as entradas das matrizes são números reais, então é válido que

$$\begin{bmatrix} (a + f) + i & (b + g) + k \\ (c + h) + l & (d + i) + m \end{bmatrix} = \left(\begin{bmatrix} a + f & b + g \\ c + h & d + i \end{bmatrix} \right) + \begin{bmatrix} j & k \\ l & m \end{bmatrix} = (A + B) + C.$$

Considere $N = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$ a matriz nula, a qual representa o elemento neutro aditivo de $M_2(\mathbb{R})$. Tomando a matriz A já definida acima, tem-se que

$$A + N = N + A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} a + 0 & b + 0 \\ c + 0 & d + 0 \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} = A.$$

O elemento simétrico, ou também chamado de elemento oposto é dado pela matriz cuja as entradas correspondem aos elementos opostos aditivos da matriz dada, ou seja, ainda tomando a matriz $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$, tem-se que existe uma e única matriz $A' \in M_2(\mathbb{R})$ de modo que $A' = \begin{bmatrix} -a & -b \\ -c & -d \end{bmatrix}$, com $a, b, c,\ d \in \mathbb{R}$, tal que

$$A + A' = \begin{bmatrix} a & b \\ c & d \end{bmatrix} + \begin{bmatrix} -a & -b \\ -c & -d \end{bmatrix} = \begin{bmatrix} a + (-a) & b + (-b) \\ c + (-c) & d + (-d) \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} = N$$

Como vale a comutatividade, então $M_2(\mathbb{R})$ é um grupo Abeliano. De fato, sejam as matrizes $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}, B = \begin{bmatrix} f & g \\ h & i \end{bmatrix} \in M_2(\mathbb{R})$, têm-se que

$$A + B = \begin{bmatrix} a & b \\ c & d \end{bmatrix} + \begin{bmatrix} f & g \\ h & i \end{bmatrix} = \begin{bmatrix} a+f & b+g \\ c+h & d+i \end{bmatrix}$$

do qual sabe-se que as entradas são adições de números reais, do qual é válido a comutatividade, logo

$$= \begin{bmatrix} f+a & g+b \\ h+c & i+d \end{bmatrix} = B + A$$

Portanto, $M_2(\mathbb{R})$ é um grupo Abeliano. O mesmo se aplica de maneira análoga aos conjuntos de matrizes quadradas de qualquer ordem maior que 2. ■

Nota-se que o conjunto dos números inteiros com a operação de multiplicação, $(\mathbb{Z}, \cdot)$, não é um grupo multiplicativo, pois dado um inteiro $a \neq 0$ e $a \neq 1, -1$, a não possui inverso multiplicativo a' em $\mathbb{Z}$, uma vez que este é dado por $a \cdot a' = 1$ o que implica dizer que

$$a' = 1/a \Rightarrow a' \notin \mathbb{Z},$$

logo $(\mathbb{Z}, \cdot)$ não é um grupo.

De maneira semelhante, o conjunto dos Naturais $(\mathbb{N})$ não é um grupo aditivo ou multiplicativo pelo mesmo motivo. O conjunto não possui elementos simétricos aditivo ou multiplicativo.

Proposição 2.4: Um grupo qualquer admite algumas propriedades imediatas, tais como:

i) a unicidade do elemento neutro;

ii) a unicidade do elemento inverso de cada elemento de G;

iii) que o elemento inverso do elemento neutro é o próprio elemento neutro, ou seja, $e' = e$;

iv) $(a')' = a$, ou seja, é o próprio elemento a, $\forall\, a \in G$;

v) que todo elemento de G é regular em relação a operação $*$, ou seja, $a * b = a * c \Rightarrow b = c$ e $b * a = c * a \Rightarrow b = c$;

vi) o conjunto solução da equação $a * x = b$ é $S = \{a' * b\}$.

A seguir, provam-se algumas das propriedades.

Demonstração: i) Considere $e \in G$ o elemento neutro de G, logo $e * a = a * e = a,\ \forall\, a \in G$. Supondo por absurdo que exista um outro elemento $n \in G$ de modo que $n * a = a * n = a, \forall\, a \in G$. Desse modo, ao operar e e n têm-se que

$$e * n = n * e = e \text{ e } n * e = e * n = n.$$

Nesse sentido percebe-se que $e = n$ por serem expressos da mesma forma. Portanto o elemento neutro existe e é único.

De maneira análoga ocorre para a propriedade ii).

Sejam pois $a, a', e \in G$ de modo que $a * a' = a' * a = e$, sendo e o elemento neutro do grupo, e a' é simétrico a a.

Suponha então que exista um outro elemento $a'' \in G$ tal que $a'' * a = a * a'' = e$. Pela propriedade do elemento neutro, $a' = a' * e$, assim

$$a' = a' * (a * a'').$$

Pela associatividade dos elementos do grupo, tem-se que $a' = (a' * a) * a''$, de modo que $a' * a = e$, logo

$$a' = e * a'' \Rightarrow a' = a''.$$

Ficando assim provado a unicidade do elemento inverso para cada elemento pertencente ao grupo. ■

As demais propriedades, $iii)$, $iv)$, $v)$, e $vi)$ ficam a cargo do leitor. As suas demonstrações podem ser encontradas no terceiro e quarto capítulo da obra de Domingues e Iezzi (2003) e no quinto capítulo de Garcia e Lequain (2005).

Sendo assim, nas próximas seções serão abordados alguns grupos específicos que se mostram necessários para a continuidade dos desdobramentos do trabalho.

2.2 Grupo Finito

O estudo anterior foi feito de maneira geral, utilizando conjuntos infinitos conhecidos, a fim de facilitar a compreensão. Porém, ao tomar um conjunto finito, ou seja, com um número finito de elementos, e ao testar as propriedades necessárias de existência de grupo (fechado para operação, associatividade, existência dos elementos neutro e inversos), se todas estas forem satisfeitas, tal conjunto também se define como grupo. Um grupo finito, em que a quantidade de elementos presentes no conjunto representa a ordem deste grupo. Desse modo, Domingues e Iezzi (2003) trazem a seguinte definição de grupos finitos:

Definição 2.5: Um grupo $(G,*)$ em que G é um conjunto finito é chamado de grupo finito.

Sendo ainda o número de elementos de G chamado de *ordem do grupo* a qual denotamos por $o(G) = n < \infty$.

Exemplo 2.6: Um dos exemplos clássicos de grupos finitos é o conjunto $H = \{-1, 1\}$ com a operação de multiplicação usual em $\mathbb{Z}$. Nota-se que H é um conjunto finito, fechado para a operação de multiplicação, satisfaz a propriedade associativa em relação a operação; possui elemento neutro, o número 1, e todo elemento de H possui elemento inverso multiplicativo, de modo que o inverso do elemento neutro é ele mesmo e o inverso de -1 é o próprio -1, uma vez que $-1 \cdot (-1) = 1$, e ainda, H é um grupo Abeliano, pois vale a comutatividade, já que

$-1 \cdot 1 = 1 \cdot (-1) = -1$. Desse modo $(H, \cdot)$ é um grupo Abeliano e sua ordem é dada por $o(H) = 2$ por possuir apenas dois elementos. ■

Exemplo 2.7: Outro exemplo de grupo finito é o conjunto $J = \{-1, 1, i, -i\}$, onde $i \in \mathbb{C}$, $i^2 = -1$, em relação a operação de multiplicação usual em $\mathbb{C}$. J é fechado para a operação, vale a associatividade herdada dos números complexos, o elemento neutro é número 1 e todo elemento do conjunto possui inverso multiplicativo. De fato, $-1 \cdot (-1) = 1$ e $i \cdot (-i) = -i^2 = -(-1) = 1$, assim o inverso do elemento -1 é ele próprio e os elementos i e $-i$ são inversos entre si, pois quando operados entre si resultam no elemento neutro. Logo, $(J, \cdot)$ é um grupo do tipo finito de ordem igual a 4, já que possui quatro elementos, além de ser um grupo Abeliano. ■

2.3 Grupo de Classes Residuais

Definição 2.8: Sejam $a, b, m \in \mathbb{Z}$ com $m > 1$. A relação de congruência $a \equiv b \ (mod\ m) \Leftrightarrow a - b = km$, para algum m inteiro, define uma relação de equivalência em $\mathbb{Z}$, ou seja, valem as propriedades reflexiva, simétrica e transitiva.

É possível mostrar ainda que dois inteiros quaisquer são equivalentes se eles deixam mesmo resto na divisão euclidiana por m. Assim, define-se uma classe de resto $\bar{r}$, ou classe residual, módulo m, como sendo o conjunto de todos os inteiros que deixam o mesmo resto r na divisão euclidiana pelo inteiro positivo m.

É dito que esses números são côngruos $(mod\ m)$. Isto ocorre graças às propriedades de congruência modular dado um inteiro m. Desse modo, por exemplo, todos os números presentes na classe $\bar{0}$ deixam resto 0 quando são divididos por m. O mesmo ocorre com as demais classes modulares.

O conjunto dessas classes, o qual será denotado por $\mathbb{Z}_m$, é do tipo finito, uma vez que as classes são representadas pelos restos possíveis da divisão de um inteiro qualquer por m. Sabe-se que, pelo algoritmo de Euclides, r é maior ou igual a 0 e estritamente menor que m, isto é, seja o resto r da divisão, tem-se que $0 \leq r < m$, logo $0 \leq r \leq m - 1$, uma vez que são números inteiros. Portanto, o conjunto das classes residuais módulo m é representado por $\mathbb{Z}_m = \{\bar{0};\ \bar{1};\ \bar{2}; \ldots;\ \overline{m-1}\}$. Segundo Domingues e Iezzi (2003):

Definição 2.9: Para todo inteiro $m > 1$, temos que o conjunto de classes de restos módulo m, ou seja, $\mathbb{Z}_m = \{\bar{0};\ \bar{1};\ \bar{2}; \ldots;\ \overline{m-1}\}$, é o conjunto quociente de $\mathbb{Z}$ pela relação de congruência módulo m. Ou seja, é a classe dos restos da divisão euclidiana de $\mathbb{Z}$ por m de modo que, pelo algoritmo euclidiano, o resto r é obrigatoriamente $0 \leq r < m$.

Por definição (DOMINGUES e IEZII, 2003, p.135), as operações de adição e multiplicação em $\mathbb{Z}_m$ são tidas como: a soma das classes é a classe da soma e, de maneira análoga, o produto das classes é a classe do produto. Assim, ao tomar $\bar{a}, \bar{b}$ por duas classes residuais quaisquer pertencentes a $\mathbb{Z}_m$, tem-se a adição, ou soma, definida por $\bar{a} + \bar{b} = \overline{a+b}$ e a multiplicação por $\bar{a} \cdot \bar{b} = \overline{a \cdot b}$. É possível mostrar que essas operações estão bem definidas, isto é, não dependem dos representantes das classes, tal qual pode ser vista da seguinte forma:

Proposição 2.10: As operações de adição e multiplicação de classes estão bem definidas em $\mathbb{Z}_m$.

Demonstração: Sejam $\bar{a}, \bar{b}, \bar{x}, \bar{y} \in \mathbb{Z}_m$ tais que $\bar{a} = \bar{x}$ e $\bar{b} = \bar{y}$. Então, pela definição de congruência

$$a \equiv x \ (mod\ m) \text{ e } b \equiv y \ (mod\ m).$$

Desse modo, para algum $u, t \in \mathbb{Z}$

$$a - x = mu \text{ e } b - y = mt.$$

Então, para a adição das classes $\bar{a}$ e $\bar{b}$ se dá pela soma das igualdades, ou seja

$$(a - x) + (b - y) = mu + mt.$$

Evidenciando m e -1,

$$(a + b) - (x + y) = m(mu + t).$$

Ora, a expressão coincide com a definição de congruência, logo

$$a + b \equiv x + y \ (mod\ m).$$

Ou seja, a classe $\overline{a+b} = \overline{x+y}$, provando assim que a operação está bem definida.

Pode-se seguir o mesmo raciocínio para demonstrar que o produto das classes está bem definido, ou seja, que dado $\bar{a} = \bar{x}$ e $\bar{b} = \bar{y}$, então $\overline{a \cdot b} = \overline{x \cdot y}$. Tais observações podem ser encontradas na página 135 de Domingues e Iezzi (2003), contudo de maneira mais direta. ■

Em relação a soma, sabendo que a e b são números inteiros, é de imediato que são válidas as seguintes propriedades:

- Associatividade

$$\bar{a} + (\bar{b} + \bar{c}) = \overline{a + (b + c)} = (\bar{a} + \bar{b}) + \bar{c}, \ \forall\ \bar{a}, \bar{b}, \bar{c} \in \mathbb{Z}_m;$$

- Comutatividade

$$\bar{a} + \bar{b} = \overline{a+b} = \overline{b+a} = \bar{b} + \bar{a}, \ \forall\ \bar{a}, \bar{b}, \bar{c} \in \mathbb{Z}_m;$$

- Existência de elemento neutro, dado por $\bar{0}$, pois

$$\bar{a} + \bar{0} = \bar{0} + \bar{a} = \overline{a+0} = \overline{0+a} = \bar{a}, \ \forall\ \bar{a} \in \mathbb{Z}_m;$$

- Existência do elemento simétrico dado por $\overline{m-a}$, pois

$$\bar{a} + \overline{m-a} = \overline{a + (m-a)} = \overline{(a-a)+m} = \bar{m} = \bar{0}.$$

Tendo em vista que em relação de soma, o conjunto das classes residuais módulo m atende todas as propriedades necessárias da definição de grupo Abeliano, portanto $(\mathbb{Z}_m, +)$ é um grupo finito, comutativo e de ordem $o(\mathbb{Z}_m) = m$, para todo $m > 1$.

Exemplo 2.11: Como exemplo de grupo aditivo $\mathbb{Z}_m$ considere $(\mathbb{Z}_6, +)$, de modo que $\mathbb{Z}_6 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$. Ao tomar duas classes quaisquer, por exemplo $\bar{3}$ e $\bar{5}$, tem-se a soma definida por $\bar{3} + \bar{5} = \overline{3+5} = \bar{8}$, onde tem-se que a classe do $\bar{8}$ coincide com a classe do $\bar{2}$, pois na divisão euclidiana de 8 por 6 o resto é 2, logo $\bar{8} = \bar{2} \in \mathbb{Z}_6$. Ao tratar do elemento inverso aditivo vemos que, pela fórmula geral dada por $\overline{m-a}$, onde $m = 6$ e, a é igual ao elemento que se queira descobrir o seu oposto, uma vez que $m = \bar{m}$ e $a = \bar{a}$. Desse modo, ao tomar $a = 1$ chega-se que o seu inverso aditivo em $\mathbb{Z}_6$ dado por $\overline{m-a} = \overline{6-1} = \bar{5}$, de modo que $\bar{a} + \overline{m-a} = \bar{1} + \bar{5} = \overline{1+5} = \bar{6}$, onde a classe $\bar{6}$ coincide com a classe $\bar{0}$, ou seja, o elemento neutro da adição, isso porque 6 é múltiplo dele mesmo e logo deixa resto zero na divisão euclidiana por 6. Sendo os elementos de $\mathbb{Z}_m$ comutativos e pela propriedade da unicidade do elemento inverso, as classes $\bar{1}$ e $\bar{5}$ são inversas entre si, tal que $\bar{5} + \bar{1} = \bar{6} = \bar{0}$, ou seja, iguais ao elemento neutro aditivo.

Isto se aplica a todas as demais classes de $\mathbb{Z}_6$, de modo que as classes $\bar{4}$ e $\bar{2}$ são inversas aditivas entre si, a classe do $\bar{3}$ é inversa de si mesmo, a classe do $\bar{0}$, o elemento neutro da adição, é inverso de si mesmo, tal que $\bar{0} + \bar{0} = \overline{0+0} = \bar{0}$. ■

Analogamente, tendo definida a multiplicação como $\bar{a} \cdot \bar{b} = \overline{a \cdot b},\ \forall\ \bar{a}, \bar{b} \in \mathbb{Z}_m$, a qual também são válidas as propriedades associativa e comutativa de maneira semelhante a soma. Para esta operação o elemento neutro do conjunto é representado pela classe $\bar{1}$ de modo que $\bar{a} \cdot \bar{1} = \bar{1} \cdot \bar{a} = \overline{a \cdot 1} = \bar{a}$.

Proposição 2.12: Um elemento em $\mathbb{Z}_m$ possui inverso multiplicativo, ou seja, um elemento $\overline{a'} \in \mathbb{Z}$ de modo que $\bar{a} \cdot \overline{a'} = \bar{1}$ se, e somente se, o $mdc(a, m) = 1$, isto é, se a e m são primos entre si.

Demonstração:

($\rightarrow$) Temos que, $\bar{a} \in \mathbb{Z}_m$ possui inverso multiplicativo, $\exists\ \overline{a'} \in \mathbb{Z}_m$ tal que $\bar{a} \cdot \overline{a'} = \overline{a \cdot a'} = \bar{1}$, logo $\overline{a \cdot a'} \equiv \bar{1}\ (mod\ m)$, que por definição é expresso como $a \cdot a' - 1 = m \cdot q$, para algum $q \in \mathbb{Z}$. Note que

$$a \cdot a' - 1 = m \cdot q \Rightarrow a \cdot a' + (-q \cdot m) = 1$$

De modo que por uma proposição dos números primos[1], se dois números inteiros w, z se relacionam pela identidade $wx_0 + zy_0 = 1$ implica que w e z são primos entre si, logo, por assimilação têm-se que a e m são primos entre si.

($\leftarrow$) Dado que se $mdc(a,m) = 1$, tem-se que existe $x_0, y_0 \in \mathbb{Z}$ tal que $ax_0 + my_0 = 1$. Assim, $ax_0 - 1 = m(-y_0)$, que pela definição de congruência modular, têm-se que $ax_0 \equiv 1\ (mod\ m)$, de modo que $\bar{a} \cdot \overline{x_0} = \overline{a \cdot x_0} = \bar{1}$, ou seja, $\overline{x_0}$ é o inverso multiplicativo de $\bar{a}$. ■

Note que, uma vez que o $mdc(a,m) \neq 1$ então $\overline{a \cdot a'} \neq 1$. Logo, a e a' não são inversíveis, o que implica que nem todo elemento de $\mathbb{Z}_m$ possui inverso multiplicativo. Pode-se concluir que o conjunto das classes residuais módulo m só será um grupo em relação à multiplicação se m for um número primo.

Proposição 2.13: Seja $\mathbb{Z}_m$ o conjunto das classes residuais módulo m. $\mathbb{Z}_m^* = \mathbb{Z}_m \backslash \{\bar{0}\}$, munido da operação usual de multiplicação ($\cdot$) é um grupo multiplicativo se, somente se, m for um número primo.

Exemplo 2.14: O grupo $(\mathbb{Z}_5, \cdot)$ é um exemplo de grupo multiplicativo, de modo que: $\bar{0}$ por ser nulo não possui naturalmente inverso multiplicativo; $\bar{1}$ é simétrico a si mesmo tal que $\bar{1} \cdot \bar{1} = \bar{1}$; de maneira análoga ocorre para à classe do $\bar{4}$, pois $\bar{4} \cdot \bar{4} = \overline{16}$ que por conta da divisão euclidiana, deixa resto 1, logo $\overline{16} = \bar{1}$. E as classes $\bar{2}$ e $\bar{3}$ são simétricas entre si, dado que $\bar{2} \cdot \bar{3} = \bar{3} \cdot \bar{2} = \bar{6} = \bar{1}$. Ou seja, todos os elementos de $\mathbb{Z}_5$, com exceção do $\bar{0}$, possuem inverso multiplicativo, tais como as demais propriedades necessárias para que tornam $(\mathbb{Z}_5, \cdot)$ um grupo multiplicativo. ■

Apenas a quesito de apresentação, note que o conjunto $\mathbb{Z}_6$ não possuirá inverso multiplicativo para as classes não nulas $\bar{2}, \bar{3}$ e $\bar{4}$, sendo apenas o elemento neutro $\bar{1}$ e a classe $\bar{5}$ que possuem um elemento simétrico, de modo que $\bar{1} \cdot \bar{1} = \bar{1}$ e $\bar{5} \cdot \bar{5} = \overline{25} = \bar{1}$.

2.4 Grupo de Permutações

Permutação é um termo específico usado na teoria de grupos para designar uma bijeção de um conjunto nele mesmo. Considere E um conjunto não vazio no qual denota-se por $S(E)$ o conjunto de permutações dos elementos de E. A operação definida em $S(E)$ é a operação de composição de aplicações, pois sendo $f: E \to E$ e $g: E \to E$ bijeções, a composta $f \circ g$ continua sendo uma bijeção, devido propriedade de composição de aplicações. É conhecido que a composição de aplicações bijetoras é bijetora (DOMINGUES e IEZZI, p. 104).

[1] Ver DOMINGUES e IEZZI, 2003, p. 43.

Definição 2.15: Seja o conjunto não vazio E. Chamamos de permutação toda bijeção de um conjunto nele mesmo. O conjunto destas permutações, denotado por $S(E)$, munido da operação de composição ($\circ$), ao satisfazer a **Definição 2.1** é chamado de Grupo de Permutações.

A associatividade pode ser vista da seguinte forma: Sejam $f: E \to E$, $g: E \to E$ e $h: E \to E$, de modo que

$$[f \circ (g \circ h)](x) = f \circ g\big(h(x)\big) = f\Big(g\big(h(x)\big)\Big)$$

e

$$[(f \circ g) \circ h](x) = \big(f \circ g(x)\big) \circ h(x) = f\big(g(x)\big) \circ h(x) = f\Big(g\big(h(x)\big)\Big)$$

Logo, $f \circ (g \circ h)(x) = (f \circ g) \circ h(x), \forall x \in E$.

O elemento neutro de $S(E)$ é a aplicação identidade i_E tal que $i_E(x) = x, \forall\, x \in E$, dado que $(i_E \circ f)(x) = i_E(f(x)) = f(x),\ \forall x \in E$. E por fim a aplicação inversa, f^{-1}, é o elemento inverso da aplicação f, dado que toda aplicação bijetora possui aplicação inversa. Portanto, $(S(E),\ \circ)$ é um grupo chamado de grupo de permutações sobre E.

O grupo $S(E)$ só é comutativo quando $o\big(S(E)\big) = 1$ ou $o\big(S(E)\big) = 2$, o que pode ser visto da seguinte forma: Se o conjunto possui apenas um elemento, $S(E) = \{i_E\}$, i_E comuta consigo mesmo tanto pela direita quanto pela esquerda. Se possuir dois elementos, têm-se i_E comuta consigo mesmo, i_E comuta com f, no qual $S(E) = \{i_E, f\}$, $(i_E \circ f)(x) = i_E\big(f(x)\big) = f(x) = f\big(i_E(x)\big) = (f \circ i_e)(x),\ \forall\, x \in E$ e, por fim $(f \circ f)(x) = (f \circ f)(x) = f\big(f(x)\big), \forall\, x \in E$.

Nesse sentido, para demonstrar que a comutatividade não é válida para um grupo de permutações cuja $o\big(S(E)\big) \geq 3$, basta tomar as seguintes aplicações: Sejam $a, b, c \in E$ de modo que

$$f(a) = b,\ f(b) = a,\ f(x) = x,\ \forall x \neq a, b,$$
$$g(a) = c,\ g(c) = a,\ g(x) = x, \forall x \neq a, c.$$

Ao aplicar a composição destas aplicações, temos que

$$(f \circ g)(a) = f\big(g(a)\big) = f(c) = c$$
$$(g \circ f)(a) = g\big(f(a)\big) = g(b) = b.$$

Ou seja, $(f \circ g)(a) \neq (g \circ f)(a)$, logo não é válido a comutatividade para a operação de composição quando $o\big(S(E)\big) \geq 3$.

Quando o conjunto E é da forma $E = \{1, 2, \ldots, n\}$, ou seja, o conjunto numérico dos n primeiros números naturais, tem-se um caso particular do grupo de permutações chamado

Grupo simétrico de grau n, que é denotado por S_n. Pela Análise Combinatória, a ordem $o(S_n) = n!$, ou seja, o número possível de permutações de n elementos em uma relação biunívoca.

A notação utilizada para descrever os elementos de s_n será a seguinte: $f \in S_n$ tal que $f(1) = i_1$, $f(2) = i_2$, ..., $f(n) = i_n$. Permutação identidade é expressa da forma

$$i_E = \begin{pmatrix} 1 & 2 & \dots & n \\ 1 & 2 & \dots & n \end{pmatrix}.$$

Uma outra característica importante desta notação para os elementos do grupo S_n é que não importa a ordem com que os elementos aparecem nas colunas, sendo que

$$f = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 3 & 2 \\ 1 & 2 & 3 \end{pmatrix},$$

pois o que é notado é a relação formada, sendo que os elementos da primeira linha representam o domínio da aplicação, apresentados em ordem crescente apenas usualmente, e o elemento que se encontra abaixo de cada elemento do domínio dado é a imagem da aplicação, como por exemplo o 2 e o 3, pois nesse caso $f(2) = 3$ e $f(3) = 2$.

Exemplo 2.16: Ao tomar duas aplicações f e g pertencentes a S_3, tais que

$$f = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, g = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix},$$

tem-se que a composição das aplicações no grupo de simetria pode ser expressa como

$$g \circ f = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix},$$

pois $(g \circ f)(1) = g\big(f(1)\big) = g(2) = 2$; $(g \circ f)(2) = g\big(f(2)\big) = g(3) = 1$ e $(g \circ f)(3) = g\big(f(3)\big) = g(1) = 3$. ■

Exemplo 2.17: Um outro exemplo que pode ser dado são as permutações $\alpha, \beta \in S_4$ tais que

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}, \beta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}.$$

Tem-se que

$$\alpha\beta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} = i_E,$$

ou seja, igual a permutação identidade, logo dizemos que α e β são permutações inversas. ■

Utiliza-se $\alpha\beta$ sem a presença do símbolo $\circ$ para a simplificação da notação, mas ainda representa a operação de composição.

Nesse sentido, denota-se por α^m a composição de uma permutação $\alpha \in S_n$ por ela mesma m-vezes. Se m é o menor inteiro tal que $\alpha^m = i_E$, dizemos que a permutação α possui ordem m, que será denotada por $o(\alpha) = m$. Por exemplo a permutação $\alpha \in S_4$ do **Exemplo 2.17**,

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix},$$

de modo que

$$\alpha^2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} ; \ \alpha^3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix} ; \ \alpha^4 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} = i_E$$

Portanto, $m = 4$ é o menor número de vezes que a permutação α precisa operacionalizar consigo mesmo para retornar à permutação identidade, logo a ordem de α será $o(\alpha) = 4$. ■

2.5 Subgrupos

Dado que um grupo G é definido a partir de um conjunto e uma operação entre seus elementos, sabe-se que podem existir subconjuntos de G, dos quais pode ocorrer de que estes subconjuntos satisfaçam as mesmas propriedades em relação à operação munida ao conjunto. Em outras palavras, o subconjunto munido da mesma operação do grupo também é definido como grupo, sendo este chamado de subgrupo. Nesse sentido, tem-se:

Definição 2.18: Sejam $(G,*)$ um grupo e $H \subseteq G$ um subconjunto não vazio. Diz-se que H é um subgrupo de G se H for fechado para a operação $*$ e se $(H,*)$ também for um grupo. Neste caso, será denotado por $H \leq G$.

Se um subgrupo $H \subseteq G$ é necessariamente um grupo, então satisfaz a existência do elemento neutro, indicado por $e \in H$. Nesse sentido, o conjunto $\{e\}$ é um subgrupo, uma vez que satisfaz a definição. Têm-se também que o próprio grupo G é um subgrupo de si próprio. Estes dois subgrupos, $\{e\}$ e G, são chamados de subgrupos triviais.

Para definir um subgrupo H de G também pode-se utilizar a seguinte proposição:

Proposição 2.19: Seja $(G,*)$ um grupo, para que $H \subseteq G, H \neq \emptyset$, seja um subgrupo de G, é necessário e suficiente que $a * b' \in H$ sempre que $a, b \in H$, sendo b' o elemento simétrico de b.

Demonstração: ($\rightarrow$) Por hipótese têm-se que $(H,*)$ é um subgrupo de G. Considere e e e_h os elementos neutros de G e H, respectivamente. Se H é subconjunto de G, então e_h também pertence a G. Onde é válido para os elementos neutros que

$$e * e_h = e_h = e_h * e$$

ou seja, sendo os elementos de G regulares para a operação $*$, têm-se que $e = e_h$.

Seja $b \in H$ e considere que os elementos $b' \in G$ e $b'_h \in H$ seus simétricos em G e H relação a operação, de modo que

$$b'_h * b = e_h = e = b' * b.$$

Novamente pela regularidade dos elementos do grupo, tem-se que $b'_h = b'$.

Ora, se $a, b \in H$ então $a * b'_h \in H$, pois por hipótese H é um grupo, logo é fechado para as operações de seus elementos. Porém, como mostrado, $b'_h = b'$, portanto $a * b' \in H$.

($\leftarrow$) Como $H \neq \emptyset$, considere $x_0 \in H$. Por hipótese temos que $x_0 * x'_0 \in H$. Como $x_0 * x'_0 = e$, onde é o elemento neutro de G, então $e \in H$. Desse modo, considerando um elemento qualquer $b \in H$ e usando novamente a hipótese, tem-se que $e * b' = b' \in H$.

Agora, se $a, b \in H$, então $a * b' \in H$. Logo, H é fechado para a operação $*$, uma vez que $a * (b')' = a * b \in H$. A associatividade vale para todos os elementos de G, em particular vale para os elementos de H. Portanto, mostra-se que $H \subseteq G$ é um subgrupo de G. ■

Vejamos agora alguns exemplos.

Exemplo 2.20: Um dos exemplos clássicos de subgrupo é $(\mathbb{Z}, +)$ que é um subgrupo de $(\mathbb{R}, +)$, uma vez que os números inteiros são números reais. É possível mostrar que $\mathbb{Z}$ é fechado para a operação $(+)$ e também é um grupo, assim como visto no início do capítulo. ■

Exemplo 2.21: O subconjunto $2\mathbb{Z} = \{2x \mid x \in \mathbb{Z}\}$ o qual representa o conjunto dos números inteiros pares é um subgrupo de $(\mathbb{Z}, +)$. De imediato, nota-se que o subconjunto não é vazio, pois existe pelo menos o elemento neutro da adição, uma vez que $2 \cdot 0 = 0$. Observe ainda que o subconjunto é fechado para a operação de subtração. De fato, sejam quaisquer $a, b \in 2\mathbb{Z}$, então $a = 2k_1$ e $b = 2k_2$, para alguns $k_1, k_2 \in \mathbb{Z}$. Tem-se que, $a - b = 2k_1 - 2k_2 = 2(k_1 - k_2) \in 2\mathbb{Z}$. Portanto, pela **Proposição 2.19**, $2\mathbb{Z} \leq \mathbb{Z}$. ■

2.6 Grupo Cíclico

Antes de adentrar propriamente na definição de grupos cíclicos, é necessário compreender previamente a potência e múltiplos de elementos de um grupo.

Seja G um grupo multiplicativo. Têm-se por $a \in G$ e $m \in \mathbb{Z}$, a potência *m-ésima* de a de expoente m, ou seja, a^m é um elemento de G, do qual é definido a partir de:

(caso 1) se $m \geq 0$, temos $, a^0 = e$, sendo e o elemento neutro de G e, sendo $a^m = \underbrace{a \cdot a \cdot a \cdot \ldots \cdot a}_{m-vezes}$, ou seja, uma multiplicação sucessiva de a por ele mesmo m vezes. Desse modo, pode-se dizer também que a potência de a elevado ao expoente m pode ser escrito da forma $a^m = a^{m-1} \cdot a$, se $m \geq 1$.

(caso 2) se $m < 0$, temos que $a^m = (a^{-m})^{-1}$.

Nota-se que a^m é um elemento de G. Ora, $a \in G$, sendo G um grupo multiplicativo, o produto de a por a, m-vezes, também pertence a G uma vez que este é fechado para a operação.

Proposição 2.22: Seja G um grupo multiplicativo, $a \in G$ e $m, n \in \mathbb{Z}$, são válidas as seguintes propriedades:

$i)\ a^m\ a^n = a^{m+n}$;

$ii)\ (a^m)^n = a^{m \cdot n}$;

$iii)\ a^{-m} = (a^m)^{-1}$.

Será demonstrada apenas a propriedade $i)$, as demonstrações das demais podem ser consultadas em Domingues e Iezzi (2003), página 175.

Demonstração: Para provar $i)\ a^m\ a^n = a^{m+n}$, toma-se primeiramente $n = 0$. Desse modo, $a^m a^0 = a^m e = a^m$, e como m é um inteiro, logo pode ser escrito da forma $m = m + 0$ pois 0 é o elemento neutro da adição em $\mathbb{Z}$, assim $a^m a^0 = a^{m+0}$.

Supondo que seja válido $a^m\ a^n = a^{m+n}$ para $n \geq 0$ (hipótese de indução), prova-se que seja válido para o sucessor de n, ou seja, para $a^m\ a^{n+1} = a^{m+n+1}$. Por definição, $a^{n+1} = a^{n+1-1} \cdot a = a^n \cdot a$, então $a^m \cdot a^{n+1} = a^m \cdot a^n \cdot a$.

A partir da hipótese pode-se escrever $a^m a^n\ a = (a^{m+n})\ a$, que por sua vez, pela definição, mostra-se da forma a^{m+n+1}, sendo $m + n + 1$ um número inteiro, logo fica provado a propriedade $i)$. ■

Dessa maneira, é possível mostrar que o conjunto das potências de a por um inteiro m é um subconjunto de G e é denotado por $\langle a \rangle = \{a^m \mid m \in \mathbb{Z}\}$, de modo que $\langle a \rangle \neq \emptyset$, pois existe nele ao menos o elemento neutro expresso da forma $a^0 = e$.

Proposição 2.23: Dado um grupo G de modo que $a \in G$.

$i)$ o subconjunto $\langle a \rangle$ é um subgrupo de G e,

$ii)$ Se $H \leq G$ de modo que $a \in H$, então $\langle a \rangle \subset H$.

Demonstração: De fato, pois $i)$ por propriedade, $\langle a \rangle \neq \emptyset$, pois existe nele ao menos o elemento neutro. Nesse sentido, sejam $x, y \in \langle a \rangle$ no qual $x = a^m$ e $y = a^n$, para algum m e n inteiro. Assim, $xy^{-1} = a^m (a^n)^{-1} = a^m a^{-n} = a^{m-n}$, no qual $m - n$ é inteiro, logo $xy^{-1} \in \langle a \rangle$, qualificando $\langle a \rangle$ como subgrupo de G.

Quando $ii)$ dado que $a \in H$, então toda potência de a também pertence a H, uma vez que a potência é uma operação sucessiva de um elemento com ele mesmo e, H por ser um subgrupo é fechado para operação, por tanto $\langle a \rangle \subset H$. ■

Dessa maneira, sendo $\langle a \rangle$ um subgrupo, chamamos de ordem de a, menor inteiro $m > 0$ tal que $a^m = e$, de modo que $\langle a \rangle = \{a, a^2, \dots, a^m\}$.

Cabe citar que, subgrupos cíclicos podem ser infinitos, onde apenas $m = 0$ capaz de $a^m = e$.

Quando ocorrer que subgrupo $\langle a \rangle$ coincida com o grupo G, ou seja, formando um subconjunto de G de modo que seja estritamente igual a este, é dito que o grupo G é *cíclico em*

a e, o elemento a é chamado de *gerador* do grupo. Assim, observa-se a definição formal a seguir.

Definição 2.24: Seja G um grupo multiplicativo e $\langle a\rangle$ o subconjunto de G constituído pelas potências inteiras de a, sendo a um elemento qualquer de G, tal que $\langle a\rangle = \{a^m \mid m \in Z\}$. G é chamado de grupo cíclico se, e somente se, $G = \langle a\rangle$, para algum $a \in G$, ou seja, $G = \{a^m \mid m \in \mathbb{Z}\}$. Se é válida a igualdade, então a é chamado de *gerador* do grupo G.

Exemplo 2.25: Considere a permutação $f = \begin{pmatrix}1 & 2 & 3\\ 3 & 1 & 2\end{pmatrix}$ pertencente ao grupo simétrico S_3. Veja o subgrupo gerado por f, o $\langle f\rangle$, no qual denota-se a permutação identidade por f_0. Desse modo, têm-se que

$$f^2 = f \circ f = \begin{pmatrix}1 & 2 & 3\\ 3 & 1 & 2\end{pmatrix} \circ \begin{pmatrix}1 & 2 & 3\\ 3 & 1 & 2\end{pmatrix} = \begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix},$$

$$f^3 = f \circ f^2 = \begin{pmatrix}1 & 2 & 3\\ 3 & 1 & 2\end{pmatrix} \circ \begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix} = \begin{pmatrix}1 & 2 & 3\\ 1 & 2 & 3\end{pmatrix} = f_0.$$

Logo, o subgrupo $\langle f\rangle = \{f, f^2, f^3 = f_0\}$, sendo cíclico a partir de $m = 3$. ■

Exemplo 2.26: Um exemplo já citado anteriormente (**Exemplo 2.7**), mas o qual convém citá-lo novamente pela sua estrutura é o grupo multiplicativo $J = \{-1,\ 1,\ i, -i\}$ das raízes quárticas da unidade. Nota-se que tomando as potências do elemento i, dado que $i^2 = -1$, constroem-se todos os elementos de J, de modo que se há $i^0 = 1$; $i^1 = i$; $i^2 = -1$ e $i^3 = -i$. Logo o subconjunto $\langle i\rangle = J$, sendo assim J um grupo cíclico gerado por i. ■

Nesse sentido, ocorre de maneira análoga, dado um grupo aditivo G de modo que exista um elemento $a \in G$ e um inteiro m. O múltiplo m-ésimo de a é um elemento do grupo da forma $a \cdot m$, uma vez que, pela propriedade de multiplicação usual

$$a \cdot m = \underbrace{a + a + \cdots + a}_{m-vezes}.$$

Se $m \geq 0$, tem-se que, para $m = 0$, então $m \cdot a = 0 \cdot a = e$, ou seja, igual ao elemento neutro da adição. Porém quando $m \geq 1$, têm-se que o múltiplo m-ésimo do elemento a também pode ser escrito da forma $a \cdot m = (m-1) \cdot a + a$. Se $m < 0$, então $m \cdot a = -[(-m) \cdot a]$

De maneira semelhante a potência, nos múltiplos são válidas algumas propriedades base das quais se pontuam:

Proposição 2.27: Sejam G um grupo aditivo, $a \in G$ e $m \in \mathbb{Z}$ um inteiro qualquer, são válidas as seguintes propriedades:

$i)\ m \cdot a + n \cdot a = (m+n) \cdot a;$

$ii)\ (-m) \cdot a = -(m \cdot a);$

$iii)\ n \cdot (m \cdot a) = (m \cdot n) \cdot a.$

Tal qual feito anteriormente, será mostrada apenas a propriedades i), ficando a cargo do leito as demais.

i) Seja $n = 0$, têm-se que $m \cdot a + 0 \cdot a = m \cdot a + 0 = m \cdot a$ que é o mesmo de dizer que $(m + 0) \cdot a$, pois $m + 0$.

Supondo que seja i) é válido $n \geq 1$, prova-se que é válido para um $n + 1$, ou seja, para $m \cdot a + (n + 1) \cdot a$.

Por hipótese, pode ser reescrito como $m \cdot a + n \cdot a + 1 \cdot a$, de tal modo que é igual a $(m + n) \cdot a + 1 \cdot a = (m + n) \cdot a + a$, ou seja, um múltiplo de $m + n + 1$, logo se iguala ao $(m + n + 1) \cdot a$, ficando assim provado a validade da propriedade i). ■

Logo, de maneira semelhante à definição para grupos multiplicativos $\langle a \rangle = \{m \cdot a \mid m \in \mathbb{Z}\} = \{(m - 1) \cdot a + a | \, m \in \mathbb{Z}\}$, ou seja, o conjunto dos múltiplos do elemento $a \in G$. Se o subconjunto $\langle a \rangle$ coincidir com o grupo G é dito que G é cíclico em a, o qual é chamado de gerador do grupo.

Dois exemplos clássicos para grupos aditivos cíclicos são os grupos $(\mathbb{Z}, +)$ e o $(\mathbb{Z}_m, +)$.

Exemplo 2.28: Tem-se que qualquer número inteiro é múltiplo de 1 ou -1, isto é, $m \in \mathbb{Z}$, então $m = m \cdot 1$ ou $m = m \cdot (-1)$. Assim, $\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle$. ■

Exemplo 2.29: De maneira análoga, mostra-se que o grupo aditivo $\mathbb{Z}_m$ é um grupo cíclico. De fato, qualquer classe $\bar{n} \in \mathbb{Z}_m$ é múltiplo da classe $\bar{1}$, isto é, $\bar{n} = \bar{n} \cdot \bar{1} = \overline{n \cdot 1}$. Logo, $\mathbb{Z}_m$ é gerado pela classe $\bar{1}$, ou seja, $\mathbb{Z}_m = \langle \bar{1} \rangle = \{\bar{n} \cdot \bar{1} \mid n \in \mathbb{Z}\}$. ■

2.7 Classes Laterais

Esta unidade atenta-se a definir e exemplificar o conceito de Classes Laterais, um dos pontos chaves para o desenvolvimento e compreensão do Teorema de Lagrange na próxima unidade.

Proposição 2.30: Sejam G um grupo e $H \leq G$. A relação em G definida por $a \, R \, b \Leftrightarrow a^{-1}b \in H$, $\forall a, b \in G$, é uma relação de equivalência de H em G.

Demonstração: De fato, pois segue que a relação R dos elementos de H assume as propriedades

i) Reflexiva, de modo que $a \, R \, a \Leftrightarrow a^{-1}a = e \in H$, pois H é subgrupo e necessariamente o elemento neutro do grupo pertence a G;

ii) Simétrica, no qual se $a \, R \, b \Rightarrow b \, R \, a$, ou seja, que se $a^{-1}b \in H$ então $b^{-1}a \in H$, por certo, pois dado que $a^{-1}b \in H$, então o seu simétrico $(a^{-1}b)^{-1}$ também pertence. Porém, através de propriedade $(a^{-1}b)^{-1} = a^{-1^{-1}}b^{-1} = ab^{-1} = b^{-1}a \in H$, logo têm-se que $b \, R \, a$;

iii) Transitiva, tal que dado $a\,R\,b$ e $b\,R\,c \Rightarrow a\,R\,c$. E de certo, pois sendo H um subgrupo e tendo $a^{-1}b \in H$ e $b^{-1}c \in H$, ou seja, elementos de H, logo válidos para a operação, de modo que $a^{-1}bb^{-1}c \in H$. Ora, pela associatividade dos elementos têm-se que $a^{-1}(bb^{-1})c = a^{-1}ec$, no qual e é o elemento neutro, logo $a^{-1}c \in H \Rightarrow a\,R\,c$. Desse modo, é tido que R é uma relação de equivalência a qual será denotada a partir deste ponto por $a \approx b$.■

Definição 2.31: Seja H um subgrupo não trivial do G tal que $a \in G$. A classe de equivalência de a é conjunto aH, no qual $\bar{a} = \{b \in G \mid a \approx b\} = \{b \in G \mid a^{-1}b \in H\} = \{b \in G \mid a^{-1}b = h\} = \{ah \mid h \in H\} = aH$ é chamada classe lateral à esquerda, módulo H, determinado por a.

De forma análoga, define-se, classe lateral à direita, módulo H tal que, $Ha = \{b \in G \mid ba^{-1} \in H\} = \{b \in G \mid ba^{-1} = h\} = \{ha \mid h \in H\}$. Toda a teoria aqui exposta é válida tanto para classes laterais à direita quanto à esquerda. Nesse sentido, para o desenvolvimento e por simplicidade, toma-se neste trabalho por se utilizar apenas classes laterais à esquerda e chamando-as apenas por classes laterais.

Contudo, é conhecido que as classes laterais formam uma partição de G, isto é, se $a, b \in G$, então $aH = bH \neq \emptyset$ ou $aH \cap bH = \emptyset$, ou seja, ou as classes laterais são disjuntas ou elas são iguais e que a união de todas as classes laterais distintas é igual ao grupo G. Dessa forma, denota-se o quociente $G/H = \{\text{classes laterais módulo H}\}$ e, $(G:H)$ o índice de H em G, o número de classes laterais.

Observe que se G for um grupo Abeliano, então as classes laterais à esquerda e à direita coincidem, ou seja, $aH = Ha, \forall\, a \in G$. E de fato, pois sendo G um grupo Abeliano, tem-se que $ag = ga, \forall a, g \in G$, logo vale em particular para os elementos do subgrupo H de G, ou seja, $ah = ha, \forall a \in G$. Portanto, as classes laterais são iguais.

Note que, a recíproca não é válida. Considerando o $G = S_3$, grupo de permutações e $H = \left\{i_E = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}\right\} \leq G$. Tomando uma permutação $j \in G$ qualquer, tem-se que $jH = Hj$, pois H é definido apenas pelo elemento neutro da composição (i_E), mas sabe-se que o grupo S_3 não é um grupo Abeliano.

Um resultado importante dentro do estudo das classes laterais é de que classes laterais distintas de mesmo módulo possuem a mesma cardinalidade, sendo esta igual à ordem do subgrupo que gera a classe. A demonstração deste resultado se dá a partir de uma bijeção de uma aplicação entre classes laterais, de modo que, os conjuntos de uma aplicação bijetora são todos representados um a um, ou seja, possuem a mesma cardinalidade. A seguir é apresentado tanto a definição formal quanto a demonstração das duas afirmações.

Proposição 2.32: Sejam G um grupo e H um subgrupo qualquer. As classes laterais distintas, módulo H possuem mesma cardinalidade de H.

Demonstração: Sendo $a \in G$, têm-se que para demonstrar tal proposição toma-se duas classes laterais, ah e bh, de modo que uma aplicação f dada por

$$f: \begin{matrix} aH \to bH \\ ah \mapsto bh \end{matrix}, \qquad \forall\, h \in H$$

é uma bijeção.

De fato, pois considerando quaisquer dois elementos h, h_1, têm-se que $f(ah) = f(ah_1)$, que pela definição da aplicação resulta em $bh = bh_1$. Sendo b elemento do grupo então este é regular para a operação então $b^{-1}bh = b^{-1}bh_1$, o que implica dizer que $h = h_1$, portanto f é injetora.

Desse modo, seja $y \in bH$, então $y = bh$, para algum $h \in H$. Nesse sentido, ao tomar $x = ah \in aH$, têm-se que $f(x) = f(ah) = bh = y$. Logo a aplicação é sobrejetora e, portanto f é uma bijeção.

Por ser uma bijeção, ambos os conjuntos, domínio e contradomínio, são totalmente representados de 1 em 1 elementos, logo os conjuntos possuem a mesma cardinalidade (DOMINGUES e IEZZI, 2003, p.161), neste caso, classes laterais de mesmo módulo possuem a mesma cardinalidade.

Porém, sabe-se que em particular existe a classe lateral, módulo H, gerada pelo elemento neutro e, de modo que $eH = H$, portanto todas as classes laterais possuem cardinalidade igual ao do subgrupo H. ■

Cabe reforçar que, assim como para toda a teoria, este caso é válido não apenas para classes laterais à esquerda, mas também para classes laterais à direita, dado que a sobrejetividade continua válida, assim como a injetividade, uma vez que se chegará na mesma situação em que ambas as parcelas serão expressas como múltiplos do elemento do subgrupo, o qual é regular para a operação e resultará que os elementos são iguais.

Exemplo 2.33: Sejam o grupo $(\mathbb{Z}_8, +)$ e $H = \{\overline{0}, \overline{2}, \overline{4}, \overline{6}\}$ um dos seus subgrupos. A classe lateral à esquerda definida pelo elemento $\overline{2}$ se mostra da forma $\overline{2} + H = \overline{2} + \{\overline{0}, \overline{2}, \overline{4}, \overline{6}\}$ que resulta em $\{\overline{2} + \overline{0}, \overline{2} + \overline{2}, \overline{2} + \overline{4}, \overline{2} + \overline{6}\} = \{\overline{2}, \overline{4}, \overline{6}, \overline{0}\}$. Definindo a partir da classe $\overline{3}$ temos que $\overline{3} + H = \{\overline{3} + \overline{0}, \overline{3} + \overline{2}, \overline{3} + \overline{4}, \overline{3} + \overline{6}\} = \{\overline{3}, \overline{5}, \overline{7}, \overline{1}\}$. Desse modo, conclui-se que $\mathbb{Z}_8/H = \{\overline{2} + H, \overline{3} + H\}$.

Exemplo 2.34: Outros exemplos que podem ser aplicados são os que derivam do grupo multiplicativo dos números reais. Seja o grupo multiplicativo $(\mathbb{R}^*, \cdot)$ e o subgrupo $\langle 2 \rangle =$

$\{2^n \mid n \in \mathbb{Z}\} = \{\ldots, \frac{1}{4}, \frac{1}{2}, 1, 2, 4, \ldots\}$. A classe lateral π módulo $\langle 2\rangle$ é escrita da forma $\pi\langle 2\rangle = \{\pi \cdot 2^n \mid n \in \mathbb{Z}\} = \{\ldots, \pi \cdot \frac{1}{4}, \pi \cdot \frac{1}{2}, \pi \cdot 1, \pi \cdot 2, \pi \cdot 4, \ldots\} = \{\ldots, \frac{\pi}{4}, \frac{\pi}{2}, \pi, \pi 2, \pi 4, \ldots\}$. Como o grupo $\mathbb{R}^*$ é comutativo, tem-se que $\pi\langle 2\rangle = \langle 2\rangle\pi$. ■

Exemplo 2.35: Seja o grupo simétrico de grau 3, $S_3 = \{i_E, f, g, h, j, k\}$, onde i_E representa a permutação identidade e

$$f = \begin{pmatrix}1 & 2 & 3\\ 1 & 3 & 2\end{pmatrix}, g = \begin{pmatrix}1 & 2 & 3\\ 2 & 1 & 3\end{pmatrix}, h = \begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix}, j = \begin{pmatrix}1 & 2 & 3\\ 3 & 1 & 2\end{pmatrix}, k = \begin{pmatrix}1 & 2 & 3\\ 3 & 2 & 1\end{pmatrix}.$$

Tomemos o subgrupo cíclico $J = \langle j\rangle = \{j, j^2, j^3 = i_E\}$, onde

$$j^2 = j \circ j = \begin{pmatrix}1 & 2 & 3\\ 3 & 1 & 2\end{pmatrix} \circ \begin{pmatrix}1 & 2 & 3\\ 3 & 1 & 2\end{pmatrix} = \begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix}$$

$$j^3 = j \circ j^3 = \begin{pmatrix}1 & 2 & 3\\ 3 & 1 & 2\end{pmatrix} \circ \begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix} = \begin{pmatrix}1 & 2 & 3\\ 1 & 2 & 3\end{pmatrix} = i_E\ .$$

Desse modo, as classes laterais de S_3 com módulo J são expressas por

$$i_E J = \{i_E \circ j, i_E \circ j^2, j^3\} = \left\{\begin{pmatrix}1 & 2 & 3\\ 3 & 1 & 2\end{pmatrix}, \begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix}, \begin{pmatrix}1 & 2 & 3\\ 1 & 2 & 3\end{pmatrix}\right\} = J$$

$$fJ = \{f \circ j, f \circ j^2, f\} = \left\{\begin{pmatrix}1 & 2 & 3\\ 2 & 1 & 3\end{pmatrix}, \begin{pmatrix}1 & 2 & 3\\ 3 & 2 & 1\end{pmatrix}, \begin{pmatrix}1 & 2 & 3\\ 1 & 3 & 2\end{pmatrix}\right\}$$

$$gJ = \{g \circ j, g \circ j^2, g\} = \left\{\begin{pmatrix}1 & 2 & 3\\ 3 & 2 & 1\end{pmatrix}, \begin{pmatrix}1 & 2 & 3\\ 1 & 3 & 2\end{pmatrix}, \begin{pmatrix}1 & 2 & 3\\ 2 & 1 & 3\end{pmatrix}\right\}$$

$$hJ = \{h \circ j, h \circ j^2, h\} = \left\{\begin{pmatrix}1 & 2 & 3\\ 1 & 2 & 3\end{pmatrix}, \begin{pmatrix}1 & 2 & 3\\ 3 & 1 & 2\end{pmatrix}, \begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix}\right\}$$

$$kJ = \{k \circ j, k \circ j^2, k\} = \left\{\begin{pmatrix}1 & 2 & 3\\ 1 & 3 & 2\end{pmatrix}, \begin{pmatrix}1 & 2 & 3\\ 2 & 1 & 3\end{pmatrix}, \begin{pmatrix}1 & 2 & 3\\ 3 & 2 & 1\end{pmatrix}\right\}$$

$$jJ = \{j \circ j, j \circ j^2, j\} = \left\{\begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix}, \begin{pmatrix}1 & 2 & 3\\ 1 & 2 & 3\end{pmatrix}, \begin{pmatrix}1 & 2 & 3\\ 3 & 1 & 2\end{pmatrix}\right\}.$$

Nota-se que $iJ = hJ$ e $fJ = gJ = kJ = jJ$. Desse modo, $S_3/J = \{hJ, fJ\}$, sendo estas as classes que descrevem o conjunto S_3. ■

3 TEOREMA DE LAGRANGE E APLICAÇÕES

Joseph Louis Lagrange, nasceu em Turim na Itália no ano de 1736, sendo o único de 11 filhos de uma família de descendência francesa a conseguir atingir a idade adulta. Teve seus estudos em sua cidade natal, tornando-se professor de matemática muito jovem numa academia militar também local.

Não demorou muito para que a fama de Lagrange crescesse, conforme divulgava seus trabalhos, sendo considerado um dos dois maiores matemáticos do século XVIII juntamente com Euler (EVES, 2011).

Em 1766, Euler deixou a corte alemã de Frederico, o Grande, que convidou Lagrange a ocupar o lugar vago, o qual não só aceitou como serviu a Frederico por 20 anos. Poucos anos após deixar Berlim, lecionou na Escola-Normal, a qual ficou conhecida futuramente como Escola Politécnica de Paris, onde diversos matemáticos da modernidade estudaram e/ou lecionaram, sendo Lagrange um dos responsáveis pela tradição de matemática elevada com que era conhecida a instituição.

Muito se deve a Lagrange aos estudos da Matemática que é conhecida hoje, pois seus trabalhos, os quais apresentavam um rigor matemático e uma escrita sucinta, tiveram muita influência no que dita as pesquisas matemáticas em diversas áreas, tendo seus escritos perpassados pela Análise, Álgebra e na Teoria dos Números, e que serviram como alicerce para muitos estudiosos, como por exemplo a Galois no desenvolvimento da Teoria de Grupos, na qual um importante resultado nesta teoria carrega o nome de Lagrange.

Desse modo, o teorema a seguir, apesar do nome, não foi demonstrado por Lagrange propriamente dito, pois em sua contemporaneidade o conceito de grupo não fora ainda desenvolvido. O matemático apenas utilizou este resultado em uma situação particular de seus estudos sobre as quínticas, no qual trabalhava em uma ligação entre as soluções algébricas das equações polinomiais e a permutações das raízes destas equações, sendo demonstrado completamente pelo matemático Pietro Abbati (1768-1842), 30 anos após que Lagrange o enunciou.

Este Teorema nomeado como Teorema de Lagrange define que, dado um grupo finito e um subgrupo, estes se relacionam de modo que a ordem do grupo é igual ao produto da ordem do subgrupo pelo índice do grupo pelo subgrupo, ou seja, a ordem do subgrupo divide a ordem do grupo. Lembrando que o índice do grupo G pelo subgrupo H é o número de classes laterais de H em G, também chamadas de classes laterais à esquerda módulo H.

Nesse sentido, o teorema de Lagrange anuncia-se como:

Teorema 3.1 (Teorema de Lagrange): Sejam G um grupo finito e H um subgrupo de G. Então $o(G) = o(H)(G:H)$, isto é, $o(H) \mid o(G)$.

Demonstração: Tomando o grupo finito G e o subgrupo $H \leq G$, supõe-se que o índice de H em G, $(G:H) = n$, com $n \in \mathbb{Z}, n > 0$. Tal qual mostrado anteriormente, o grupo G pode ser representado pela união de todas as classes laterais à esquerda disjuntas módulo H, logo $G/H = a_1H \cup a_2H \cup \ldots \cup a_nH$.

Assim como mostrado no capítulo anterior, tem-se que todas as classes laterais disjuntas módulo H, possuem a mesma cardinalidade e iguais a ordem do subgrupo H. Segue que

$$o(G) = \underbrace{o(H) + o(H) + \ldots + o(H)}_{n\ vezes}.$$

Por se tratar de uma soma sucessiva da $o(H)$ por ela mesma n vezes, tem-se por propriedade da operação de multiplicação que $o(G) = o(H) \cdot n$. Porém, por hipótese, temos que $n = (G:H)$, logo

$$o(G) = o(H)(G:H).$$

Sendo assim, a $o(G)$ é um múltiplo da $o(H)$, isto é,

$$o(H) \mid o(G). \qquad \blacksquare$$

A partir deste teorema, emergem algumas aplicações importantes relacionados a grupos finitos.

Corolário 3.2: Sendo G um grupo finito, então a ordem de um elemento $a \in G$ divide a ordem de G e o quociente é $(G:H)$, de modo que $H = \langle a \rangle$.

Demonstração: De fato, considere $H = \langle a \rangle$ o subgrupo cíclico de G gerado por a. Temos que a ordem do elemento a é igual a cardinalidade de H. Portanto, pelo Teorema de Lagrange, a ordem de a divide a ordem de G, ou seja $o(G) = (G:H) \cdot o(a)$. $\blacksquare$

Corolário 3.3: Se a é um elemento do grupo finito G, então $a^{o(G)} = e$, ou seja, igual ao elemento neutro de G.

Demonstração: Ora, sendo h a ordem de a, é tido que h é o menor inteiro positivo tal que $a^h = e$. Pelo **Corolário 3.2** sabe-se que $o(G) = (G:H)h$, onde $h = \langle a \rangle$. Desse modo

$$a^{o(G)} = a^{(G:H)h} = (a^h)^{(G:H)} = e^{(G:H)} = e. \qquad \blacksquare$$

Corolário 3.4: Seja G um grupo finito de ordem igual a um número primo. Então G é cíclico e os únicos subgrupos de G são os triviais, ou seja, $\{e\}$ e o próprio G.

Demonstração: Dado que $o(G) = p$, com p primo, logo existe um elemento $a \neq e$. Tomemos pois $H = \langle a \rangle$, o subgrupo gerado por a.

Uma vez que o Teorema de Lagrange garante que $o(H) \mid o(G)$, então ou $o(H) = 1$ ou $o(H) = p$, dado que p é um número primo. Logo ou $H = \{e\}$ ou $H = G$. Porém, como que por hipótese $a \neq e$, então $H = \{e\}$ não é possível pela definição do subgrupo, assim $H = G$ e, portanto, G é um grupo cíclico gerado por a.

De maneira semelhante, sendo $J \leq G$, pelo **Teorema 3.1** temos que $o(J) \mid o(G)$, então ou $J = \{e\}$ ou $J = \{G\}$, ou seja, J é um subgrupo trivial. ■

Exemplo 3.5: Considere o grupo aditivo das classes residuais módulo 8, $\mathbb{Z}_8 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \dots, \bar{7}\}$, de ordem igual 8. Desse modo, pelo Teorema de Lagrange, os possíveis subgrupos de $\mathbb{Z}_8$ possuem ordens $1, 2, 4$ e 8. Os subgrupos de ordem 1 e 8 são os subgrupos triviais $\{\bar{0}\}$ ou $\mathbb{Z}_8$, respectivamente. Agora vejamos os subgrupos de ordem 2 e 4, dos quais tornam-se simples descobrir quais são.

Assim, para determinar um subgrupo de ordem 4, tome o elemento $\bar{2}$, por exemplo, do qual sua ordem é 4, pois $4 \cdot \bar{2} = \bar{8} = \bar{0}$. Logo é possível gerar um subgrupo $H = \langle \bar{2} \rangle = \{\bar{0}, \bar{2}, \bar{4}, \bar{6}\}$ de G, o que implica dizer que a $o(H) = o(\bar{2}) = 4$. Note que é possível criar outros subgrupos de ordem 4 a partir do elemento $\bar{6}$, ao multiplicados por 4 resulta em um múltiplo de oito, retornando assim para o elemento neutro, $\bar{0}$.

Ao voltar o olhar para o elemento $\bar{4}$, nota-se que este é capaz de gerar um subgrupo Q de ordem dois, pois $\langle \bar{4} \rangle = \{0 \cdot \bar{4}, 1 \cdot \bar{4}, 2 \cdot \bar{4}, 3 \cdot \bar{4}, 4 \cdot \bar{4}\} = \{\bar{0}, \bar{4}, \bar{8}, \overline{12}, \overline{16}\} = \{\bar{0}, \bar{4}\} \coloneqq Q$. ■

Exemplo 3.6: Seja K o grupo de Klein[2] definido a partir de um conjunto $K = \{e, a, b, c\}$ e uma operação $*$ de tal forma que os elementos de K se comportam da seguinte maneira à operação:

i) toma-se e como elemento neutro do conjunto de modo que $e * a = a * e = a$;

ii) todo elemento é seu próprio simétrico, ou seja, $a * a = e$, $b * b = e$ e $c * c = e$, o que leva dizer que cada elemento possui ordem 2.

iii) a operação entre dois elementos distintos, que não seja e, resulta no terceiro elemento do conjunto diferente do neutro, ou seja, $a * b = c$; $a * c = b$ e $b * c = a$.

Nota-se ainda que os elementos de K atendem a propriedade associativa, de modo que tomando $a * (b * c) = a * a = e$ e, $(a * b) * c = c * c = e$ para qualquer disposição dos elementos do conjunto e, $a * b = c = b * a$, valendo assim também a comutatividade.

[2] Desenvolvido pelo matemático alemão Felix Christian Klein (1849-1925), o qual se dedicava aos estudos tanto na Geometria não euclidianas quanto na ligação entre a Geometria e a Teoria de Grupos.

Dessa maneira, têm-se que $(K,*)$ é um grupo Abeliano no qual possui $o(K) = 4$. Pelo Teorema de Lagrange, os possíveis subgrupos de K possuem ordens $1, 2$ e 4. Os subgrupos de ordem 1 e 4 são os subgrupos triviais, $\{e\}$ e K, respectivamente. Vejamos agora os subgrupos de ordem 2.

Nesse sentido, ao tomar um elemento a, o qual sabe-se que sua ordem é igual a 2 o subgrupo cíclico gerado por a, $H = \langle a \rangle = \{e, a\}$, possui ordem 2, assim como os subgrupos cíclicos gerados pelos elementos b e c.

Agora, vamos determinar o número de classes laterais de H em G, ou seja, o índice de H em K, $(K: H)$. Pelo teorema de Lagrange, $o(K) = o(H)(K: H)$. Portanto,

$$4 = 2 \cdot (K: H)$$

que pela operação de multiplicação usual chega-se que $(K: H) = 2$.

É possível construir e visualizar rapidamente as classes laterais módulo H pelos diferentes elementos do grupo K, principalmente por ser um grupo finito pequeno, de modo que

$$e * H = \{e * e, e * a\} = \{e, a\} = H;$$
$$a * H = \{a * e, a * a\} = \{a, e\} = H;$$
$$b * H = \{b * e, b * a\} = \{b, c\};$$
$$c * H = \{c * e, c * a\} = \{c, b\} = b * H;$$

Logo ver-se que $K/H = \{H, b * H\}$, o que implica dizer que $(K: H) = 2$, coincidindo assim com o valor dado ao aplicar o teorema. ■

3.1 Pierre de Fermat

Nesta seção, traz-se uma demonstração do Pequeno Teorema de Fermat utilizando a Teoria de Grupos, mais especificamente o Teorema de Lagrange. Mas antes, veja um pouco da biografia de Fermat e de seu teorema.

O francês Pierre de Fermat (1601? - 1665)[3] era advogado da província de Toulouse na França e se dedicava à Matemática por hobby em seu tempo livre. Filho de um rico comerciante e uma aristocrata, Fermat possuía subsidio para os estudos. Segundo Eves (2011), alguns pesquisadores apontam que Fermat teve sua educação inicial em casa, enquanto outros afirmam que tenha frequentado um mosteiro franciscano local e, a Universidade de Toulouse, onde se formou em direito (OLIVEIRA, 2019).

[3] Costuma-se escrever sua data de nascimento e morte como (1601?-1665) por um conflito da transferência de sua laje tumular de Toulouse para o museu local, mas registros aparentemente confiáveis mostram que Fermat nasceu no ano de 1601, por isso o usa nas escritas, mas a depender do escritor, seu nascimento varia entre 1590 a 1608. (EVES, 2011, p. 389-390).

A pesar de sua carreira como advogado e conselheiro do parlamento de Toulouse, Fermat dedicou-se também a estudar Matemática, mas apenas após seus 30 anos de idade, mas seguiu uma linha desvinculada à carreira científica, tratando estes estudos ao lazer ou hobby para seu tempo livre. Este fato não diminuiu a influência de Fermat no desenvolvimento da Matemática. Pelo contrário, seus trabalhos tiveram tamanho peso e eficácia para o avanço de diversas áreas da Matemática que o fez conhecido com o "Príncipe dos Amadores" (OLIVEIRA, 2019).

Por não almejar o reconhecimento científico, Fermat, assim como outros grandes matemáticos, possui seus escritos, trabalhos e descobertas em forma de cartas destinadas a outros matemáticos com quem se correspondia, entre eles encontram Marin Mersenne (1588-1648), também um encorajador para as publicações das descobertas matemáticas da época, Blaise Pascal (1623-1662), sobre o qual conversavam métodos de solucionar o conhecido "Problema dos Pontos" na probabilidade e, Bernard Frénicle de Bessy (1605-1675), que em uma de suas correspondências, Fermat enunciou o conhecido "Pequeno Teorema de Fermat".

Muitos de seus amigos com os quais se correspondia incentivavam e pediam para que publicasse suas descobertas, porém Fermat se contentava com o prazer que pesquisa em Matemática lhe dava, tendo publicado apenas um manuscrito anos antes de sua morte. Fato este que fez com que seus amigos iniciassem um movimento de divulgação dos trabalhos de Fermat, passando cartas de mãos em mãos ou produzindo cópias e as distribuindo entre seus contatos (OLIVEIRA, 2019).

Mesmo perpassando por diversas áreas da Matemática, Pierre de Fermat detinha maior atenção e contribuições ao que se refere a Teoria dos Números, tendo elaborado diversos teoremas e enunciados que se perpetuam até os dias de hoje, sendo o "pequeno teorema de Fermat" um destes resultados, tal qual foi apresentado pela primeira vez em uma correspondência destinada a Frénicle Bessy no ano de 1640 e, será abordado a seguir.

3.2 O Pequeno Teorema de Fermat

A correspondência de Fermat e Bessy formulou o que é hoje conhecido por Pequeno Teorema Fermat. Utilizando a Teoria de Grupos, apresentaremos a seguir uma demonstração desse teorema que foi baseado na dissertação de mestrado de (Oliveira, 2019).

Teorema 3.7 (Pequeno Teorema de Fermat): Sejam $a, p \in \mathbb{Z}$ com $p > 0$ primo. Então, $p \mid a^p - a$, isto é,

$$a^p \equiv a \ (mod\ p).$$

Demonstração: Seja $\mathbb{Z}_p^* = \mathbb{Z}_p \backslash \{\bar{0}\} = \{\bar{1}, \bar{2}, \dots, \overline{p-1}\}$ o grupo multiplicativo de ordem $p-1$, onde p é primo.

Toma-se $\bar{a} \in \mathbb{Z}_p^*$ de modo que a $o(\bar{a}) = k$, ou seja, $(\bar{a})^k = \bar{1}$. Considere o subgrupo cíclico H de $\mathbb{Z}_p^*$ gerado pelo elemento $\bar{a}$, então $H = \langle \bar{a} \rangle = \{\bar{a}, \bar{a}^2, \dots, \bar{a}^k\}$. Note que $o(H) = k$.

Pelo **Teorema 3.1**, sabe-se que a ordem do subgrupo divide a ordem do grupo. Então, $k \mid p-1$, isto é

$$p - 1 = kw, \text{ para algum } w \in \mathbb{Z}.$$

Nesse sentido, tem-se que

$$a^{p-1} = a^{kw}$$
$$a^{p-1} = (a^k)^w.$$

Pela congruência módulo p, segue que

$$\overline{a^{p-1}} = \overline{(a^k)^w} = (\overline{a^k})^w = (\bar{a}^k)^w.$$

Usando o fato de que

$$\bar{a}^k = \bar{1} \Leftrightarrow a^k \equiv 1 \ (mod\ p),$$

então é certo que

$$a^{p-1} \equiv 1^w \ (mod\ p)$$
$$a^{p-1} \equiv 1 \ (mod\ p).$$

Assim, multiplicando a em ambos os lados da congruência, conclui-se que

$$a^p \equiv a \ (mod\ p).$$ ■

Uma segunda versão desse teorema é a seguinte:

Teorema 3.8: Sejam $a, p \in \mathbb{Z}$ com p primo e a não divisível por p. Então, $p \mid a^{p-1} - 1$, isto é,

$$a^{p-1} \equiv 1 \ (mod\ p).$$

A demonstração desta versão segue resultados da análise combinatória e pode ser vista em Travello, 2014.

O Pequeno teorema de Fermat tornou-se muito conhecido, assim como o próprio Fermat, fazendo com que surgissem diversos métodos de demonstrar este resultado do Principe dos Amadores, firmando ainda mais a sua importância na história da Matemática. Por de trás de tantas demonstrações, há diversos matemáticos que se aventuraram em provar o teorema de Fermat, entre eles se encontra Euler em 1736, que faz uma série de demonstrações por indução deste resultado, a qual pode ser encontrado na dissertação de Oliveira (2019). O autor não só traz as demonstrações feitas por Euler em sua forma mais próxima do original, como também outras maneiras de se demonstrar o teorema, das quais se valem, por exemplo de congruência linear, Análise Combinatória, Séries de Taylor e via Sistemas Dinâmicos.

O Pequeno teorema de Fermat, além de sua popularidade, possui uma importante aplicação na Teoria dos Números quando se trata de encontrar restos de divisões envolvendo grandes potências e números primos. Há muitos exemplos clássicos de mesma natureza que o de encontrar o resto da divisão de 2^{11000} por 11.

Exemplo 3.9: Nota-se de imediato que 11 é primo e que não divide 2, desse modo sabe-se então que $2^{10} \equiv 1\ (mod\ 11)$. Porém, $11000 = 1100 \cdot 10$, o que implica em

$$\begin{aligned} 2^{11000} &= (2^{10})^{1100} \\ &\equiv 1^{1100}\ (mod\ 11) \\ &\equiv 1\ (mod\ 11). \end{aligned}$$

Ou seja, a divisão de 2^{11000} por 11 deixa resto 1. ■

Exemplo 3.10: De maneira semelhante ocorre para a divisão de 10^{2022} por 7. Dado que 7 é primo e não divide 10, então sabe-se pelo teorema que $10^6 \equiv 1\ (mod\ 7)$. Mas há visto que 2022 pode ser expresso pelo produto de 337 por 6, temos que

$$\begin{aligned} 10^{2022} &= (10^6)^{337} \\ &\equiv 1^{337}\ (mod\ 7) \\ &\equiv 1\ (mod\ 7). \end{aligned}$$

Implicando assim, pelo Pequeno Teorema de Fermat que, 10^{2022} na divisão por 7 deixa resto 1. ■

4 CONSIDERAÇÕES FINAIS

Em decorrência da escrita do presente trabalho, pode-se perceber, primeiramente, a grande contribuição de Évariste Galois para a estruturação dos objetos de estudos presentes na Álgebra Abstrata, dando por base o sistema matemático concedido por Grupos, o qual foi abordado nesta monografia.

Nesse sentido, acredita-se ter contemplado os objetivos propostos de se trabalhar os principais conceitos dentro da teoria de grupos, dando maior ênfase no teorema enunciado por Lagrange, o qual relaciona a ordem de um grupo finito como sendo o produto da ordem de um subgrupo qualquer pelo número de classes laterais disjuntas de ordem igual ao subgrupo dado.

Julga-se ainda que se tenha alcançado a aplicação da teoria de grupos nos estudos de restos de divisões por números primos através da elegante prova do Pequeno Teorema de Fermat, utilizando para este, conceitos da teoria de grupos, inclusive o próprio teorema de Lagrange.

Mesmo voltada para área da Matemática Pura, ao decorrer da escrita foi possível compreender de maneira mais ampla, desenvolver e aperfeiçoar conceitos que são presentes na Matemática da Educação Básica como por exemplo, conjuntos, propriedades das operações de adição e multiplicação usual dos números inteiros e, tipos de aplicações de conjuntos, contribuindo assim também para o aperfeiçoamento enquanto futuro professor.

Por fim, este trabalho se caracterizou como subsídio pessoal tanto para aprofundar os conhecimentos no campo da Álgebra Moderna quanto, incentivar para estudos futuros na área visando desenvolvimento intelectual e profissional.

REFERÊNCIAS

BOYER, Carl B.; MERZBACH, Uta C.. **História da matemática**. 3. ed. São Paulo: Blucher, 2012. Tradução de Helena Castro.

D'AMBROSIO, U. **DE GALOIS A BOURBAKI, PASSANDO POR FELIX KLEIN IMPLICAÇÕES PEDAGÓGICAS**. Revista História da Matemática para Professores, [S. l.], v. 7, n. 1, p. 120–145, 2021. Disponível em: https://rhmp.com.br/index.php/RHMP/article/view/71. Acesso em: 22 nov. 2022.

DOMINGUES, Hygino H.; IEZZI, Gelson. **Álgebra Moderna**. 4. ed. Reform. São Paulo: Atual, 2003.

EVES, Howard. **Introdução à história da matemática**. tradução Hygino H. Domingues. 5. ed. Campinas, SP: Editora da Unicamp, 2011.

GARCIA, Arnaldo; LEQUAIN, Yves. **Elementos de álgebra**. 3. ed. Rio de Janeiro: Associação Instituto Nacional de Matemática Pura e Aplicada, 2005.

GONÇALVES, Adilson. **Introdução à Álgebra**. Rio de Janeiro: Associação Instituto Nacional de Matemática Pura e Aplicada, 2003.

GUELLI, O. **Contando a História da Matemática: História da Equação do 2° Grau.** 5°ed. São Paulo: Ática, 1995.

OLIVEIRA, Francisco Erilson Freire de. **Sobre várias demonstrações do pequeno teorema de Fermat e as inter-relações entre as áreas da matemática**. 60 f, 2019. Dissertação (Mestrado Profissional em Matemática em Rede Nacional) - Centro de Ciências, Universidade Federal do Ceará, Fortaleza, 2019. Disponível em: http://www.repositorio.ufc.br/handle/riufc/44231. Acesso em: 11 nov. 2022.

OLIVEIRA, Rubens Alves de. **Equações do segundo grau:** resgate histórico dos seus métodos de resolução. 2018.93f. Dissertação (Mestrado Profissional em Matemática) – Universidade Federal do Tocantins, Programa de Pós-Graduação em Matemática, Arraias, 2018. Disponível em: http://repositorio.uft.edu.br/handle/11612/1069. Acesso em: 10 nov. 2022.

SCHUVAAB, Jair Luis**. Resolução de equações algébricas até quarto grau:** uma abordagem histórica. Orientador: Wesley Vagner Inês Shirabayashi. 2013. 39f. Dissertação (Mestrado) - Programa de Mestrado Profissional em Matemática em Rede Nacional, Universidade Estadual de Maringá. Maringá, 2013. Disponível em: https://sca.profmat-sbm.org.br/profmat_tcc.php?id1=209&id2=45960. Acesso em 07 nov. 2022.

SOUZA, J. A. UMA NOTA SOBRE A TEORIA DOS GRUPOS: DA TEORIA DE GALOIS À TEORIA DE GAUGE. **Revista Brasileira de História da Matemática**, [S. l.], v. 12, n. 24, p. 71-81, 2020. DOI: 10.47976/RBHM2012v12n2471-81. Disponível em: https://www.rbhm.org.br/index.php/RBHM/article/view/108. Acesso em: 13 set. 2022.

TRAVELLO, Vanessa de Freitas. *et al*. Aplicações do Pequeno Teorema de Fermat. **Colloquium Exactarum**, Presidente Prudente, vol. 6, n. Especial, p. 01-10, Jul-Dez, 2014.

Disponível em: http://www.unoeste.br/site/enepe/2014/suplementos/area/Exactarum/Matem%C3%A1tica/APLICA%C3%87%C3%95ES%20DO%20PEQUENO%20TEOREMA%20DE%20FERMAT.pdf . Acesso em: 02 dez. 2022.