INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E
TECNOLOGIA DA BAHIA - CAMPUS VALENÇA
LICENCIATURA EM MATEMÁTICA

FLAVIANE PAIXÃO PANTA

Recíprocas do Teorema de Lagrange

Valença-BA
2023

FLAVIANE PAIXÃO PANTA

Recíprocas do Teorema de Lagrange

Trabalho de conclusão de curso apresentado, como requisito parcial para a obtenção do título de Licenciada em Matemática junto ao Instituto Federal de Educação, Ciência e Tecnologia da Bahia - Campus Valença.

Orientadora: Profª. Ma. Ana Carolina Moura Teixeira

Valença-BA
2023

FICHA CATALOGRÁFICA ELABORADA PELO SISTEMA DE BIBLIOTECAS DO IFBA, COM OS DADOS FORNECIDOS PELO(A) AUTOR(A)

P197r Panta, Flaviane Paixão

Recíprocas do Teorema de Lagrange: / Flaviane Paixão Panta; orientadora Ana Carolina Moura Teixeira -- Valença: IFBA, 2023.

84f.

Trabalho de Conclusão de Curso (Licenciatura em Matemática) -- Instituto Federal da Bahia, 2023.

1. Álgebra. 2. Teoria de grupos. 3. Teorema de Lagrange. 4. Teorema de Cauchy. 5. Teorema de Sylow. I. Teixeira, Ana Carolina Moura, orient. II. TÍTULO.

CDD: 512

FOLHA DE APROVAÇÃO

Autor: Flaviane Paixão Panta
Título: Recíprocas do Teorema de Lagrange

Banca Examinadora:

Profª. Ma. Ana Carolina Moura Teixeira (Orientadora)
Instituto Federal de Educação, Ciência e Tecnologia da Bahia
Assinatura: _____

Prof. Me. Diego Coutinho Vieira Santiago
Instituto Federal de Educação, Ciência e Tecnologia da Bahia
Assinatura: _____

Prof. Me. Joezito Costa dos Santos Júnior
Universidade Federal da Bahia
Assinatura: _____

Valença-BA, 08 de Dezembro de 2023.

Um trabalho matemático é, para quem o sabe ler, o mesmo que um trecho musical para quem o sabe ouvir, um quadro para quem o sabe ver, uma ode para quem a sabe sentir.

Gomes Teixeira

“Gostaria de dedicar este trabalho de conclusão de curso a mim mesmo, como um reconhecimento à minha perseverança, empenho e capacidade de superação ao longo desta jornada acadêmica, destacando, sobretudo, a minha determinação em não ceder diante dos desafios.”

Agradecimentos

Antes de mais nada, quero expressar minha profunda gratidão a Deus por me possibilitar alcançar este ponto na minha jornada. Agradeço de todo coração pela sabedoria e dedicação que Ele generosamente me concedeu, por cuidar não apenas de mim, mas também da minha família, moldando assim a pessoa que sou hoje.

Expresso minha gratidão eterna à minha amada mãe, Vera Lúcia Santos Paixão Sacramento, e ao meu grandioso pai, Flávio Luís Sousa Mendes. Seu amor inabalável e apoio incansável foram a bússola que guiou cada passo ao longo desta jornada, e reconheço plenamente que sem eles, eu não estaria aqui hoje. Agradeço por serem os alicerces sólidos que sustentaram meu caminho, proporcionando uma trajetória repleta de carinho e aprendizado. Sou profundamente grata por ter pais tão incríveis ao meu lado.

Quero expressar minha sincera gratidão à minha querida irmã, Monick Luíza Santos Mendes. Em cada instante, ela esteve presente, iluminando meus dias com alegria nos momentos de fraqueza e solidão. Seu amor e carinho foram como um abraço reconfortante, dando-me a força necessária para persistir quando a ideia de desistir surgia. Agradeço por ser a luz que guiou meu caminho e por todos os momentos preciosos compartilhados, tornando minha jornada mais rica e significativa.

Agradeço profundamente à minha estimada orientadora, Ana Carolina Moura Teixeira. Agradeço não apenas por sua orientação acadêmica, mas também por ser uma amiga magnífica, por seu apoio incansável, paciência e sabedoria que ela gentilmente compartilhou ao longo desta jornada. Obrigado por acreditar em mim e por todos os conselhos construtivos que foram essenciais para o desenvolvimento e realização deste trabalho. Sua presença e influência positiva foram fundamentais, e sou imensamente grata por ter uma mentora tão dedicada e inspiradora ao meu lado.

Gostaria de expressar minha sincera gratidão ao meu inestimável amigo, Robson Jesus dos Santos, por sempre estar ao meu lado. Agradeço por fazer parte da minha vida, pelos inúmeros momentos compartilhados, pelos sorrisos trocados, por suportar todos os meus estresses e paranoias, e por ser um grande amigo ao longo desses anos. Desde o primeiro semestre, jamais poderia imaginar o quanto você se tornaria uma pessoa tão importante para mim. Sua amizade é

um tesouro que valorizo imensamente, e estou profundamente agradecida por tudo que vivemos juntos.

Agradeço à minha família, amigos e colegas por fazerem parte da minha vida, por oferecerem apoio constante e por vibrarem pelo meu sucesso. Suas contribuições foram inestimáveis, e sinto uma profunda gratidão por compartilhar esta jornada com pessoas tão especiais.

Desejo expressar minha profunda gratidão a alguns amigos que são verdadeiramente especiais para mim, bem como àqueles que, em algum momento, compartilharam uma parte significativa da minha vida, mesmo que hoje nossos caminhos tenham tomado direções diferentes. Mesmo sem citar nomes, é importante que saibam que cada um de vocês desempenhou um papel fundamental ao me oferecer suporte nos momentos mais desafiadores, trazendo risos quando a vontade era apenas chorar, e sendo fundamentais em cada passo desta jornada. Agradeço sinceramente por todo apoio e importância que cada um trouxe à minha vida.

Quero expressar minha sincera gratidão a todos os professores que tive o privilégio de conhecer ao longo desta jornada. Agradeço por depositarem confiança em mim, por acreditarem no meu potencial, pelos conhecimentos generosamente compartilhados, pelos sorrisos sinceros que tornaram o aprendizado mais leve e pelo constante estímulo. Sinto que cresci de maneira significativa graças a cada um de vocês. Cada professor desempenhou um papel inestimável na minha trajetória acadêmica, e é com profunda gratidão que reconheço o impacto positivo dessa colaboração enriquecedora. Em especial, gostaria de expressar meu agradecimento a Ana Carolina Moura Teixeira, Marcelo Lino, Roque Lyro, Diogo Dórea, Diego Coutinho e Ruth da Silva Araújo. Suas contribuições foram fundamentais para meu crescimento acadêmico, profissional e pessoal.

Por fim, quero estender meu agradecimento aos professores Diego Coutinho e Joezito Costa por terem prontamente aceitado o convite para participar da banca examinadora. Suas valiosas contribuições durante as avaliações enriqueceram significativamente o desenvolvimento deste trabalho. Agradeço profundamente pela dedicação e sabedoria que compartilharam, contribuindo para o aprimoramento deste projeto acadêmico.

Resumo

A Teoria de Grupos é amplamente reconhecida como o mais antigo ramo da álgebra moderna. Suas origens remontam aos estudos pioneiros de matemáticos renomados, como Joseph Louis Lagrange (1736-1813), Paolo Ruffini (1765-1822) e Évariste Galois (1811-1832), que se destacaram no contexto da teoria das Equações Algébricas. Dentre os teoremas mais notáveis da Teoria de Grupos, destaca-se o Teorema de Lagrange. Assim, o propósito deste trabalho é formular e demonstrar as principais recíprocas deste teorema. A recíproca do Teorema de Lagrange indaga que: se G é um grupo de ordem n e d é divisor de G, então existe um subgrupo em G de ordem d? Em geral, a resposta para essa indagação é não. No entanto, é fundamental destacar que sob determinadas condições e para grupos específicos, essa recíproca é verdadeira. Para atingir o propósito deste trabalhado, optamos em realizar uma pesquisa com uma abordagem qualitativa, do tipo bibliográfica, com base em livros que apresentam uma organização estrutural sólida e linguagem coesa. Inicialmente fornecemos uma revisão dos conceitos introdutórios sobre Grupos, abrangendo tópicos como Subgrupos, Homomorfismo de grupos, Grupos Cíclicos, Grupos de Permutações, Grupos Diedrais, Classes Laterais, Subgrupo Normal, Grupo Quociente e outros. Detalhamos também o Teorema de Lagrange e sua demonstração, com o intuito de facilitar a compreensão do leitor quanto aos resultados seguintes. Além disso, a fim de entendermos e demonstrarmos os resultados principais acerca da recíproca do Teorema de Lagrange, que são os três Teoremas de Sylow, com ênfase no primeiro, e o Teorema de Cauchy, outras ferramentas mais avançadas foram apresentadas e utilizadas, como, por exemplo, Ação de um Grupo em um Conjunto, Classe de Conjugação, Equação de Classes, Órbita, Estabilizador e P-Grupos.

Palavras-chave: Teoria de grupos. Teorema de Lagrange. Teorema de Cauchy. Teorema de Sylow.

Abstract

Group Theory is widely recognized as the oldest branch of modern algebra. Its origins date back to the pioneering studies of renowned mathematicians, such as Joseph Louis Lagrange (1736-1813), Paolo Ruffini (1765-1822) and Évariste Galois (1811-1832), who stood out in the context of the theory of Algebraic Equations. Among the most notable theorems in Group Theory, Lagrange's Theorem stands out. Thus, the purpose of this work is to formulate and demonstrate the main reciprocals of this theorem. The converse of Lagrange's Theorem asks that: if G is a group of order n and d is a divisor of G, then is there a subgroup in G of order d? In general, the answer to this question is no. However, it is essential to highlight that under certain conditions and for specific groups, this reciprocal is true. To achieve the purpose of this work, we chose to carry out research with a qualitative, bibliographical approach, based on books that have a solid structural organization and cohesive language. Initially we provide a review of the introductory concepts about Groups, covering topics such as Subgroups, Group Homomorphism, Cyclic Groups, Permutation Groups, Dihedral Groups, Classes laterals, Normal Subgroup, Quotient Group and others. We also detail Lagrange's Theorem and its demonstration, in order to facilitate the reader's understanding of the following results. Furthermore, in order to understand and demonstrate the main results regarding the reciprocal of Lagrange's Theorem, which are the three Sylow Theorems, with emphasis on the first, and Cauchy's Theorem, other more advanced tools were presented and used, such as, for example, Group Actions, Conjugacy Classes, Class Equation, Orbit, Stabilizer and P-Groups.

Keywords: Group Theory. Lagrange's Theorem. Cauchy's Theorem. Sylow Theorem.

Lista de Ilustrações

Figura 3.1 – Joseph Louis Lagrange 55

Figura 4.1 – Augustin Louis Cauchy 71
Figura 4.2 – Peter Ludwig Mejdell Sylow 72

Lista de Tabelas

2.1 Tábua de Cayley de ordem n 26
2.2 Tábua de Cayley de ordem 1 26
2.3 Tábua de Cayley de ordem 2 26
2.4 Tábua de Cayley de ordem 3 27
2.5 Tábua de Cayley do grupo D_3 48
2.6 Tábua de Cayley do grupo D_4 49

4.1 Tábua de multiplicação do grupo D_4 66

Sumário

1 Introdução **12**

2 Teoria de Grupos **15**

2.1 Operações binárias 15

2.2 Grupos 15

2.2.1 Grupo Abeliano 20

2.2.2 Propriedades Elementares de um Grupo 21

2.3 Grupo Finito 23

2.3.1 Congruência 24

2.3.2 A Tabela de Cayley para Grupos Finitos 25

2.3.3 Potências de um elemento 27

2.4 Subgrupos 30

2.5 Grupos Cíclicos 35

2.6 Ordem de um elemento 37

2.7 Homomorfismo de Grupos 40

2.8 Grupos especiais 44

2.8.1 Grupos de Permutações 44

2.8.2 Grupos Diedrais 47

3 Classes Laterais e Teorema de Lagrange **50**

3.1 Classes Laterais 50

3.1.1 Propriedades das Classes Laterais 53

3.2 Joseph Lagrange 55

3.3 Teorema de Lagrange 56

3.3.1 Consequências Imediatas do Teorema de Lagrange 57

3.4 Subgrupos Normais e Grupos Quocientes 58

3.4.1 Subgrupos Normais 58

3.4.2 Grupos Quocientes 61

4 Recíprocas para o Teorema de Lagrange **64**
4.1 Conceitos Essenciais 64
4.1.1 Ação de um Grupo em um Conjunto 64
4.1.2 Classe de Conjugação e Equação de Classes 65
4.1.3 Estabilizador e Órbita 67
4.1.4 P-Grupos 70
4.2 Teorema de Cauchy 71
4.3 Teoremas de Sylow 72
4.4 Aplicações dos Teoremas de Sylow 79
4.4.1 Grupos de ordem **pq** 79
4.4.2 Grupos de ordem $\mathbf{p^2q}$ não são simples 80
4.4.3 Grupos de ordem **30** não são simples 81

5 Conclusão e Perspectivas **82**

Referências **84**

Capítulo 1

Introdução

De acordo com uma famosa frase de Cayley, "um grupo é definido por meio de leis que combinam seus elementos". Essa explicação concisa continua sendo uma abordagem válida até hoje. Um dos recursos amplamente empregados na Matemática Moderna é o conceito de grupos. Esse conceito desempenha um papel fundamental em várias áreas científicas, incluindo a Teoria Quântica, as Estruturas Atômica e Molecular, a Cristalografia e o estudo da Álgebra Abstrata. Na Álgebra Abstrata, em particular, grupos são utilizados para construir outras estruturas algébricas, tais como Anéis, Corpos e Espaços Vetoriais. Essas estruturas podem ser visualizadas como grupos equipados com operações e axiomas adicionais.

A Teoria de Grupos é considerada o mais antigo ramo da Álgebra Moderna. Seus primeiros desenvolvimentos remontam aos trabalhos de renomados matemáticos, como Joseph Louis Lagrange (1736-1813), Paolo Ruffini (1765-1822) e Évariste Galois (1811-1832), no contexto da Teoria das Equações Algébricas. Inicialmente, os grupos consistiam em permutações das variáveis ou das raízes de polinômios, e durante grande parte do século XIX, todos os grupos estudados eram grupos de permutação finita, no entanto esses primeiros pesquisadores e seus sucessores, incluindo Augustin Louis Cauchy (1789-1857), Peter Ludwig Mejdell Sylow (1832-1918) e Camille Jordan (1838-1922), introduziram muitas das ideias fundamentais que moldaram a Teoria de Grupos.

A obra de Arthur Cayley (1821-1895) desempenhou um papel crucial no reconhecimento claro do conceito de grupo abstrato, embora tenha demorado para ganhar ampla aceitação até que Walther von Dyck (1856-1934) introduziu as apresentações de grupos. O estudo de grupos de dimensão infinita foi estimulado pela Geometria e Topologia, influenciados por nomes como o matemático Felix Klein (1840-1925), Marius Sophus Lie (1842-1899), Henri Poincaré (1854-1912), Max Dehn (1878-1952) e Peter Ludwig Mejdell Sylow (1832-1918). Nessa época, o estudo dos grupos assumiu uma forma abstrata independente e se desenvolveu rapidamente.

A primeira fase significativa da Teoria de Grupos Finitos alcançou seu ponto culminante no período imediatamente anterior à Primeira Guerra Mundial, por meio dos trabalhos do matemático Ferdinand Georg Frobenius (1849-1917), William Burnside (1852-1927) e Issai Schur (1875-1936). Após 1928, importantes contribuições foram realizadas pelos matemáticos Philip

Hall (1904-1982), Helmut Wielandt (1910-2001) e Richard Dagobert Brauer (1901-1977), este último notável por suas colaborações no âmbito das representações de grupos. A classificação dos Grupos Finitos foi finalmente concluída em 1982, graças à colaboração de centenas de matemáticos, sob a liderança do matemático norte-americano Daniel Gorenstein (1923-1992).

Nesta perspectiva, um resultado muito importante na Classificação dos Grupos Finitos é o Teorema de Lagrange. Esse teorema estabelece que, em um grupo G de ordem finita, a ordem de todos os subgrupos H de G é um divisor da ordem de G, ou seja, $|H|\big||G|$. Esse resultado permitiu avanços significativos nos estudos matemáticos, como, por exemplo, no estudo dos grupos comutativos, em que se constatou que todos os grupos de ordem até cinco são comutativos.

Além disso, como dito anteriormente, este teorema é particularmente útil na Classificação de Grupos Finitos. Suponha que tenhamos um grupo finito G e queremos estudar suas estruturas internas. Uma abordagem comum é analisar os subgrupos de G. O Teorema de Lagrange nos diz que as ordens dos subgrupos de G são sempre divisores da ordem de G. Isso significa que podemos usar o Teorema de Lagrange para restringir as possíveis ordens dos subgrupos de G, o que por sua vez nos ajuda a entender melhor a estrutura de G. Por exemplo, se a ordem de G for um número primo, então seus únicos subgrupos serão o grupo trivial (com ordem 1) e o próprio G (com ordem igual à ordem de G). Isso nos dá uma restrição significativa sobre os subgrupos possíveis e nos ajuda a classificar o grupo G.

Por outro lado, uma pergunta natural que podemos pensar relacionada a este teorema é: qual é a validade da sua recíproca? Em outras palavras, se G é um grupo de ordem n e d é divisor de G, então existe um subgrupo de G de ordem d? Em geral, a resposta é não. Todavia é importante ressaltar que sob certas condições e para alguns grupos específicos, essa recíproca é verdadeira. O Teorema de Cauchy e o primeiro Teorema de Sylow fornecem recíprocas parciais para o teorema supracitado.

Diante disso, o presente trabalho tem como finalidade apresentar condições sob as quais é valida a recíproca do Teorema de Lagrange. Deste modo, com o objetivo de reunir informações para esclarecer a questão de pesquisa mencionada anteriormente, apresentaremos a seguir uma lista de alguns objetivos que irão guiar esse processo.

- Sistematizar a Teoria de grupos.
- Apresentar os resultados que fornecem recíprocas para o Teorema de Lagrange.
- Aplicar os resultados vistos na Classificação de Grupos Finitos.

Para atingir os objetivos estabelecidos, optaremos por conduzir a pesquisa utilizando uma abordagem qualitativa que, segundo Minayo (2001), compreende responder a perguntas muito singulares, trabalhando com o universo de interpretações, razões, desejos, convicções e condutas. Desse modo, os caminhos metodológicos percorridos na construção deste estudo serão baseados na pesquisa bibliográfica que, de acordo com Gil (2002, p.3), "é desenvolvida com base em material já elaborado, constituído principalmente de livros e artigos científicos".

Neste sentido, a pesquisa bibliográfica desempenha um papel crucial na geração de conhecimento e no progresso da ciência. É uma ferramenta essencial para embasar teoricamente um estudo, permitindo que o pesquisador explore o conhecimento já existente sobre um tema específico, identifique lacunas na literatura e estabeleça uma base sólida para a sua pesquisa. Assim, as principais fontes de referência utilizadas para a elaboração deste trabalho foram: Hernstein (1964), IEZZI e Domingues (1970), Robinson (1996), VIEIRA (2013), Yartey (2017) e notas de aula da disciplina de Estruturas Algébricas, ministradas pela professora Ma. Ana Carolina Moura Teixeira, no curso de Licenciatura em Matemática do Instituto Federal de Educação, Ciência e Tecnologia da Bahia - Campus Valença.

Capítulo 2

Teoria de Grupos

Este capítulo tem como finalidade apresentar conceitos fundamentais da Teoria de Grupos que serão essenciais para o entendimento dos capítulos seguintes. O Capítulo foi fragmentado em oito seções: Operações Binárias, Grupos, Grupo Finito, Subgrupos, Grupos Cíclicos, Ordem de um elemento, homomorfismos de Grupos e Grupos Especiais.

2.1 Operações binárias

Para iniciar o estudo de Grupos será dada a definição e exemplos de operação binária.

Definição 2.1. Considere G um conjunto não vazio. Uma operação binária $*$ definida em G, é uma função:

$$\begin{array}{rcl} *: G \times G & \longrightarrow & G \\ (a,b) & \longmapsto & a*b. \end{array} \tag{2.1}$$

Isto significa que, cada par ordenado (a,b) corresponde, pela operação $*$, um único elemento de G, a saber, $a*b$.

Exemplo 2.1. As operações usuais $+$, $-$, $\times$, $\div$ são operações binárias no conjunto dos números reais $\mathbb{R}$.

Exemplo 2.2. A função $f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ dada por, $f(a,b) = a+3$ é um operação binária de adição sobre $\mathbb{Z}$, diferente da usual. Neste caso, temos $f(3,5) = 3+3 = 6$ e $f(5,3) = 5+3 = 8$.

Exemplo 2.3. A adição e multiplicação de matrizes são operações binárias no conjunto de todas as matrizes de ordem m.

2.2 Grupos

O conceito de "grupo" surgiu a partir de estudos sobre a Resolubilidade de Equações Algébricas, com contribuições de vários matemáticos, incluindo Joseph-Louis Lagrange (1736-

1813), de origem italiano-francesa, e Niels Henrik Abel (1802-1829), norueguês. Foi Évariste Galois (1811-1832), matemático francês, quem formalmente definiu a Teoria de Grupos, na tentativa de descrever as simetrias das equações satisfeitas pelas soluções de uma Equação Polinomial.

Definição 2.2. Um grupo consiste de um conjunto não vazio G e uma operação binária 2.1, $*$. Afirmamos que G com a operação $*$ é um grupo se os seguintes axiomas são satisfeitos:

(G1) (Associatividade): quaisquer que sejam a, b e c em G, tem-se:

$$(a*b)*c = a*(b*c);$$

(G2) (Existência do elemento neutro): existe em G um elemento e tal que:

$$a*e = e*a = a, \text{ para todo } a \text{ em } G;$$

(G3) (Existência do elemento inverso) para todo elemento a de G, existe um elemento b em G, denominado elemento inverso, de modo que:

$$a*b = b*a = e.$$

Notação: Denotamos um grupo G com a operação $*$ por $(G,*)$.

Observação 2.1. Essa operação pode ser de diversas formas, como por exemplo, a multiplicação ou a adição. Se a operação em questão for a multiplicação, designaremos o inverso de a como a^{-1}. No caso da operação ser uma adição, o inverso de a será expresso como $(-a)$. E, caso estejamos lidando com uma operação arbitrária, utilizaremos a notação de inverso aplicada à multiplicação.

Vários conjuntos de números têm a estrutura de grupos relativamente às operações de adição e multiplicação, que nos são familiares. Como veremos nos exemplos a seguir:

Exemplo 2.4. O conjunto dos números naturais, $\mathbb{N}$, com a operação usual de adição, "$+$", não é um grupo, uma vez que não existe elemento inverso para todo elemento de $\mathbb{N}$. Neste caso, dizemos que $\mathbb{N}$ é um semigrupo.

Exemplo 2.5. Considere o conjunto dos números inteiros $\mathbb{Z}$, com a operação usual de adição $+$. Verifique que $(\mathbb{Z},+)$ é um grupo.

Solução: De fato, $\mathbb{Z}$ é fechado em relação a operação de adição, pois a soma de dois números inteiros é um número inteiro. Além disso, valem os axiomas de grupo:

(G1) $(\mathbb{Z},+)$ é associativo, pois:

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

(G2) Existe elemento neutro, pois para todo $a \in \mathbb{Z}$, existe $0 \in \mathbb{Z}$, tal que:

$$a+0=0+a=a.$$

(G3) Existe elemento inverso, pois para todo $a \in \mathbb{Z}$, existe $(-a) \in \mathbb{Z}$, tal que:

$$a+(-a)=(-a)+a=0.$$

Logo, pela definição 2.2, $(\mathbb{Z},+)$ é um grupo.

Exemplo 2.6. Analogamente, $(\mathbb{Q},+)$ e $(\mathbb{R},+)$ são grupos com elemento neutro 0 e o inverso aditivo de a igual $-a$.

Exemplo 2.7. Mostre que $(5\mathbb{Z},+)$ é um grupo.

Solução: Seja $5\mathbb{Z}=\{\ldots-15,-10,-5,0,5,10,15,\ldots\}$ um subgrupo de $\mathbb{Z}$ e diferente de vazio, temos:
$(5\mathbb{Z},+)$ é fechado, pois

$$\forall\, a,b \in \mathbb{Z},\ 5a+5b=5(a+b) \in 5\mathbb{Z}.$$

Além disso, será verificado os axiomas de grupo.

(G1) $(5\mathbb{Z},+)$ é associativo pois, $5\mathbb{Z}$ é o conjunto dos múltiplos de cinco e um subconjunto de $\mathbb{Z}$, como $\mathbb{Z}$ é associativo temos que $5\mathbb{Z}$ também será associativo. Assim,

$$\begin{aligned}(5a+5b)+5c &= 5(a+b)+5c\\ &= 5[(a+b)+c]\\ &= 5[a+(b+c)]\\ &= 5a+5(b+c)\\ &= 5a+(5b+5c) \in 5\mathbb{Z}\end{aligned}$$

Logo, $5\mathbb{Z}$ é associativo;

(G2) Existe elemento neutro, pois para todo $a \in 5\mathbb{Z}$ existe $e \in 5\mathbb{Z}$ tal que:

$$5a+e=e+5a=5a.$$

neste caso, $e=0$.

(G3) Existe elemento inverso, uma vez que dado $a=5b \in 5\mathbb{Z}$, existe $-a=-5b$ tal que:

$$a+(-a)=5b+(-5b)=5b-5b=0.$$

Portanto $(5\mathbb{Z},+)$ é um grupo.

Exemplo 2.8. Considere o conjunto dos números racionais não nulo $(\mathbb{Q}^*)$, com a operação usual de multiplicação. Verifique que $(\mathbb{Q}^*, \cdot)$ é um grupo.

Solução: De fato, $\mathbb{Q}^*$ é fechado em relação a operação de multiplicação, pois a multiplicação de dois números racionais não nulos, é um número racional não nulo, logo $\cdot$ é uma operação binária em $\mathbb{Q}^*$. Além disso, vale os axiomas de grupos:

(G1) $(\mathbb{Q}^*, \cdot)$ é associativo, pois:

$$(a \cdot b) \cdot c = a \cdot (b \cdot c),\ \forall\ a, b, c \in \mathbb{Q}^*;$$

(G2) Existe elemento neutro, pois para todo $a \in \mathbb{Q}^*$, existe $1 \in \mathbb{Q}^*$, tal que:

$$a \cdot 1 = 1 \cdot a = a.$$

(G3) Existe elemento inverso, pois para todo $a \in \mathbb{Q}^*$, existe $\frac{1}{a} \in \mathbb{Q}^*$, tal que:

$$a \cdot \frac{1}{a} = \frac{1}{a} \cdot a = 1.$$

Portanto, $(\mathbb{Q}^*, \cdot)$ é um grupo.

Exemplo 2.9. Analogamente, $(\mathbb{R}^*, \cdot)$ é um grupo, com elemento neutro 1, e o inverso multiplicativo de $a \in \mathbb{R}^*$ é $\frac{1}{a}$.

Exemplo 2.10. $(\mathbb{Z}, \cdot)$, $(\mathbb{Q}, \cdot)$ e $(\mathbb{R}, \cdot)$ não são grupos, uma vez que 0 não possui inverso em nenhum destes conjuntos.

Observação 2.2. Por vezes, neste texto, a operação $\cdot$ será suprimida, de modo que, $a \cdot b$ será denotado por ab.

Observação 2.3. Grupos cuja operação é adição são denominados de grupos aditivos, e grupos cuja operação é a multiplicação são denominados de grupos multiplicativos. Note que, os grupos dos exemplos anteriores 2.5, 2.6, 2.7 são denominados de grupos aditivos e 2.8, 2.9 são chamados de grupos multiplicativos.

Temos, também exemplos de conjuntos não numéricos que, com suas respectivas operações usuais, formam estruturas de grupos. Como, por exemplo:

Exemplo 2.11. O conjunto das matrizes $n \times n$ invertíveis com entradas em $\mathbb{R}$, isto é,

$$GL_n(\mathbb{R}) = \{A \in M_n(\mathbb{R}),\ det(A) \neq 0\}.$$

Com a operação usual de multiplicação, é um grupo multiplicativo $(GL_n(\mathbb{R}), \cdot)$, chamado de Grupo Linear de grau n sobre $\mathbb{R}$.

Observe que o elemento neutro é a matriz identidade de mesma ordem n e a propriedade de associatividade é satisfeita, pois se resume à associatividade presente no grupo dos $(\mathbb{R}, \cdot)$, e o próprio conjunto garante a existência da matriz inversa, para cada elemento.

Exemplo 2.12. O conjunto $G = M_{n\times m}$ de todas as matrizes reais de ordem $n \times m$ é um grupo aditivo. De fato, dados $A = (a_{ij})_{n\times m}$, $B = (b_{ij})_{n\times m}$, $C = (c_{ij})_{n\times m} \in G$ tem-se:

(G1) Para todo $A, B, C \in G$, temos:

$$\begin{aligned} A+(B+C) &= (a_{ij})_{n\times m} + [(b_{ij})_{n\times m} + (c_{ij})_{n\times m}] \\ &= (a_{ij})_{n\times m} + (b_{ij}+c_{ij})_{n\times m} \\ &= (a_{ij}+b_{ij}+c_{ij})_{n\times m} \\ &= [(a_{ij})_{n\times m} + (b_{ij})_{n\times m}] + (c_{ij})_{n\times m} \\ &= (A+B)+C. \end{aligned}$$

(G2) Para todo $A \in G$, temos:

$$A + O = (a_{ij})_{n\times m} + (0_{ij})_{n\times m} = (a_{ij}+0_{ij})_{n\times m} = (a_{ij})_{n\times m} = A,$$

onde $(0_{ij})_{n\times m}$ é a matriz nula.

(G3) Para todo $A \in G$, temos:

$$A + (-A) = [(a_{ij})_{n\times m} + (-a_{ij})_{n\times m}] = (a_{ij} - a_{ij})_{n\times m} = (0_{ij})_{n\times m}.$$

Exemplo 2.13. Consideremos os grupos $(G_1, \star)$ e $(G_2, \triangle)$. Vamos mostrar que o produto cartesiano $G_1 \times G_2$ dotado da operação "$*$" dada por,

$$(a,b) * (c,d) = (a \star c, b \triangle d)$$

para quaisquer (a,b) e (c,d) em $G_1 \times G_2$ é um grupo.

Solução: Como as operações em G_1 e G_2 são associativas, então a operação em $G_1 \times G_2$ também é associativa. Agora, se $e_1 \in G_1$ e $e_2 \in G_2$ são elementos neutros das operações $\star$ e $\triangle$, respectivamente, então $e = (e_1, e_2) \in G_1 \times G_2$ satisfaz,

$$(a,b) * (e_1,e_2) = (a,b) = (e_1,e_2) * (a,b), \ \ \forall\, (a,b) \in G_1 \times G_2,$$

ou seja, $e = (e_1, e_2)$ é o elemento neutro da operação em $G_1 \times G_2$. Por fim, dado $(a,b) \in G_1 \times G_2$, existem $a_1 \in G_1$ e $b_1 \in G_2$ tais que $a \star a_1 = e_1 = a_1 \star a$ e $b \triangle b_1 = e_2 = b_1 \triangle b$. Por isso,

$$(a,b) * (a_1,b_1) = (e_1,e_2) = (a_1,b_1) * (a,b),$$

isto é, (a_1, b_1) é o inverso de (a,b) em $G_1 \times G_2$. Por conseguinte, $(G_1 \times G_2, *)$ é um grupo.

O grupo $(G_1 \times G_2, *)$ é chamado produto direto de G_1 e G_2. De um modo geral, se $(G_1, \cdot), (G_2, \cdot), ..., (G_n, \cdot)$ são grupos, 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 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 Produto Direto de Grupos.

Observação 2.4.

1. O produto direto $G_1 \times G_2 \times ... \times G_n$ é abeliano[1] se, e somente se, G, é abeliano, para cada $i = 1, 2, ..., n$.

2. Quando a operação em G, for aditiva para $i = 1, 2, ..., n$, então a operação em $G_1 \times G_2 \times ... \times G_n$ também será aditiva. Assim, para os elementos $(x_1, x_2, ..., x_n)$ e $(y_1, y_2, ..., y_n)$ em G,
$$(x_1, x_2, ..., x_n) + (y_1, y_2, ..., y_n) = (x_1 + y_1, x_2 + y_2, ..., x_n + y_n).$$

2.2.1 Grupo Abeliano

Os Grupos Abelianos têm uma operação binária comutativa, isto é, a ordem dos elementos não influencia o resultado da operação. Essa propriedade é conhecida como comutatividade ou propriedade comutativa. O termo "Abeliano" foi atribuído como uma homenagem ao matemático norueguês Niels Henrik Abel (1802-1829), que fez importantes contribuições tanto na Teoria das Equações quanto na Teoria de Grupos.

Definição 2.3. Se a operação $*$ de um grupo G satisfaz o axioma $(G4)$, (Comutatividade): quaisquer que sejam a e b em G, tem-se,
$$a * b = b * a.$$

Diremos que G é um grupo comutativo ou abeliano.

Exemplo 2.14. Mostre que os grupos do exemplo 2.5 e do exemplo 2.7 são abelianos, respectivamente.

Solução: Para mostrar que um grupo é abeliano deve-se verificar se vale a comutatividade (G4). Com efeito,
$$a + b = b + a, \ \forall \ a, b \in \mathbb{Z},$$

e

$$5a + 5b = 5(a + b) = 5(b + a) = 5b + 5a, \ \forall \ a, b \in \mathbb{Z}.$$

Portanto, os grupos dos exemplos 2.5 e 2.7 são abelianos.

Exemplo 2.15. Prove que o conjunto $H = \mathcal{L}[0,1] = \{f : [0,1] \longrightarrow \mathbb{R}; \ f \text{ é contínua}\}$, com operação de adição de funções, é um grupo abeliano.

Solução: De fato, H é diferente de vazio, pois a função identicamente nula, $f(x) \equiv 0 \in H$ e H é fechado, uma vez que a soma de funções contínuas é ainda uma função contínua. Além disso, valem os axiomas de grupos:

[1] Na próxima seção estudaremos grupos abelianos.

(G1) $(H,+)$ é associativo, pois:

$$f(x)+(g+h)(x)=f(x)+g(x)+h(x)=(f+g)(x)+h(x),\ \forall\ f,g,h\in H;$$

(G2) Existe um elemento neutro $e(x)$ em H, tal que:

$$e(x)+f(x)=f(x)+e(x)=f(x),\ \forall\ f\in H;$$

neste caso, $e(x)=0(x)=0$, ou seja, $e(x)$ é a função nula.

(G3) Existe um elemento inverso $-f(x)$ em H, tal que:

$$-f(x)+f(x)=f(x)+[-f(x)]=0(x),\ \forall\ f\in H.$$

(G4) $(H,+)$ é comutativo, pois:

$$(f+g)(x)=f(x)+g(x)=g(x)+f(x)=(g+f)(x),\ \forall\ f,\ g\in H;$$

Portanto, $(H,+)$ é um grupo abeliano.

2.2.2 Propriedades Elementares de um Grupo

Nesta seção, destacaremos as propriedades de um grupo G que seguem quase imediatamente da definição.

Proposição 2.1. Seja $(G,*)$ um grupo. Então,

(1) O elemento neutro de um grupo G é único.

Demonstração. Suponha e e e_1 elementos neutros de G. Do fato de e ser elemento neutro de G, segue, em particular:

$$e*e_1=e_1*e=e_1. \tag{2.2}$$

Agora, sendo e_1 elemento neutro de G,

$$e_1*e=e*e_1=e. \tag{2.3}$$

Assim, de (2.2) e (2.3), concluímos que $e_1=e$. Logo, o elemento neutro é único. ■

(2) O elemento inverso de um grupo G é único.

Demonstração. De fato, considere $a\in G$ e supondo $b_1,b_2\in G$, tais que são ambos inversos de a, temos:

$$a*b_1=b_1*a=e.$$

$$a*b_2=b_2*a=e.$$

Logo,

$$b_1=b_1*e=b_1*(a*b_2)=(b_1*a)*b_2=e*b_2=b_2.$$

Portanto, $b_1=b_2$. Assim, concluímos que o elemento inverso é único. ■

(3) $e^{-1} = e$, ou seja, o inverso do elemento neutro é o próprio elemento neutro.

Demonstração. De fato, como $e * e^{-1} = e$, então $e^{-1} = e$. ■

(4) $(a^{-1})^{-1} = a$.

Demonstração. Dado $a \in G$, um elemento $b \in G$ é, por definição, o inverso de a ou vice-versa, quando

$$a * b = b * a = e.$$

Como $a^{-1} * a = a * a^{-1} = e$, concluímos que, o inverso de a^{-1} é a, ou seja, $(a^{-1})^{-1} = a$. ■

(5) $(a * b)^{-1} = b^{-1} * a^{-1}$.
Note que se G é um grupo abeliano, então $(a * b)^{-1} = a^{-1} * b^{-1}$.

Demonstração. De fato,

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

E

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

Portanto, concluímos que $(a * b)^{-1} = b^{-1} * a^{-1}$. ■

(6) **(Lei do Cancelamento)** Se $a * x = a * y$, então $x = y$.

Demonstração. De fato,

$$a * x = a * y.$$

Operando a^{-1} à esquerda em ambos os membros:

$$a^{-1} * (a * x) = a^{-1} * (a * y).$$

Usando a associatividade:

$$(a^{-1} * a) * x = (a^{-1} * a) * y.$$

Existência do elemento inverso:

$$e * x = e * y.$$

Existência do elemento neutro:

$$x = y.$$

■

(7) Dados $a, b \in G$, existe um único elemento $x \in G$ tal que $a * x = b$.

Demonstração. De fato, a equação $a * x = b$ admite uma única solução em G, uma vez que:

$$a * x = b.$$

Operando a^{-1} em ambos os membros à esquerda:

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

Usando a associatividade:

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

Existência do elemento inverso:

$$e * x = a^{-1} * b.$$

Existência do elemento neutro:

$$x = a^{-1} * b.$$

Como o elemento inverso de um grupo qualquer é único, então existe $x = a^{-1} * b$ e é única. ■

2.3 Grupo Finito

Os Grupos Finitos desempenham um papel fundamental para o estudo dos grupos de modo geral e são frequentemente utilizados como exemplos e ferramentas para entender propriedades mais gerais dos grupos.

Definição 2.4. Diremos que um grupo G é finito se o conjunto G for finito, ou seja, quando G contiver um número finito de elementos. Neste caso, definimos a ordem de G, que será indicado por $o(G)$ ou $|G|$, sendo o número de elementos de G. Caso contrário, diremos que G é um grupo infinito e que a ordem de G é infinita.

Vamos agora abordar a definição de congruência, apresentando alguns exemplos para ilustrar seu conceito.

2.3.1 Congruência

Definição 2.5. Sejam a, b e n números inteiros, $n > 0$. Dizemos que a é côngruo a b, módulo n, se $n \big| (a-b)$.

Neste caso, afirmamos que eles são côngruos ou congruentes, e representamos como

$$a \equiv b \bmod n.$$

Exemplo 2.16. $7 \equiv 15 \pmod 8$, pois $7 - 15 = -8$ é divisível por 8.

Exemplo 2.17. $3 \equiv 21 \pmod 6$, uma vez que $3 - 21 = -18$ é divisível por 6.

Se n não divide a diferença $a - b$, então afirmamos que a é incongruente a b módulo n, e denotamos por $a \not\equiv b \pmod n$.

Exemplo 2.18. $25 \not\equiv 12 \pmod 7$, pois $7 \nmid (25-12)$;

Exemplo 2.19. $16 \not\equiv 9 \pmod 4$, uma vez $4 \nmid (16-9)$.

Teorema 2.20. Dois inteiros a e b são congruentes módulo n se, e somente se, a e b deixam o mesmo resto quando divididos por n.

Demonstração. $(\Rightarrow)$ Suponhamos que $a \equiv b \pmod n$. Então, por definição:

$$a - b = kn, \text{ com } k \in \mathbb{Z}$$

Seja r o resto da divisão de b por n. Logo, pelo algoritmo da divisão:

$$b = nq + r, \text{ onde } 0 \leqslant r < n$$

Portanto:

$$a = kn + b = kn + nq + r = (k+q)n + r$$

e isso implica que r é o resto da divisão de a por n, ou seja, os inteiros a e b divididos por n deixam o mesmo resto r.

$(\Leftarrow)$ Reciprocamente, suponhamos que a e b divididos por m deixam o mesmo resto r. Então, podemos escrever:

$$a = nq_1 + r \text{ e } b = nq_2 + r, \text{ onde } 0 \leqslant r < n$$

e, portanto:

$$a - b = nq_1 + r - (nq_2 + r) = nq_1 - nq_2 + r - r = nq_1 - nq_2 = n(q_1 - q_2).$$

Então:

$$n \big| (a-b) \Rightarrow a \equiv b \pmod n.$$

■

Com base na definição e no teorema mencionados anteriormente, podemos analisar exemplos específicos de grupos abelianos finitos, nos quais esses conceitos são fundamentais para uma compreensão mais aprofundada.

Exemplo 2.21. O conjunto $\mathbb{Z}_n = \{\overline{0}, \overline{1}, \overline{2}, ..., \overline{n-1}\}$, dos inteiros módulo n com operação da soma definida por,

$$\overline{a} + \overline{b} = \overline{a+b}$$

é um grupo aditivo abeliano finito, com ordem n, e com elemento neutro $\overline{0}$ e inverso de $\overline{a}$ é $\overline{(n-a)}$.

Observação 2.5. O conjunto $\mathbb{Z}_n$ é formado pelos restos da divisão de qualquer inteiro por n, $n \in \mathbb{Z}$.

Exemplo 2.22. O conjunto $U_n = \{\overline{a} \in \mathbb{Z}_n;\ mdc(a,n) = 1\}$ dos elementos invertíveis de $\mathbb{Z}_n$ com a operação,

$$\overline{a} \cdot \overline{b} = \overline{a \cdot b}$$

é um grupo multiplicativo abeliano finito, de ordem n, com elemento neutro $\overline{1}$ e o inverso multiplicativo de $\overline{a} \in U_n$ é o elemento $\overline{b}$ tal que $\overline{a} \cdot \overline{b} = \overline{1}$.

Observação 2.6. O conjunto U_n é formado pelos números pertencentes a $\mathbb{Z}_n$ que são primos com n, ou seja, números que não possuem divisores comuns com n, além do trivial.

O matemático Arthur Cayley (1821-1899) introduziu uma outra forma de representação para os grupos finitos, a tábua da operação $*$, chamada de tabela de Cayley, que veremos a seguir:

2.3.2 A Tabela de Cayley para Grupos Finitos

Definição 2.6. Seja $(G, *)$ um grupo finito com n elementos. Suponha,

$$G = \{e, a_1, a_2, a_3, ..., a_{n-1}\}$$

onde e é elemento neutro. A operação binária $*$ em G pode ser descrita por meio da tabela da forma:

Tabela 2.1: Tábua de Cayley de ordem n

$*$	e	a_1	a_2	a_3	$\ldots$	a_{n-1}
e	e	a_1	a_2	a_3	$\ldots$	a_{n-1}
a_1	a_1	$a_1 * a_1$	$a_1 * a_2$	$a_1 * a_3$	$\ldots$	$a_1 * a_{n-1}$
a_2	a_2	$a_2 * a_1$	$a_2 * a_2$	$a_2 * a_3$	$\ldots$	$a_2 * a_{n-1}$
a_3	a_3	$a_1 * a_3$	$a_3 * a_2$	$a_3 * a_3$	$\ldots$	$a_3 * a_{n-1}$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
a_{n-1}	a_{n-1}	$a_{n-1} * a_1$	$a_{n-1} * a_2$	$a_{n-1} * a_3$	$\ldots$	$a_{n-1} * a_{n-1}$

Fonte: Autoria própria

Esta tabela é denominada tábua de Cayley para $(G, *)$.

Exemplo 2.23. Construa as tabelas de Cayley de grupos finitos de ordens 1, 2 e 3.
Solução:

(a) Sendo G um grupo de ordem 1, então G contém unicamente o elemento neutro, ou seja, $G = e$. A tabela de Cayley do grupo $G = e$ está abaixo:

Tabela 2.2: Tábua de Cayley de ordem 1

$*$	e
e	e

Fonte: Autoria própria

Neste caso, $G = \{e\}$ é um grupo abeliano.

(b) Sendo G um grupo de ordem 2. Logo, G contém dois elementos, onde vamos representá-los por $G = \{e, a\}$, o elemento neutro e mais outro elemento. Sabendo da unicidade do elemento neutro, segue abaixo a tabela de Cayley do grupo $G = \{e, a\}$:

Tabela 2.3: Tábua de Cayley de ordem 2

$*$	e	a
e	e	a
a	a	e

Fonte: Autoria própria

Portanto, também nesse caso G é um grupo abeliano.

(c) Sendo G um grupo de ordem 3. Logo, G contém três elementos, onde vamos representá-los por $G = \{e, a, b\}$, o elemento neutro e mais dois elementos. Segue abaixo a tabela de Cayley do grupo $G = \{e, a, b\}$:

Tabela 2.4: Tábua de Cayley de ordem 3

$*$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

Fonte: Autoria própria

Observe que:

- $a*b$ pode ser e, ou a, ou b. Se $a*b=a$ então $b=e$, impossível pois o elemento neutro de um grupo é único. Da mesma maneira, $a*b\neq b$. Portanto, $a*b=e$ isso implica que $a=b^{-1}$.
- $a*a$ pode ser a, ou e, ou b. Se $a*a=a$ então $a=e$ como citado anteriormente, não é possível, pois o elemento neutro de um grupo é único. Além disso, se $a*a=e$ isso implica que $a=a^{-1}=b$ também não pode. Logo, $a*a=b$.
- Da mesma forma $b*a=e$ e $b*b=a$.

Portanto, também nesse caso G é um grupo abeliano.

2.3.3 Potências de um elemento

Considere G um grupo com operação de multiplicação e a sendo um elemento de G. Definimos as potências de a por:

$$a^n=\begin{cases} e, \text{ se } n=0 \\ \underbrace{a\cdot a\cdot a\cdot \ldots \cdot a}_{n \text{ vezes}}, \text{ se } n>0 \\ (a^{-1})^{|n|}, \text{ se } n<0. \end{cases} \tag{2.4}$$

Contudo, se G for um grupo aditivo, então as potências de a é definida por:

$$n\cdot a=\begin{cases} e, \text{ se } n=0 \\ \underbrace{a+a+a+\ldots+a}_{n \text{ vezes}}, \text{ se } n>0 \\ |n|(-a), \text{ se } n<0. \end{cases} \tag{2.5}$$

Exemplo 2.24. Considere o grupo multiplicativo $U_{11}=\{\overline{1},\overline{2},\overline{3},\overline{4},\overline{5},\overline{6},\overline{7},\overline{8},\overline{9},\overline{10}\}$. As potências de 4 são:

Solução:

$$\begin{aligned}
\overline{4}^1 &= \overline{4} = \overline{4};\\
\overline{4}^2 &= \overline{4}\cdot\overline{4} = \overline{5};\\
\overline{4}^3 &= \overline{4}\cdot\overline{4}\cdot\overline{4} = \overline{9};\\
\overline{4}^4 &= \overline{4}\cdot\overline{4}\cdot\overline{4}\cdot\overline{4} = \overline{3};\\
\overline{4}^5 &= \overline{4}\cdot\overline{4}\cdot\overline{4}\cdot\overline{4}\cdot\overline{4} = \overline{1};\\
\overline{4}^6 &= \overline{4}\cdot\overline{4}\cdot\overline{4}\cdot\overline{4}\cdot\overline{4}\cdot\overline{4} = \overline{4};
\end{aligned}$$

assim, sucessivamente.

Exemplo 2.25. Considere o grupo aditivo $\mathbb{Z}_8 = \{\overline{0},\overline{1},\overline{2},\overline{3},\overline{4},\overline{5},\overline{6},\overline{7}\}$. As potências de 6 são:

Solução:

$$\begin{aligned}
1\cdot\overline{6} &= \overline{6} = \overline{6};\\
2\cdot\overline{6} &= \overline{6}+\overline{6} = \overline{12} = \overline{4};\\
3\cdot\overline{6} &= \overline{6}+\overline{6}+\overline{6} = \overline{18} = \overline{2};\\
4\cdot\overline{6} &= \overline{6}+\overline{6}+\overline{6}+\overline{6} = \overline{24} = \overline{0};\\
5\cdot\overline{6} &= \overline{6}+\overline{6}+\overline{6}+\overline{6}+\overline{6} = \overline{30} = \overline{6};
\end{aligned}$$

e assim, por diante.

Vejamos, agora, algumas propriedades das potências.

Proposição 2.2. Seja $(G,\cdot)$ um grupo. Dados $a \in G$ e $n,m \in \mathbb{Z}$, temos que:

(1) $a^n \cdot a^m = a^{n+m}$

Demonstração. Consideremos dois casos separadamente.

Inicialmente, se $n \geq 0$ e $n+m \geq 0$. Utilizando indução sobre n. Se $n = 0$,

$$a^m \cdot a^0 = a^m \cdot e = a^m = a^{m+0}.$$

Suponhamos que o resultado seja válido para n, ou seja, $a^n \cdot a^m = a^{m+n}$. Assim, como $a^n \cdot a = a^{(n+1)-1} \cdot a = a^{n+1}$,

$$\begin{aligned}
a^m \cdot a^{n+1} &= a^m \cdot a^n \cdot a\\
&= a^{n+m} \cdot a\\
&= a^{(n+m+1)-1} \cdot a\\
&= a^{n+m+1}.
\end{aligned}$$

Agora, suponhamos que m e n sejam quaisquer inteiros. Vamos considerar um inteiro $r > 0$ de maneira que $r+m > 0$, $r+n > 0$ e $r+m+n > 0$. Logo, considerando o fato que $a^r \cdot a^{-r} = e$, obtemos usando a primeira parte da demostração,

$$\begin{aligned} a^{m+n} = a^{m+n} \cdot (a^r \cdot a^{-r}) &= (a^{m+n} \cdot a^r) \cdot a^{-r} \\ &= a^{m+n+r} \cdot a^{-r} \\ &= a^{m+(n+r)} \cdot a^{-r} \\ &= a^m \cdot (a^n \cdot a^r) \cdot a^{-r} \\ &= a^n \cdot a^m. \end{aligned}$$

■

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

Demonstração. Vamos usar indução sobre n. Se $n = 1$,

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

Suponhamos, agora, que o resultado é válido para algum n, isto é,

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

Assim,

$$\begin{aligned} (a^m)^{(n+1)} &= (a^m)^n \cdot (a^m)^1 \\ &= (a)^{mn} \cdot (a)^{m1} \\ &= a^{m \cdot n + m} \\ &= a^{m(n+1)}. \end{aligned}$$

■

(3) $(a^n)^{-1} = (a^{-1})^n = a^{-n}$

Demonstração. Vamos usar indução sobre n. Se $n = 1$,

$$(a^1)^{-1} = a^{1 \cdot (-1)} = a^{-1}$$

Suponhamos, agora, que o resultado é valido para algum n, isto é,

$$(a^n)^{-1} = (a^{-1})^n = a^{-n}.$$

Assim,

$$(a^{n+1})^{-1} = (a^{-1})^{(n+1)}$$

=

$$\begin{aligned} &= (a^{-1})^n \cdot (a^{-1})^1 \\ &= a^{-n} \cdot a^{-1} \\ &= a^{-(n+1)}. \end{aligned}$$

■

Observação 2.7. Se na proposição anterior, a operação do grupo for "+", então para quaisquer inteiros n e m, os itens (1), (2) e (3) são reescritos da forma:

(1) $n \cdot a + m \cdot a = (n+m) \cdot a$

(2) $m(n \cdot a) = (mn) \cdot a$

(3) $(-m) \cdot a = -(m \cdot a)$

2.4 Subgrupos

Os subgrupos têm um papel crucial na Teoria de Grupos, proporcionando uma estrutura interna de grande relevância para a compreensão e análise de grupos mais abrangentes. São conjuntos que possuem sua própria estrutura de grupo e compartilham propriedades específicas com o grupo maior ao qual pertencem.

Definição 2.7. Seja $(G, *)$ um grupo. Um subconjunto não vazio H de G é um subgrupo de $(G, *)$ se, e somente se, as seguintes condições forem verificadas:

(a) H é fechado em relação à operação $*$;

(b) H é um grupo em relação à operação induzida sobre H pela operação $*$.

A condição (a) afirma que se a e b são dois elementos quaisquer de H, então $a * b \in H$; por consequência, $*$ é uma operação binária sobre o conjunto H. Por outro lado, a condição (b) impõe que a restrição da operação $*$, ao subconjunto H, deve satisfazer os axiomas $(G1), (G2)$ e $(G3)$, ou seja, um subconjunto H de G, é um subgrupo de $(G, *)$ se, e somente se, H é um grupo em relação à operação $*$.
Notação: Se H é subgrupo de G, então denotamos $H \leq G$.

Observação 2.8. Como a operação $*$ é associativa em G, logo, ela satisfaz a propriedade associativa $(G1)$ para os elementos de H. Portanto, as propriedades a serem satisfeitas para que H seja um subgrupo de G são dadas pelos axiomas $(G2)$ e $(G3)$.

Observação 2.9.

1. $\{e\}$ e G são subgrupos de G denotados subgrupos triviais de G.

2. Se H é um subgrupo de G, diferente de $\{e\}$ e G, então dizemos que H é um subgrupo próprio de G e escrevemos $H < G$.

Exemplo 2.26. Temos a seguinte sequência de subgrupos:

i. $(\mathbb{Z},+) < (\mathbb{Q},+) < (\mathbb{R},+) < (\mathbb{C},+)$.

ii. $(\mathbb{Q}^*,\cdot) < (\mathbb{R}^*,\cdot) < (\mathbb{C}^*,\cdot)$.

Exemplo 2.27. Considere em $\mathbb{Z}$ com operação $*$ definida por,

$$a * b = a + b + 1.$$

Verifique se $I = \{z \in \mathbb{Z};\ z \text{ é ímpar}\}$ é um subgrupo de $(\mathbb{Z},*)$.
Solução: I é fechado, pois para a e $b \in I$, temos $a = 2n+1$ e $b = 2m+1$ com $n,m \in \mathbb{Z}$. Portanto,

$$\begin{aligned} a * b &= (2n+1) * (2m+1) \\ &= 2n+1+2m+1+1 \\ &= 2n+2m+2+1 \\ &= 2(n+m+1)+1. \end{aligned}$$

Fazendo, $n+m+1 = z$, $\quad a * b = 2z+1 \in I$.

(G2) Existe elemento neutro, pois, para todo $a = 2n+1 \in I$, existe $e \in I$ tal que:
Se $a * e = e * a = a$. Então,

$$\begin{aligned} (2n+1) * e &= 2n+1 \\ 2n+1+e+1 &= 2n+1 \end{aligned}$$

neste caso, $e = -1$.

(G3) Existe elemento inverso, se dado $a = 2n+1 \in I$, tem-se: $a * a^{-1} = a^{-1} * a = e$. Então,

$$(2n+1) * a^{-1} = (2n+1) + a^{-1} + 1 = e.$$

Como $e = -1$. Temos,

$$\begin{aligned} (2n+1) + a^{-1} + 1 &= -1 \\ 2n + a^{-1} &= -3 \\ a^{-1} &= -2n-2-1 \\ a^{-1} &= -2(n+1)-1. \end{aligned}$$

Portanto, I é subgrupo de $\mathbb{Z}$.

Veremos agora um critério que será muitas vezes utilizado para mostrar que um dado conjunto é um subgrupo.

Proposição 2.3 (**Critério de Subgrupo**)**.** Seja G um grupo com operação qualquer e H uma parte do conjunto G. H é um subgrupo de G se, e somente se, as seguintes condições forem verificadas:

1. H é diferente de vazio ($H \neq \varnothing$);
2. Quaisquer que sejam $a, b \in H$, então $a * b^{-1} \in H$.

Demonstração. ($\Rightarrow$) De fato, se H é um subgrupo de G, então H é fechado, existe elemento neutro e elemento inverso em H. Logo, $a * b^{-1} \in H$ para todo $a, b \in H$.
($\Leftarrow$) Para provar a recíproca, vamos mostrar que H é um subgrupo de G por meio da definição de subgrupo 2.4. Portanto,

- A associatividade em H, é trivial, pois, se $a, b, c \in H$, então $a, b, c \in G$ e, portanto, $a * (b * c) = (a * b) * c$, ou seja, como a operação em H é a mesma de G, logo H é associativa;
- Por hipótese, $H \neq \varnothing$, assim, podemos considerar um elemento $x \in H$. Juntando esse fato à hipótese, temos:

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

  Considerando agora um elemento $b \in H$, da hipótese e da conclusão anterior segue que:

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

  Provaremos agora que H é fechado para a operação $*$. De fato, se $a, b \in H$, então, levando em consideração a conclusão anterior $a, b^{-1} \in H$. Tem-se:

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

■

Observação 2.10. A partir da demonstração, podemos concluir que a condição de $H \neq \varnothing$ pode ser substituída por, $e \in H$. É importante observar que, se mostrarmos que o elemento neutro não pertence a H ($e \notin H$), então automaticamente provamos que H não é subgrupo.

Exemplo 2.28. O conjunto $2\mathbb{Z}$ de todos os inteiros pares, ou seja, os múltiplos de 2,

$$2\mathbb{Z} = \{2n;\ n \in \mathbb{Z}\},$$

é um subgrupo de $(\mathbb{Z}, +)$?
solução: Sejam $a, b \in 2\mathbb{Z}$, com $a = 2n$ e $b = 2m$. Como o inverso aditivo de b é $-b = -2m$, temos:

$$a + (-b) = 2n + (-2m) = 2n - 2m = 2\underbrace{(n - m)}_{\in\,;\,\mathbb{Z}} \in 2\mathbb{Z},$$

isso mostra que $2\mathbb{Z} < \mathbb{Z}$.

Exemplo 2.29. Sendo G um grupo abeliano, com elemento neutro e. Prove que

$$H = \{x \in G \mid x^2 = e\},$$

é subgrupo de G.

Solução:
Primeiro método: usando a definição
H é fechado, pois, para todo x e $y \in H$, temos $x^2 = e$ e $y^2 = e$. Então,

$$(xy)^2 = (xy)(xy) = x(yxy) = x(xyy) = x(xy^2) = x(xe) = xx = x^2 = e.$$

Ou seja, $xy \in H$.

(G2) Existe elemento neutro, pois, $e^2 = e$, logo $e \in H$.

(G3) Para todo, $x \in H$, temos $x^2 = e$, isto implica, $x = x^{-1}$, logo $x^{-1} \in H$ e existe o inverso de cada elemento de H.

Portanto, H é subgrupo de G.
Segundo método: usando o Critério de Subgrupo:

1. De fato, $H \neq \varnothing$ pois, $e \in H$, uma vez que $e^2 = e$.

2. Além disso, para todo x e $y \in H$ temos,

$$(xy^{-1})^2 = (x^2)(y^{-1})^2 = e(y^2)^{-1} = (y^2)^{-1} = (e)^{-1} = e.$$

Portanto, H é um subgrupo de G.

Veremos propriedades importantes de subgrupos. A primeira diz que a intersecção de subgrupos é ainda um subgrupo.

Proposição 2.4. Se H_1 e H_2 são subgrupos de um grupo G, então $H_1 \cap H_2$ é um subgrupo de G.

Demonstração.

- De fato, $e \in H_1 \cap H_2$. Pois $e \in H_1$ e H_2.

- Dados x, $y \in H_1 \cap H_2$, temos $x, y \in H_1$ e $x, y \in H_2$. Daí, como H_1 e H_2 são subgrupos de G, então $xy \in H_1$ e $xy \in H_2$, logo $xy \in H_1 \cap H_2$. Como $x \in H_1 \cap H_2 \Rightarrow x \in H_1$ e $x \in H_2 \Rightarrow x^{-1} \in H_1$ e $x^{-1} \in H_2 \Rightarrow x^{-1} \in H_1 \cap H_2$. Logo, $H_1 \cap H_2$ é subgrupo de G.

■

O subgrupo $H = H_1 \cap H_2$ é o maior subgrupo de G, contido em H_1 e H_2, no seguinte sentido: se K é qualquer grupo de G contido em H_1 e H_2, então $K \subset H$.

Observação 2.11. Note que o resultado anterior pode ser generalizado para uma quantidade n de subgrupos, isto é, se $H_1, H_2, ..., H_n$ são subgrupos de G, então $H_1 \cap H_2 \cap ... \cap H_n$ também será.

Agora veremos dois importantes conjuntos de G, que posteriormente mostraremos no avanço de sua teoria que são também subgrupos.

Definição 2.8. Sendo G um grupo e a um elemento de G. Definimos:

(a) O centro de G é o conjunto $Z(G) = \{x \in G;\ xa = ax \quad \text{para todo} \quad a \in G\}$.

(b) O centro de a é o conjunto $N(a) = \{x \in G;\ xa = ax\ \}$.Também chamado de normalizador de a em G.

Proposição 2.5. Sendo G um grupo e a um elemento de G. Então $Z(G)$ e $N(a)$ são subgrupos de G.

Demonstração. (a) $Z(G) = \{x \in G;\ xa = ax \ \text{ para todo } \ a \in G\} \leqslant G$.
Para demonstrar que $Z(G)$ é um subgrupo de G, faremos uso da definição de subgrupo. Assim,

- Sendo $x, y \in Z(G)$, então como $xa = ax$ e $ya = ay$ para todo $a \in G$, temos

$$(xy)a = x(ya) = x(ay) = (xa)y = (ax)y = a(xy), \forall a \in G.$$

Logo, $xy \in Z(G)$.

(G2) De fato, $Z(G) \neq \varnothing$ pois, $ea = a = ae$ para todo $a \in G$ temos que $e \in Z(G)$.

(G3) Existe elemento inverso, uma vez que para todo $x \in G$ tem-se

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

Logo, $x^{-1} \in Z(G)$, e portanto $Z(G)$ é um subgrupo de G.

Observe que, se G é abeliano, $Z(G) = G$, pois, todos os elementos de G comutariam.

(b) $N(a) = \{x \in G; xa = ax\} \leqslant G$.

Para mostrar que $N(a)$ é subgrupo de G, utilizaremos o Critério de Subgrupo:

1. $N(a) \neq \varnothing$ pois, $ea = ae = a$ para $e \in G$.

2. Sendo $x, y \in N(a)$, então $xa = ax$ e $ya = ay$. Assim,

$$\begin{aligned} a(xy^{-1}) &= (xy^{-1}yx^{-1})(axy^{-1}) \ \text{ pois, } \ xy^{-1}yx^{-1} = e \\ &= xy^{-1}yx^{-1}(ax)y^{-1} \\ &= xy^{-1}y(x^{-1}x)ay^{-1} \ \text{ pois, } \ ax = xa \\ &= xy^{-1}(yeay^{-1}) \\ &= xy^{-1}(ya)y^{-1} \\ &= xy^{-1}(ayy^{-1}) \ \text{ pois, } \ ay = ya \\ &= (xy^{-1})a. \end{aligned}$$

Logo, $(xy^{-1}) \in N(a)$. Portanto, $N(a)$ é um subgrupo de G.

■

Estes dois grupos desempenham papéis muito importantes no avanço da Teoria de Grupos.

Proposição 2.6. Sejam H e K subgrupos de um grupo G. Então $HK = \{x \in G\,;\, x = hk,\ h \in H \text{ e } k \in K\}$ é um subgrupo de G se, e somente se, $HK = KH$.

Demonstração. Suponhamos, inicialmente, que $HK = KH$; ou seja, se $h \in H$ e $k \in K$, então $hk = k_1h_1$ para alguns $k_1 \in K$ e $h_1 \in H$. Para mostrar que HK é um subgrupo, temos de verificar que é fechado e que todo elemento de HK tem inverso em HK. Demonstraremos o fechamento em primeiro lugar; portanto, considerando que $x = hk \in HK$ e $y = h^1k^1 \in HK$. Então,

$$xy = hkh^1k^1, \text{ mas } kh^1 \in KH = HK,\ kh^1 = h_2k_2 \text{ com } h_2 \in H \text{ e } k_2 \in K.$$

Logo, $xy = h(h_2k_2)k^1 = (hh_2)(k_2k^1) \in HK$ é fechado. Além disso,

$$x^{-1} = (hk)^{-1} = k^{-1}h^{-1} \in HK = KH.$$

Portanto, $x^{-1} \in HK$. Assim, HK é um subgrupo de G.

Por outro lado, se HK é um subgrupo de G, então, para todos $h \in H$, $k \in K$, tem-se $h^{-1}k^{-1} \in HK$ e então $hk = (h^{-1}k^{-1})^{-1} \in HK$. Assim, $KH \subset HK$. Agora, se x é um elemento qualquer de HK, $x^{-1} = hk \in HK$ e então $x = (x^{-1})^{-1} = (hk)^{-1} = k^{-1}h^{-1} \in KH$, portanto $HK \subset KH$. Desse modo, podemos concluir que $HK = KH$. ■

Como consequência, temos o caso particular em que G é um grupo abeliano, nessa situação, é evidente que $HK = KH$. Portanto, podemos deduzir o seguinte corolário.

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

Na próxima seção, estudaremos os Grupos Cíclicos, os quais são essenciais para estabelecer importantes resultados na Teoria de Grupos.

2.5 Grupos Cíclicos

Sendo G um grupo e $a \in G$. Denotamos por $\langle a \rangle$ o conjunto de todas as potências de a, ou seja,

$$\begin{aligned} \langle a \rangle &:= \{a^n;\ n \in \mathbb{Z}\} \\ &= \{\ldots, a^{-2}, a^{-1}, e, a, a^2, \ldots\}. \end{aligned}$$

O próximo resultado nos diz que $\langle a \rangle$ é subgrupo de G.

Proposição 2.7 (O Subgrupo cíclico gerado por a). Sejam $(G,\cdot)$ um grupo e $a \in G$. Então $\langle a\rangle$ é um subgrupo de G, chamado de subgrupo cíclico gerado por a.

Demonstração. De fato, podemos observar que $\langle a\rangle \neq \varnothing$, pois $a^0 = e \in \langle a\rangle$.
Sejam $x, y \in \langle a\rangle$, com $x = a^m$ e $y = a^n$ e $m, n \in \mathbb{Z}$. Daí,

$$xy = a^m a^n = a^{m+n} \in \langle a\rangle$$

e, para todo n, temos $(a^n)^{-1} = a^{-n} \in \langle a\rangle$. ■

Exemplo 2.30. Sendo $\mathbb{Z}$ um grupo aditivo. Prove que $\langle n\rangle$, o subgrupo cíclico gerado por n, é $n\mathbb{Z} = \{kn;\ k \in \mathbb{Z}\}$. Em particular, $2\mathbb{Z} = \langle 2\rangle$. Note também que $\mathbb{Z} = \langle 1\rangle$.

Solução: Por definição,

$$\langle n\rangle = \{\ldots, -3n, -2n, -n, 0, n, 2n, 3n, \ldots\} = n\mathbb{Z}.$$

Em particular,

$$\langle 2\rangle = \{\ldots, -6, -4, -2, 0, 2, 4, 6, \ldots\} = 2\mathbb{Z}.$$

Definição 2.9. Um grupo G é dito cíclico, se existir $a \in G$ tal que.

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

Observe que para um grupo cíclico $G = \langle a\rangle$, temos duas possibilidades:

1. $a^n = e$, para algum $n \in \mathbb{N}$. Neste caso, G tem ordem finita;
2. $a^n \neq e$, para todo $n \in \mathbb{N}$. Neste caso, todas as potências de a são distintas e portanto G tem ordem infinita.

Observação 2.12. Se G é um grupo cíclico, então o gerador de G, ou seja, o elemento $a \in G$ tal que $G = \langle a\rangle$, em geral, não é único. Por exemplo, $\mathbb{Z}_4 = \langle 1\rangle$ e $\mathbb{Z}_4 = \langle 3\rangle$.

veremos, agora, uma propriedade dos grupos cíclicos, quanto a sua comutatividade.

Proposição 2.8. Todo grupo cíclico é abeliano.

Demonstração. Considere G um grupo cíclico, ou seja, $G = \langle a\rangle = \{a^n;\ n \in \mathbb{Z}\}$ Sejam $x, y \in G$, com $x = a^m$ e $y = a^n$ e $m, n \in \mathbb{Z}$. Daí,

$$xy = a^m a^n = a^{m+n} = a^{n+m} = a^n a^m = yx.$$

Logo, G é abeliano. ■

Estudaremos, agora, três teoremas fundamentais para a compreensão de subgrupos gerados por um conjunto.

Teorema 2.31. Sendo G um grupo e C a coleção de todos os subgrupos de G. Então

$$\bigcap_{H \in C} H$$

é um subgrupo de G.

Teorema 2.32. Sendo G um grupo e $S \subseteq G$. Seja C a coleção de todos os subgrupos de G que contenha S. Então o conjunto,

$$\langle S \rangle = \bigcap_{H \in C} H$$

satisfaz as seguintes condições:

1. $\langle S \rangle$ é um subgrupo de G que contenha S.
2. Para todo $H \in C$, $\langle S \rangle \subseteq H$.

Portanto, $\langle S \rangle$ é o menor subgrupo de G que contenha S.

Como consequência,

Corolário 2.2. $\langle S \rangle$ é o único subgrupo de G que satisfaz as condições 1. e 2. do Teorema 2.32.

2.6 Ordem de um elemento

Nesta seção, exploraremos algumas afirmações e teoremas que se relacionam com a ordem de um elemento. A ordem de um elemento, em termos gerais, é o menor número inteiro positivo que, ao elevarmos o elemento a essa potência, resulta no elemento identidade do grupo.

Definição 2.10. Sendo G um grupo e a um elemento pertencente a G. Afirmamos que:

(a) a tem ordem finita, se existe $n \in \mathbb{Z}_+$ tal que $a^n = e$.

Neste contexto, o menor inteiro positivo n_0 tal que $a^{n_0} = e$, denominamos a ordem de a e representamos por $O(a) = n_0$ ou $Ord(a) = n_0$.

(b) a tem ordem infinita caso não exista $n \in \mathbb{N}$ tal que $a^n = e$ e denotamos por $O(a) = \infty$ ou $Ord(a) = \infty$.

Em um grupo G, tem-se sempre,

$$Ord(a) = 1 \Leftrightarrow a = e.$$

Exemplo 2.33. (a) Em $\mathbb{Z}_8$ temos que $Ord(6) = 4$, visto que $4 \cdot 6 = 24 \equiv 0(mod 8)$.

(b) Em $\mathbb{U}_{11}$ temos que $Ord(4) = 5$, pois $4^5 = 1024 \equiv 1(mod 11)$.

(c) Em $\mathbb{Z}$ temos que $Ord(5) = \infty$, pois não existe $n \in \mathbb{Z}$ tal que $n \cdot 5 = 0$.

Proposição 2.9. Sendo G um grupo finito. Então todo elemento $a \in G$ tem ordem finita.

Demonstração. Levando em consideração o seguinte conjunto

$$\{a^n;\ n \in \mathbb{N}\} = \{e, a, a^2, a^3, ...\}.$$

Como G é finito, temos pelo Princípio da casa dos Pombos (se n objetos são distribuídos em m lugares e se $n > m$, então alguns lugares recebem pelo menos dois objetos) que este conjunto de potências de a não pode ser infinito. Portanto, duas potências de a devem ser iguais, digamos $a^i = a^j$ em que $i \neq j$. Se assumimos que $i > j$ então tem-se,

$$a^{i-j} = a^i \cdot a^{-j} = a^i \cdot a^{-i} = e.$$

Em especial $Ord(a) \leqslant i - j$. Logo a ordem de a é finita. ■

Proposição 2.10. Seja G um grupo.

(1) Dado $a \in G$, $a \neq e$, tem-se:

$$Ord(a) = 2 \Leftrightarrow a = a^{-1}.$$

Demostração: Se $Ord(a) = 2$, então $a^2 = e$. Assim,

$$a^{-1}a^2 = a^{-1} \Rightarrow a = a^{-1}.$$

Reciprocamente, se $a = a^{-1}$, então $aa = aa^{-1}$, ou seja, $a^2 = e$, o que implica em $Ord(a) = 2$, pois $a \neq e$. ■

(2) $Ord(a) = Ord(a^{-1})$, para todo $a \in G$.

Demostração:

Caso 1: Suponha que ordem de a é finita, isto é $Ord(a) = n$. Então,

$$(a^{-1})^n = (a^n)^{-1} = e^{-1} = e$$

isso mostra que $Ord(a^{-1}) \leqslant n = Ord(a)$. Por outro lado, se $m = Ord(a^{-1})$ então

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

isto implica que $Ord(a) \leqslant m = Ord(a^{-1})$. Portanto $n = m$, ou, $Ord(a) = Ord(a^{-1})$.

Caso 2: Considere que a tem ordem infinita. Então para todo $n \in \mathbb{Z}_+$ temos que $a^n \neq e$. Porém,

$$(a^{-1})^n = (a^n)^{-1} \neq e, \forall n \in \mathbb{Z}_+.$$

portanto, a^{-1} tem ordem infinita.

■

(3) Se $Ord(a) = 2$ para todo $a \in G - \{e\}$, então G é abeliano.

Demostração: Por hipótese, $Ord(a) = 2$ para todo $a \in G - \{e\}$. Logo, pelo item (1),

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

Agora, dados $a, b \in G$, temos que $ab \in G$. Desse modo,

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

o que mostra que G é abeliano. ■

(4) Se $Ord(a) = nm$, então $Ord(a^m) = n$.

Demostração: Inicialmente,

$$Ord(a) = nm \Rightarrow a^{nm} = e \Rightarrow (a^m)^n = e.$$

só nos resta mostrar que n é o menor inteiro positivo satisfazendo $(a^m)^n = e$. Se $r \in \mathbb{N}$ e $r < n$ é tal que $(a^m)^r = e$, então

$$\begin{cases} a^{mr} = e \\ mr < mn. \end{cases} \tag{2.6}$$

Isso contradiz o fato de mn ser a ordem de a. Portanto, $Ord(a^m) = n$.

■

Proposição 2.11. Se $Ord(a) = n$ e $m \in \mathbb{Z}_+$, então $a^m = e \iff n|m$.

Demonstração. $(\Leftarrow)$ Considere que $n|m$. Então existe $k \in \mathbb{Z}_+$ tal que, $m = kn$. Portanto,

$$a^m = a^{kn} = (a^n)^k = e^k = e.$$

$(\Rightarrow)$ Suponha, agora que $a^n = e$. Considere que $m \geq n$. pelo algoritmo da divisão, euclidiana, existem $q, r \in \mathbb{Z}$ tal que $m = q \cdot n + r$, com $0 \leqslant r < n$. Logo:

$$e = a^m = a^{q \cdot n + r} = a^{q \cdot n} \cdot a^r = (a^n)^q \cdot a^r = e^q \cdot a^r = a^r$$

Como $r < n = Ord(a)$ temos que $r = 0$. Portanto $m = qn \Rightarrow n|m$. ■

Teorema 2.34. Sejam G um grupo e $a \in G$.

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

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

Demostração. (1) Basta notar que para cada $k \in \mathbb{Z}$, $k = mq + r$, com q, $r \in \mathbb{Z}$ e $0 \leqslant r < m$, o que acarreta em $a^k = a^r$.

(2) Se $Ord(a) = m$, segue que os elementos $e, a, a^2, \ldots, a^{m-1}$ são todos distintos. Com efeito, se $a^i = a^j$ para $0 \leqslant i < j \leqslant m-1$, então $a^{j-i} = e$ e $j - i < m$, o que é uma contradição, pois $Ord(a) = m$. Agora, seja $H = \langle a \rangle$. Pelo item (1), sabemos que dado $k \in \mathbb{Z}$, $a^k = a^r$, sendo $r \in \{0, 1, \ldots, m-1\}$. Por isso,

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

tem ordem m.

Reciprocamente, suponhamos que $H = \langle a \rangle$ tem ordem finita. Isso significa que as potências a^i, com $i \in \mathbb{Z}$, não podem ser todas distintas. Por conseguinte, existem $i, j \in \mathbb{Z}$, com $i < j$, de maneira que $a^i = a^j$, ou seja, $a^{j-i} = e$. Mas, isso implica que a tem ordem finita, digamos $Ord(a) = m$. Assim, como mencionado anteriormente, os elementos,

$$e, a, a^2, \ldots, a^{m-1}$$

são todos distintos. Por isso, pelo item (1),

$$H = \langle a \rangle = \{a^r;\ r = 0, 1, \ldots, m-1\} = \{e, a, a^2, \ldots, a^{m-1}\}.$$

isto é, a ordem de H é m.

■

De acordo com o item (2) do Teorema anterior, a ordem de um elemento a de um grupo G é igual a ordem do subgrupo cíclico por ele gerado. No caso de a ter ordem finita, $Ord(a) = |\langle a \rangle|$. Em virtude disto, concluímos que se G é um grupo finito, então todo elemento $a \in G$ tem ordem finita. No entanto, é importante notar que a recíproca não é necessariamente verdadeira. Ou seja, se todo elemento em um grupo G for de ordem finita, isso não implica necessariamente que G também tenha uma ordem finita.

2.7 Homomorfismo de Grupos

O conceito de homomorfismo é fundamental para o estudo de grupos, sendo uma poderosa ferramenta algébrica nesse contexto. De maneira geral, o homomorfismo de grupos é uma função que mantém a estrutura algébrica entre dois grupos, estabelecendo uma correspondência entre os elementos de um grupo inicial e um grupo final, de forma que as operações do grupo sejam preservadas. Em suma, é uma relação que assegura a preservação das operações entre grupos distintos.

Definição 2.11. Sejam $(G_1, *)$ e $(G_2, \cdot)$ dois grupos. Uma função,

$$f : G_1 \to G_2$$

denota-se homomorfismo de G_1 em G_2, quando

$$f(a*b) = f(a)\cdot f(b), \text{ para todo } a,b \in G_1.$$

Exemplo 2.35. Para quaisquer grupos G_1 e G_2, a função $f : G_1 \to G_2$ dada por $f(g) = e_2$ para todo $g \in G_1$, é homomorfismo, denotado **homomorfismo trivial**.

Exemplo 2.36. Para um grupo G qualquer, a aplicação $id : G \to G$ dada por $id(a) = a$ para todo $a \in G$, é um homomorfismo, chamado **homomorfismo identidade**.

Exemplo 2.37. A função $f : \mathbb{R}_+^* \to \mathbb{R}$, dada por $f(x) = logx$ para todo $x \in \mathbb{R}_+^*$, é homomorfismo de $(\mathbb{R}_+^*, \cdot)$ em $(\mathbb{R}, +)$, pois se x, $y \in \mathbb{R}_+^*$,

$$f(x\cdot y) = log(xy) = log(x) + log(y) = f(x) + f(y).$$

Exemplo 2.38. Seja $g : \mathbb{Z} \to \mathbb{Z}$ dada por $g(x) = x+2$, para qualquer $x \in \mathbb{Z}$ não é homomorfismo, pois:

$$g(x+y) = x+y+2 \neq (x+2)+(y+2) = g(x)+g(y).$$

Definição 2.12. Sendo $f : G_1 \to G_2$ um homomorfismo de grupos.

(1) Se f é injetora, então dizemos que f é um monomorfismo.

(2) Se f é sobrejetora, então f é um epimorfismo.

(3) Se f é bijetora, então f é um isomorfismo.

(4) Se $G_1 = G_2$, então f é um endomorfismo.

(5) Se f é bijetora e $G_1 = G_2$, então dizemos que f é um automorfismo.

A seguir, apresentamos uma proposição que ilustra como um homomorfismo de grupos $f : G_1 \to G_2$ pode nos fornecer informações sobre uma propriedade algébrica específica do grupo G_2.

Proposição 2.12. Seja $f : G_1 \to G_2$ um homomorfismo de grupos. Se f é sobrejetor de G_1 e G_1 for abeliano, então G_2 é necessariamente abeliano.

Demonstração. Para $a_1, b_1 \in G_2$, provaremos que $a_1 \cdot b_1 = b_1 \cdot a_1$. Como f é sobrejetor, existem $a, b \in G_1$ tais que $f(a) = a_1$ e $f(b) = b_1$. Desde que G_1, é abeliano, então $a \cdot b = b \cdot a$. Portanto,

$$\begin{aligned} a_1 \cdot b_1 = f(a)\cdot f(b) &= f(a\cdot b) \\ &= f(b\cdot a) \\ &= f(b)\cdot f(a) \\ &= b_1 \cdot a_1. \end{aligned}$$

Isto é, $a_1 \cdot b_1 = b_1 \cdot a_1$, o que prova que G_2 é também abeliano. ■

Vamos esboçar algumas propriedades básicas específicas aos homomorfismos. Tais propriedades nos conduzirão a importantes resultados.

Proposição 2.13. Sendo $f : G_1 \to G_2$ um homomorfismo de grupos. Então,

(1) $f(e_1) = e_2$.

Demonstração. Como $e_1 = e_1 \cdot e_1$, então

$$f(e_1) = f(e_1 \cdot e_1) = f(e_1) \cdot f(e_1).$$

Portanto, $f(e_1)$ é necessariamente a identidade de G_2, isto é, $f(e_1) = e_2$. ■

(2) $f(a^{-1}) = f(a)^{-1}$, para todo $a \in G_1$.

Demonstração. Para todo $a \in G_1$, $a \cdot a^{-1} = e_1$. Então,

$$f(a \cdot a^{-1}) = f(e_1) = e_2,$$

ou seja, $f(a) \cdot f(a^{-1}) = e_2$, o que implica que $f(a^{-1}) = f(a)^{-1}$. ■

(3) $Im(f) = \{f(a);\ a \in G_1\}$ é um subgrupo de G_2, denotado a imagem de f.

Demonstração. Sendo $f(e_1) = e_2$, então $Im(f) \neq \varnothing$. Agora, dados $x, y \in Im(f)$, existem $a, b \in G_1$ tais que $f(a) = x$ e $f(b) = y$. Por isso,

$$x \cdot y^{-1} = f(a) \cdot f(b)^{-1} = f(a) \cdot f(b^{-1}) = f(a \cdot b^{-1}),$$

de maneira que $x \cdot y^{-1} \in Im(f)$ e $Im(f) < G_2$. ■

As conclusões provenientes da proposição 2.13 podem ser expressas nas seguintes afirmações: um homomorfismo não apenas "preserva" as operações dos grupos, mas também a identidade de G_1 e o inverso de cada elemento $a \in G_1$.

Proposição 2.14. Seja $f : G_1 \to G_2$ um homomorfismo de grupos. Se H é um subgrupo de G_2, então a imagem inversa $f^{-1}(H)$ de H por f,

$$f^{-1}(H) = \{x \in G_1;\ f(x) \in H\},$$

é um subgrupo de G_1.

Demonstração. Como $e_2 \in H$ e $f(e_1) = e_2$, então $f^{-1}(H) \neq \varnothing$. Agora, suponhamos que $a, b \in f^{-1}(H)$. Assim, por definição, $f(a) \in H$ e $f(b) \in H$. Como H é subgrupo de G_2, também, podemos afirmar que $f(b)^{-1} = f(b^{-1})$ está em H. Portanto, temos

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

Logo, $a \cdot b^{-1} \in f^{-1}(H)$, implicando que $f^{-1}(H) < G_1$. ■

Entre os subgrupos $f^{-1}(H)$ de G_1, vamos ressaltar de modo especial o caso em que $H = \{e_2\}$, denotando $f^{-1}(H)$ por $ker(f)$, isto é,

$$ker(f) = \{x \in G_1;\ f(x) = e_2\}.$$

Tal subgrupo, de importância fundamental, chama-se núcleo de f.

Teorema 2.39. Seja $f : G_1 \to G_2$ um homomorfismo de grupos. Então,

(1) $ker(f) = \{e_1\}$ se, e somente se, f é injetora.

(2) $ker(f) < G_1$.

Demonstração.

(1) Suponhamos que $ker(f) = \{e_1\}$, e sejam $x_1, x_2 \in G_1$. Tem-se:

$$\begin{aligned} f(x_1) = f(x_2) &\Rightarrow f(x_1)\cdot f(x_2)^{-1} = e_2 \ \text{(operando à direita com } f(x_2)^{-1}) \\ &\Rightarrow f(x_1)\cdot f(x_2^{-1}) = e_2 \ \text{(pois } f(x_2)^{-1} = f(x_2^{-1})) \\ &\Rightarrow f(x_1\cdot x_2^{-1}) = e_2. \ \text{(pois } f \text{ é homomorfismo)} \end{aligned}$$

Mas, $f(x_1 \cdot x_2^{-1}) = e_2$ implica em $x_1 \cdot x_2^{-1} \in ker(f) = \{e_1\}$, de modo que $x_1 \cdot x_2^{-1} = e_1$. Ou seja, $x_1 = x_2$. Portanto, f é injetora. Reciprocamente, dado $x \in G_1$,

$$x \in ker(f) \Leftrightarrow f(x) = e_2 = f(e_1).$$

Como por hipótese f é injetora, $f(x) = f(e_1)$ nos diz que $x = e_1$ e, por conseguinte, $ker(f) = \{e_1\}$.

(2) Já provamos na proposição 2.14 que $ker(f)$ é um subgrupo de G_1. Agora, para $g \in G_1$ e $h \in ker(f)$, $f(h) = e_2$ e

$$\begin{aligned} f(g\cdot h\cdot g^{-1}) = f(g)\cdot f(h)\cdot f(g^{-1}) &= f(g)\cdot e_2\cdot f(g^{-1}) \\ &= f(g)\cdot f(g)^{-1} \\ &= e_2. \end{aligned}$$

Portanto, podemos concluir que $g \cdot h \cdot g^{-1} \in ker(f)$, assim, $ker(f) < G_1$. ■

Proposição 2.15. Sendo G_1 e G_2 grupos e seja $\alpha : G_1 \to G_2$ um homomorfismo. Se $a \in G_1$ tem ordem finita, então $Ord(\alpha(a))$ divide $Ord(a)$.

Demonstração. Sendo $n = Ord(a)$. Então $a^n = e_1$, assim

$$\alpha(a)^n = \alpha(a^n) = \alpha(e_1) = e_2.$$

Portanto, $\alpha(a)^n = e_2$. Logo, temos que $Ord(\alpha(a))$ divide $Ord(a)$. ■

2.8 Grupos especiais

Nesta seção, estudaremos alguns grupos que são considerados significativos na Teoria de Grupos.

2.8.1 Grupos de Permutações

Um grupo formado por funções bijetoras de um conjunto em si mesmo, é chamado de Grupo de Permutação. Mais precisamente:

Definição 2.13. Seja X um conjunto qualquer. Uma bijeção $f : X \to X$ chama-se uma permutação e denota-se por S_X o conjunto de todas as permutações de X, ou seja

$$S_X = \{f : X \to X;\ f \text{ é uma bijeção}\}.$$

É possível verificar que $(S_X, \circ)$ é um grupo, no qual a operação $\circ$ corresponde à composição de funções. Este grupo é denotado de grupo simétrico de X ou grupo de permutações de X. De modo particular, quando o conjunto X tem um número finito de elementos, digamos $X = \{1,2,3,...,n\}$, então S_X tem uma representação e nome especiais. Neste caso, denota-se S_X por S_n e chama-se grupo simétrico de grau n ou grupo das permutações de n letras. Nota-se que S_n só é abeliano quando $X = \{1\}$ ou $X = \{1,2\}$.

Notação: Dado $f \in S_n$ é usual representar f por meio de uma matriz $2 \times n$, da seguinte maneira:

$$f = \begin{pmatrix} 1 & 2 & ... & n \\ f(1) & f(2) & ... & f(n) \end{pmatrix}.$$

Na primeira linha os elementos de $\{1,2,...,n\}$ e abaixo de cada i, onde $1 \leq i \leq n$, encontra-se a sua imagem $f(i)$.

Teorema 2.40. Seja $n \geq 1$. O grupo das permutações S_n de grau n tem $n!$ elementos.

Demonstração. Seja $f \in S_n$. Temos n possibilidades para a imagem $f(1)$, $(n-1)$ possibilidades para $f(2)$, $(n-2)$ possibilidades para $f(3)$, ... , 2 possibilidades para $f(n-1)$ e uma possibilidade para $f(n)$. Portanto pelo principio multiplicativo, f é uma das bijeções possíveis:

$$n \cdot (n-1) \cdot (n-2) \cdot ... \cdot 2 \cdot 1 = n!$$

Portanto $|S_n| = n!$. ■

Exemplo 2.41. S_A é abeliano se, e somente se, $|A| \leq 2$.
De fato,

1. Se $A = 1$, é trivial.

2. Se $A = 2$, temos $f : \{1,2\} \to \{1,2\}$. Assim, considerando:

$$f = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix} \text{ e } g = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}.$$

Logo,

$$f \circ g = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \text{ e } g \circ f = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}.$$

Portanto, $f \circ g = g \circ f$.

3. Agora, se $|A| > 2$, considerando $x, y, z \in A$ e $f, g \in S_A$. Assim, definindo f como sendo,

$$\begin{aligned} f(x) &= y \\ f(y) &= x \\ f(a) &= a \,\forall\, a \in A - \{x,y\} \end{aligned}$$

e definindo g como sendo,

$$\begin{aligned} g(y) &= z \\ g(z) &= y \\ g(a) &= a \,\forall\, a \in A - \{y,z\}. \end{aligned}$$

Observe que,

$$f \circ g(x) = f(g(x)) = f(x) = y$$

mas

$$g \circ f(x) = g(f(x)) = g(y) = z$$

Logo, $f \circ g \neq g \circ f$. Portanto, S_A não é abeliano para $|A| > 2$.

Exemplo 2.42. (O Grupo S_3). S_3 denota o conjunto das bijeções $\{1,2,3\} \to \{1,2,3\}$, sendo um grupo composto por 6 elementos, onde a operação entre eles é a composição de funções. Logo,

$$S_3 = \{\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5, \alpha_6\},$$

ou seja,

$$\alpha_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \ \alpha_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \ \alpha_3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix},$$

$$\alpha_4 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \ \alpha_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \ \alpha_6 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}.$$

Façamos $\lambda = \alpha_6$ e $\beta = \alpha_2$. Assim,

$$\lambda^2 = \lambda \circ \lambda = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \alpha_5$$

$$\lambda^3 = \lambda^2 \circ \lambda = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = e = \alpha_1$$

$$\beta^2 = \beta \circ \beta = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = e = \alpha_1$$

$$\beta \circ \lambda = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \alpha_3$$

$$\lambda \circ \beta = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \alpha_4$$

Note que a partir de λ e β é possível formar o grupo S_3. Isso é equivalente a dizer que os elementos λ e β geram o grupo S_3. Foi possível observar também que $\beta \circ \lambda \neq \lambda \circ \beta$, assim, não é comutativo, como foi visto no exemplo anterior.

Para concluir essa seção, vamos estudar o Teorema de Cayley que destaca a relevância dos grupos de permutação na Teoria de Grupos, uma vez que ele viabiliza a representação de qualquer grupo por meio de um subgrupo apropriado do grupo de permutações. O Teorema de Cayley estabelece que todo grupo G é isomorfo a um grupo de permutações; mais precisamente, ele é isomorfo a um subgrupo de S_G.

Arthur Cayley (1821-1895) foi um matemático inglês que conduziu investigações em diversas áreas da Álgebra. Ele se destacou como um dos matemáticos mais produtivos de sua época, caracterizando-se pela clareza e elegância em sua forma de expressão textual.

Lema 2.1. Seja $(G, \cdot)$ um grupo. Para cada $g \in G$ a função $f_g : G \to G$ dada por $f_g(x) = gx$ para todo $x \in G$, é uma permutação de G, isto é $f_g \in S_g$.

Note que f_g denota-se translação à esquerda definida por g. Analogamente, $f_g(x) = xg$ denota-se translação à direita definida por g.

Demonstração. Dados $x_1, x_2 \in G$, com $f(x_1) = f(x_2)$, ou seja, $gx_1 = gx_2$, obtemos pela Lei do cancelamento (6) que $x_1 = x_2$. Por isso, f_g é injetora. Por outro lado, dado $y \in G$, $g^{-1}y \in G$ e $f_g(g^{-1}y) = g(g^{-1}y) = y$. Portanto, f é sobrejetora e, em decorrência disso, f é bijetora. ■

Teorema 2.43. Todo grupo G é isomorfo a um grupo de permutações.

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

$$\begin{aligned} \varphi : G &\longrightarrow G \\ g &\longmapsto f_g, \end{aligned}$$

sendo f_g definida de acordo com o Lema 2.1. Primeiramente, observamos que para $a, b \in G$,

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

de modo que $f_{ab} = f_a \cdot f_b$. Portanto,

$$\varphi(ab) = f_{ab} = f_a \cdot f_b = \varphi(a)\varphi(b).$$

Isso significa que φ é um homomorfismo. Agora,

$$\varphi(a) = \varphi(b) \Rightarrow f_a = f_b \Rightarrow ax = bx, \text{ para todo } x \in G.$$

Mas, em G, a igualdade $ax = bx$ implica em $a = b$, ou seja, φ é injetora. Consequentemente, $\varphi_1 : G \longrightarrow \varphi_1(G)$ dada por $\varphi_1(g) = \varphi(g)$ para todo $g \in G$ é um homomorfismo injetivo; naturalmente φ_1 é sobrejetora, pois toda aplicação $f : A \longrightarrow f(A)$ é naturalmente sobrejetora e, assim, bijetora. portanto, φ_1 é um isomorfismo, e como $\varphi_1(g) = \varphi(g)$, segue que G é isomorfo a $\varphi(G) < S_G$. ■

Embora o Teorema de Cayley não permita classificar todos os grupos, ele aponta o ambiente onde as informações dos grupos a princípio devem ser estudadas. A relevância do Teorema de Cayley é principalmente de ordem teórica, superando sua utilidade prática. Ele ilustra a capacidade de conceber a Teoria de Grupos como a análise de grupos de permutação. Em termos simples, grupos de permutação representam um modelo universal para a compreensão de todos os grupos concebíveis.

Na próxima subseção, vamos estudar uma classe essencial de Grupos de Permutações, os grupos de simetrias. Especificamente, enfatizaremos os Grupos Diedrais D_n, que são subgrupos de S_n com $2n$ elementos.

2.8.2 Grupos Diedrais

Chamamos de Diedrais e denotamos por D_n, o grupo das simetrias espaciais de um polígono regular de n lados.

Seja $P_1P_2P_3\cdots P_n$ um polígono regular de n lados. Sejam $E_1, E_2, ..., E_n$ seus eixos. Considerando o conjunto das transformações espaciais que preservam o polígono com a operação de composição temos:

- $e, R_{\frac{2\pi}{n}}$,..., $R_{\frac{2(n-1)\pi}{n}}$: as rotações no plano em torno do centro do polígono, no sentido anti-horário, de ângulos $0, \frac{2\pi}{n}$,..., e $\frac{2(n-1)\pi}{n}$, respectivamente.
- R_1, R_2,..., R_n: as rotações espaciais de ângulo com os eixos E_1, E_2,...,E_n, respectivamente.

Observação 2.13. O grupo D_n, munido com a operação de composição é um grupo não abeliano, uma vez que, em geral, as rotações planas e as rotações espaciais não comutam quando são combinadas.

Teorema 2.44. O grupo Diedral D_n é um grupo de ordem $2n$ gerado por dois elementos α e β, satisfazendo $\alpha^n = \beta^2 = e$, em que:

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & \dots & (n-1) & n \\ 3 & 1 & 2 & \dots & n & 1 \end{pmatrix} \text{ e } \beta = \begin{pmatrix} 1 & 2 & 3 & \dots & (n-1) & n \\ 1 & n & (n-1) & \dots & 3 & 2 \end{pmatrix}.$$

Observa-se também que o grupo D_n, contém ele próprio um subgrupo de ordem n. Com efeito,

$$R_n = \{e, \alpha, \alpha^2, ..., \alpha^{n-1}\}$$

é um subgrupo de D_n, com ordem n - o grupo das rotações do polígono P_n.

Vamos mencionar dois casos específicos e construir suas tabelas de multiplicação de forma detalhada. Esses casos são o grupo D_n das simetrias espaciais de um triângulo equilátero e o grupo D_n das simetrias espaciais de um quadrado.

Exemplo 2.45. (O Grupo D_3) Seja $P_1P_2P_3$ um triângulo equilátero e sejam $E_1E_2E_3$ seus eixos. Considerando o conjunto das transformações espaciais que preservam o triângulo com a operação de composição temos:

- e, $R_{\frac{2\pi}{3}}$, $R_{\frac{4\pi}{3}}$: as rotações no plano em torno do centro do triângulo, no sentido anti-horário, de 0, $\frac{2\pi}{3}$ e $\frac{4\pi}{3}$, respectivamente.
- R_1, R_2, R_3: as rotações espaciais de ângulo com os eixos E_1, E_2, E_3 respectivamente.

Assim, $S_3 = \{e, R_{\frac{2\pi}{3}}, R_{\frac{4\pi}{3}}, R_1, R_2, R_3\}$ e com a operação de composição de funções é um grupo, que não é abeliano pois $R_1 \circ R_2 = R_{\frac{4\pi}{3}}$ e $R_1 \circ R_2 = R_{\frac{2\pi}{3}}$.

O grupo D_3 pode ser gerado por dois elementos, por exemplo $R_{\frac{2\pi}{3}}$ e R_1.

Tabela 2.5: Tábua de Cayley do grupo D_3

$\cdot$	e	$R_{\frac{2\pi}{3}}$	$R_{\frac{4\pi}{3}}$	R_1	R_2	R_3
e	e	$R_{\frac{2\pi}{3}}$	$R_{\frac{4\pi}{3}}$	R_1	R_2	R_3
$R_{\frac{2\pi}{3}}$	$R_{\frac{2\pi}{3}}$	$R_{\frac{4\pi}{3}}$	e	R_3	R_1	R_2
$R_{\frac{4\pi}{3}}$	$R_{\frac{4\pi}{3}}$	e	$R_{\frac{2\pi}{3}}$	R_2	R_3	R_1
R_1	R_1	R_2	R_3	e	$R_{\frac{4\pi}{3}}$	$R_{\frac{2\pi}{3}}$
R_2	R_2	R_3	R_1	$R_{\frac{2\pi}{3}}$	e	$R_{\frac{4\pi}{3}}$
R_3	R_3	R_1	R_2	$R_{\frac{4\pi}{3}}$	$R_{\frac{2\pi}{3}}$	e

Fonte: Autoria própria

Exemplo 2.46 (O Grupo D_4). Seja $P_1P_2P_3P_4$, um quadrado, sejam D_1, D_2, M e N os seus eixos. Considerando o conjunto das transformações espaciais que preservam o quadrado com a operação de composição temos:

- e, $R_{\frac{\pi}{2}}$, R_π, $R_{\frac{3\pi}{2}}$: as rotações no plano em torno do centro do quadrado, no sentido anti-horário, de ângulo 0, $\frac{\pi}{2}$, π e $\frac{3\pi}{2}$, respectivamente.
- R_M, R_N, R_1, R_2: as rotações espaciais de ângulo π com eixos M, N, D_1 e D_2, respectivamente.

Assim $D_4 = \{e, R_{\frac{\pi}{2}}, R_\pi, R_{\frac{3\pi}{2}}, R_M, R_N, R_1, R_2\}$ e com a operação de composição de funções é um grupo, que não é abeliano pois $R_1 \circ R_M = R_{\frac{\pi}{2}}$ e $R_M \circ R_1 = R_{\frac{3\pi}{2}}$.

O grupo D_4, pode ser gerado por dois elementos, por exemplo $R_{\frac{\pi}{2}}$ e R_M.

Tabela 2.6: Tábua de Cayley do grupo D_4

$\cdot$	e	$R_{\frac{\pi}{2}}$	R_{π}	$R_{\frac{3\pi}{2}}$	R_M	R_N	R_1	R_2
e	e	$R_{\frac{\pi}{2}}$	R_{π}	$R_{\frac{3\pi}{2}}$	R_M	R_N	R_1	R_2
$R_{\frac{\pi}{2}}$	$R_{\frac{\pi}{2}}$	R_{π}	$R_{\frac{3\pi}{2}}$	e	R_2	R_1	R_M	R_N
R_{π}	R_{π}	$R_{\frac{3\pi}{2}}$	e	$R_{\frac{\pi}{2}}$	R_N	R_M	R_2	R_1
$R_{\frac{3\pi}{2}}$	$R_{\frac{3\pi}{2}}$	e	$R_{\frac{\pi}{2}}$	R_{π}	R_1	R_2	R_N	R_M
R_M	R_M	R_1	R_N	R_2	e	R_{π}	$R_{\frac{3\pi}{2}}$	$R_{\frac{\pi}{2}}$
R_N	R_N	R_2	R_M	R_1	R_{π}	e	$R_{\frac{\pi}{2}}$	$R_{\frac{3\pi}{2}}$
R_1	R_1	R_N	R_2	R_M	$R_{\frac{\pi}{2}}$	$R_{\frac{3\pi}{2}}$	e	R_{π}
R_2	R_2	R_M	R_1	R_N	$R_{\frac{3\pi}{2}}$	$R_{\frac{\pi}{2}}$	R_{π}	e

Fonte: Autoria própria

Os Grupos Diedrais são usados para descrever simetrias em formas geométricas regulares, como triângulos, quadrados e polígonos regulares em geral. Além disso, eles exemplificam grupos não abelianos, ou seja, mostram a ideia de grupos que não seguem a comutatividade na operação binária.

Capítulo 3

Classes Laterais e Teorema de Lagrange

Neste capítulo, será abordada o estudo das classes laterais e suas propriedades fundamentais. Além disso, iremos estabelecer e apresentar a demonstração do Teorema de Lagrange.

3.1 Classes Laterais

Definição 3.1. Considere G um grupo e H um subgrupo de G. Sobre G, definimos a relação de equivalência ($\sim$) da seguinte maneira:

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

de fato, é uma relação de equivalência pois,

1. **Reflexiva:** como $e = a^{-1}a \in H$, então $a \sim a$.
2. **Simétrica:** se $a \sim b$ então $a^{-1}b \in H$. Contudo, sendo H um subgrupo de G, então $(a^{-1}b)^{-1} = b^{-1}a \in H$. Isso mostra que $b \sim a$.
3. **Transitiva:** suponhamos que $a \sim b$ e $b \sim c$, então $a^{-1}b$, $b^{-1}c \in H$ tem-se,

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

   Portanto, $a \sim c$.

Diante disso, sendo G um grupo e H um subgrupo de G com a, $b \in G$ temos:
$a \sim b \Leftrightarrow a^{-1}b \in H$ se, somente se, existe $h \in H$ tal que $a^{-1} \in H \Leftrightarrow b = ah$, para algum $h \in H \Leftrightarrow b \in aH$. Assim, de acordo com a definição, a classe de equivalência que contém a é o conjunto,

$$\{b \in G;\ b \sim a\} = \{ah;\ h \in H\};$$

chamaremos esse conjunto por aH e será denotado de **classe lateral à esquerda de H em G que contém** a. Em específico, H é a classe lateral do elemento neutro e à esquerda. De maneira análoga, é possível estabelecer a seguinte relação de equivalência,

$$b \sim a \text{ se, e somente se, existe } h \in H \text{ tal que } b = ha \text{ ou } ba^{-1} \in H.$$

Desse modo, o conjunto Ha será à **classe lateral à direita de H em G que contém a**. Sendo assim, à classe lateral à direita de H em G é:

$$Ha = \{ha;\ h \in H\}.$$

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

$$G = \bigcup_{a \in G} aH$$

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

$$aH = bH \text{ ou } aH \cap bH = \varnothing.$$

Observação 3.1. É importante destacar que:

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

$$aH = \{ah;\ h \in H\} = \{ha;\ h \in H\} = Ha.$$

Logo, a classe lateral à direta de a coincide com sua classe à esquerda. Ao eliminar a suposição de comutatividade de G, não é mais possível afirmar que as classes à esquerda e à direita de algum subgrupo H são idênticas. Portanto, de forma geral, concluímos que $aH \neq Ha$.

(b) O subgrupo H é considerado uma classe lateral de si mesmo tanto à esquerda quanto à direita, pois

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

(c) Se H é finito então Ha e aH são finitas e $|Ha| = |H| = |aH|$.

(d) $a \in H \Leftrightarrow Ha = H$ e $a \in H \Leftrightarrow aH = H$.

(e) Na notação aditiva, em vez de aH denotamos $a + H = \{a + h;\ h \in H\}$.

Exemplo 3.1. Seja o grupo aditivo $G = \mathbb{Z}_6 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}\}$. Considerando o subgrupo $H = \{\overline{0}, \overline{3}\}$, encontre as classes laterais à esquerda e à direita de G sobre H.

Solução:

- $\overline{0} + H = \{\overline{0}, \overline{3}\} = H = H + \overline{0}$.
- $\overline{1} + H = \{\overline{1}, \overline{4}\} = H + \overline{1}$.

- $\overline{2}+H=\{\overline{2},\overline{5}\}=H+\overline{2}$.
- $\overline{3}+H=\{\overline{3},\overline{0}\}=H=H+\overline{3}$.

Portanto,

$$G=(\overline{0}+H)\cup(\overline{1}+H)\cup(\overline{2}+H),\ \text{ou}\ G=(H+\overline{0})\cup(H+\overline{1})\cup(H+\overline{2}).$$

Note que encontramos todas as classes laterais tanto à direita quando à esquerda que formam todo o grupo $\mathbb{Z}_6$.

Exemplo 3.2. Sejam $G=(\mathbb{Z},+)$ e $H=3\mathbb{Z}=\{3k;\ k\in\mathbb{Z}\}$. Como G é abeliano, então o conjunto aH é igual Ha. Sendo G infinito, vamos considerar um elemento arbitrário $n\in\mathbb{Z}$ e analisar $n+3\mathbb{Z}$. Não há mais nada natural do que fazer uso do algoritmo da divisão e considerar os resultados sobre classes laterias (de equivalência) vistos até aqui. Por esse algoritmo, existem q, $r\in\mathbb{Z}$ tais que,

$$n=3q+r,\ \text{com}\ \ r\in\{0,1,2\}.$$

Dessa forma,

$$n-r=3q\in H\Leftrightarrow n\sim r.$$

Portanto, sendo $\sim$ uma relação de equivalência sobre G, temos

$$n+3\mathbb{Z}=r+3\mathbb{Z}.$$

Como $r=0$, $r=1$ ou $r=2$, então $0+3\mathbb{Z}=3\mathbb{Z}$, $1+3\mathbb{Z}=\{1+3\lambda;\ \lambda\in\mathbb{Z}\}$ e $2+3\mathbb{Z}=\{2+3\lambda;\ \lambda\in\mathbb{Z}\}$ são as únicas classes à esquerda (à direita) de H. Consequentemente,

$$aH=Ha=\{3\mathbb{Z},1+3\mathbb{Z},2+3\mathbb{Z}\}.$$

Exemplo 3.3. Vamos agora considerar um caso em que o grupo não é abeliano. Consideremos $G=S_3=\{\alpha_1,\alpha_2,\alpha_3,\alpha_4,\alpha_5,\alpha_6\}$,

$$\alpha_1=\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix},\ \alpha_2=\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix},\ \alpha_3=\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix},$$

$$\alpha_4=\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix},\ \alpha_5=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix},\ \alpha_6=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}.$$

O conjunto $H=\{\alpha_1,\alpha_2\}$ é um subgrupo de S_3, pois $\alpha_2\circ\alpha_2=\alpha_1$. Como α_1, $\alpha_2\in H$, então $\alpha_1H=\alpha_2H=H$. As outras classes são:

$$\alpha_3H=\{\alpha_3\circ\alpha_1,\alpha_3\circ\alpha_2\}=\{\alpha_3,\alpha_5\}=\alpha_5H,$$

$$\alpha_4H=\{\alpha_4\circ\alpha_1,\alpha_4\circ\alpha_2\}=\{\alpha_4,\alpha_6\}=\alpha_6H.$$

Essas são as classes laterias à esquerda, de maneira que $aH = \{H, \{\alpha_3, \alpha_5\}, \{\alpha_4, \alpha_6\}\}$. Da mesma forma, $H\alpha_1 = H\alpha_2 = H$ e

$$H\alpha_3 = \{\alpha_1 \circ \alpha_3, \alpha_2 \circ \alpha_3\} = \{\alpha_3, \alpha_6\} = H\alpha_6,$$

$$H\alpha_4 = \{\alpha_1 \circ \alpha_4, \alpha_2 \circ \alpha_4\} = \{\alpha_4, \alpha_5\} = H\alpha_5.$$

Isso mostra que $Ha = \{H, \{\alpha_3, \alpha_6\}, \{\alpha_4, \alpha_5\}\}$ e, desse modo, $aH \neq Ha$.

O exemplo 3.3 reforça o que foi observado anteriormente: nem sempre as classes laterais à esquerda coincidem com as classes laterais à direita. Isso ocorre devido ao fato que S_3 não é um grupo abeliano. No entanto, essa característica não é essencial para que se tenha $aH = Ha$. Um grupo G pode não ser abeliano e ainda assim satisfazer $aH = Ha$, mesmo quando $H \neq \{e\}$. Neste contexto, H é denominado subgrupo normal ou invariante. Estudaremos esses grupos na próximo seção.

3.1.1 Propriedades das Classes Laterais

Nesta subseção, iremos enfatizar algumas propriedades fundamentais das Classes laterais que são consequências imediatas da definição anterior. Diante disso, sendo G um grupo com uma operação de multiplicação e H um subgrupo de G em que $a, b \in G$ tem-se:

(a) $aH = bH$ se, e somente se, $b^{-1}a \in H$.

(b) $aH = bH \Leftrightarrow a \in bH$.

(c) Se $a \in G$, então $aH \neq \varnothing$

O conjunto quociente de G por essa relação, denotado por G/H, é o conjunto das classes laterais aH, com $a \in G$. Um dos elementos desse conjunto é o próprio H, pois $H = eH$.

Proposição 3.1.

1. Todas as classes laterais de H em G têm a mesma cardinalidade, igual à de H.

$$\begin{aligned} \alpha : E &\longrightarrow D \\ aH &\longmapsto Ha^{-1}. \end{aligned}$$

   Em que $E = \{aH;\ a \in G\}$, $D = \{Ha;\ a \in G\}$ e α bijetiva.

   Note que E são as classes laterais à esquerda e D são as classes laterais à direita.

2. As funções

$$\begin{aligned} \beta_1 : H &\longrightarrow aH \\ h &\longmapsto ah \end{aligned}$$

e

$$\begin{aligned} \beta_2 : H &\longrightarrow Ha \\ h &\longmapsto ha \end{aligned}$$

são bijetivas.

Demonstração.

1. Observe que α é claramente uma função sobrejetiva. Portanto, vamos demonstrar sua injetividade. É necessário demostrar que se $\alpha(a_1H) = \alpha(a_2H)$, então, tomando $x \in a_1H$, se existe $h \in H$, tal que $x = a_1h$. Logo,

   $$x = a_1h \Rightarrow h^{-1}a_1^{-1} = x^{-1} \in Ha_1^{-1}.$$

   Então, existe $h_1 \in H$ tal que:

   $$x^{-1} = h_1a_2^{-1} \Rightarrow x = a_2h_1^{-1} \in a_2H.$$

   Isto é, $a_1H \subset a_2H$.

2. Como ambas tem a mesma cardinalidade, vamos ponderar que β_1 e β_2 são bijetivas. Analisando β_1 observamos que o mesmo é sobrejetiva. Para verificar a injetividade, tem-se $h,k \in H$ então,

   $$\beta_1(h) = \beta_1(k) \Rightarrow ah = ak \Rightarrow a^{-1}ah = a^{-1}ak \Rightarrow h = k.$$

   Do mesmo modo, β_2 é sobrejetiva então basta verificar a injetividade. Sendo assim, temos $p,q \in H$ logo,

   $$\beta_2(p) = \beta_2(q) \Rightarrow ap = aq \Rightarrow a^{-1}ap = a^{-1}aq \Rightarrow p = q.$$

Portanto, concluímos que aH e Ha têm a mesma cardinalidade de H. ■

Definição 3.2. Sendo G um grupo e H um subgrupo de G. A cardinalidade do conjunto $aH = Ha$ chama-se o índice de H em G, ou seja, o número de classes laterais à direita ou à esquerda de H em G, o qual será denotado por $(G : H)$.

Note que o índice é a quantidade de classes laterais.

Observação 3.2. O índice $(G : H)$ pode ser finito ou infinito. Se G é finito, então $(G : H)$ é finito, uma vez que os elementos de aH são subconjuntos de G. Além do mais, é possível que um grupo infinito G possua um subgrupo $H \neq G$, para o qual o índice $(G : H)$ é finito; também pode ocorrer que esse mesmo grupo contenha um subgrupo $P \neq G$, de modo que $(G : P)$ é infinito.

Exemplo 3.4. De acordo com o exemplo 3.1, com $G = (\mathbb{Z}_6, +)$ e o subgrupo $H = \{\overline{0}, \overline{3}\}$, temos que $\overline{0}+H = H = H+\overline{0}$, $\overline{1}+H = H+\overline{1}$ e $\overline{2}+H = H+\overline{2}$ são as únicas classes laterais à esquerda e à direita de H. Por isso, $(G : H) = (6 : 2) = 3$.

3.2 Joseph Lagrange

Figura 3.1: Joseph Louis Lagrange



Fonte: Google Imagens

Joseph Louis Lagrange (1736-1813) foi um renomado matemático e físico-matemático italiano, considerado um dos grandes matemáticos do século XVIII. Ele foi contemporâneo e colaborador de Leonhard Euler (1707-1783) e sucedeu Euler na Academia de Berlim.

A principal obra-prima de Lagrange é a "Mécanique Analytique" (Mecânica Analítica), cujo conteúdo transparente e notação elegante abrange quase todas as áreas da matemática pura. É importante mencionar que este foi o primeiro livro sobre mecânica publicado sem a necessidade de diagramas, motivo de grande orgulho para Lagrange.

Lagrange introduziu o cálculo variacional na mecânica e fez importantes contribuições para a Teoria das Equações Diferenciais, elevando-a de estratagemas para uma ciência estabelecida. Seu livro "Théorie des fonctions analytiques" estabeleceu fundamentos para a Teoria de Grupos e antecipou o trabalho de Galois.

Joseph Louis Lagrange teve uma carreira notável com diversas realizações em várias áreas da matemática pura. Ele inventou o método de Resolução de Equações Diferenciais chamado "variação de parâmetros" e introduziu o sistema de coordenadas esféricas. Além disso, Lagrange destacou-se na Teoria dos Números, resolvendo problemas propostos por Fermat e acrescentando seus próprios teoremas. Sua contribuição proeminente estendeu-se praticamente a todas as áreas da Matemática pura. Sua visão de que a mecânica era um ramo da matemática pura trouxe uma abordagem inovadora, caracterizada pela generalização e universalidade presentes em seus trabalhos.

Seu objetivo principal na Matemática, e aparentemente em sua vida, era revisar e aprimorar os fundamentos do cálculo, oferecendo uma explicação mais rigorosa de como e por que o cálculo funciona. Antes de Lagrange, não existia um formalismo de limite estabelecido. Ele

acreditava que explicações conceituais ou intuitivas não deveriam ser incluídas em uma demonstração rigorosa, daí seu esforço em reduzir os fundamentos do cálculo à álgebra.

Uma consequência dessa linha de pensamento, é o Teorema de Lagrange, um dos teoremas mais fundamentais na Teoria de Grupos. Esse teorema surgiu após décadas de pesquisa dedicadas a responder a uma questão proposta pelo matemático italiano Scipione del Ferro aos algebristas entre os anos de 1500 e 1515. A questão era se as equações de grau igual ou superior a 3 poderiam ser resolvidas por meio de radicais. Lagrange desenvolveu as primeiras ideias relacionadas a essa questão, mas foi Abel quem conseguiu, pela primeira vez, provar de forma geral que essas equações não podem ser resolvidas por radicais. No próximo tópico iremos estudar esse teorema considerado a base da Teoria de Grupos Finitos.

3.3 Teorema de Lagrange

Teorema 3.5. Sejam G um grupo finito e H um subgrupo de G. Então a ordem de H divide a ordem de G, isto é,

$$|G| = |H|(G:H) \text{ e, portanto, } o(H)|o(G). \tag{3.1}$$

Demonstração: Por G ser finito, temos que $(G:H)$ também será. Além disso, de resultados anteriores sabemos que o número de classes laterais à direita e à esquerda é o mesmo, portanto, iremos considerar apenas as classes laterais à esquerda de H. Sendo assim, suponha que $(G:H) = n$ e considere $aH = \{a_1H, a_2H, a_3H, ..., a_nH\}$. Como aH é uma partição de G então

$$G = a_1H \cup a_2H \cup a_3H \cup ... \cup a_nH,$$

e ainda $a_iH \cap a_jH = \varnothing$ para $i \neq j$. Dessa maneira, levando em consideração o fato de a cardinalidade de cada classe à esquerda (aH) é igual a ordem de H, obtemos

$$\begin{aligned} |G| &= |a_1H| + |a_2H| + |a_3H| + ... + |a_nH| \\ |G| &= \underbrace{|H| + |H| + |H| + ... + |H|}_{n} = n|H| \end{aligned}$$

onde a ordem de H se repete n vezes. Portanto, $|G| = |H|(G:H)$. ■

Com base nesse teorema, é possível verificar facilmente se um determinado subconjunto de G é um subgrupo. Por exemplo, dado o subconjunto $H = \{\overline{0}, \overline{2}\}$ de $G = \mathbb{Z}_7$, com ordem igual a 2, teremos, de acordo com o Teorema de Lagrange que H não é subgrupo de G, uma vez que 2 não divide 7. No entanto, conforme foi destacado o Teorema de Lagrange, assegura que se H é um subgrupo de um grupo finito G, então $|H|$ divide $|G|$. E quanto a recíproca? Ou seja, se G é um grupo de ordem n e d divide n, então G possui necessariamente um subgrupo de ordem d? Isso certamente é verdade para grupos abelianos; contudo, não é para todo grupo finito.

Finalizaremos está seção destacando algumas consequências do Teorema de Lagrange e estudaremos Subgrupos Normais e Grupos Quocientes. Nos próximos capítulos debruçaremos

sobre as principais recíprocas do Teorema de Lagrange, nomeadamente os Teoremas de Cauchy e Sylow, explorando suas implicações no entendimento da estrutura e das propriedades dos grupos finitos.

3.3.1 Consequências Imediatas do Teorema de Lagrange

O Teorema de Lagrange trás algumas consequências imediatas, tais quais podemos analisar abaixo:

Corolário 3.1. Todo grupo finito de ordem prima é cíclico (em particular, é abeliano).

Demonstração. Seja G um grupo tal que, $|G| = p$, com p um número primo. Considere $x \in G$, com $x \neq e$, temos $\langle x \rangle$ um subgrupo de G que contém o conjunto $\{e, x\}$. Assim, pelo Teorema de Lagrange $|\langle x \rangle|$ é um divisor de $|G| = p$ e $|\langle x \rangle| > 1$. Portanto $|\langle x \rangle| = p$ e isso indica que $G = \langle x \rangle$. ■

Corolário 3.2. Se G é um grupo tal que, $|G| \leq 5$, então G é abeliano.

demonstração.

- Se $|G| = 1$, então $G = e$,
- Se $|G| = 2$, 3 ou 5, $\Rightarrow |G|$ é número primo, então é cíclico, logo, abeliano.
- Considere G tal que, $|G| = 4$. Se existir $x \neq e$, $x \in G$ tal que $\langle x \rangle = G$, então G é cíclico e portanto abeliano. Neste caso, G é isomorfo a $\mathbb{Z}_4$.

Suponha então que, para todo $x \in G$, $x \neq e$, temos $\langle x \rangle \neq G$. Ora, pelo Teorema de Lagrange segue imediatamente que, $|\langle x \rangle| = 2$. Assim,

$$x^2 = e, \text{ para todo } x \in G,$$

logo se $x, y \in G$ tem-se $xy = (xy)^{-1} = y^{-1}x^{-1} = yx$, isto é, G é abeliano (note que nesse caso G é do tipo $(\mathbb{Z}_2 \times \mathbb{Z}_2, +)$). ■

Corolário 3.3. Sejam G um grupo finito e K, H subgrupos de G, com $K \subset H$. Então,

$$(G : K) = (G : H) \cdot (H : K).$$

Demonstração. O Teorema de Lagrange implica que

$$(G : H) \cdot (H : K) = \frac{|G|}{|H|} \cdot \frac{|H|}{|K|} = \frac{|G|}{|K|} = (G : K).$$

■

Corolário 3.4. Sejam G um grupo finito e $a \in G$, então a ordem de a divide a ordem de G, ou seja, $ord(a) \big| |G|$.

Demonstração. O subgrupo gerado por a, $\langle a\rangle$, é um subgrupo do grupo finito G. Portanto, pelo Teorema de Lagrange, temos que $|\langle a\rangle|$ divide $|G|$. Mas, como por definição, a ordem do elemento a é a ordem do subgrupo $\langle a\rangle$, concluímos que, $ord(a)\big||G|$. ■

Observação 3.3. Este corolário implica que se G é um grupo de ordem n, então as possíveis ordens de seus elementos são divisores de n. Por exemplo, se $|G| = 30$, então para cada $a \in G$, $ord(a) \in \{1,2,3,5,6,10,15,30\}$. Mas não significa, necessariamente que para cada possível valor de ordem tenha elemento de G possuindo tal valor.

Corolário 3.5. Sejam G um grupo finito de ordem n e $a \in G$, então $a^n = e$.

Demonstração. Seja m a ordem do elemento $a \in G$, logo, $a^m = e$. De acordo com o Corolário 3.4, $m|n$, ou seja, existe um inteiro k, tal que $n = km$. Portanto,

$$a^n = a^{mk} = (a^m)^k = e^k = e.$$

■

Corolário 3.6. Se $H, K < G$ e G finito com $mdc(|H|,|K|) = 1$, então $H \cap K = \{e\}$.

Demonstração. Suponha que $a \in H \cap K$, então pelo Teorema de Lagrange:

$$Ord(a)\big||H| \text{ e } Ord(a)\big||K|,$$

como $mdc(|H|,|K|) = 1$, temos que $Ord(a) = 1$, daí $a = e$. ■

3.4 Subgrupos Normais e Grupos Quocientes

Na seção anterior abordamos um conceito muito interessante relacionado a grupos, a saber, o conceito de classe lateral. Subsequentemente, apresentamos e demostramos o principal teorema que versa sobre grupos finitos, o Teorema de Lagrange. Além disso, observamos que, dado um subgrupo $H < G$, nem sempre a igualdade das classes laterais à direita e à esquerda $aH = Ha$ se verifica, óbvia apenas para grupos abelianos. Deste modo, nesta seção, vamos apresentar condições que permitam a igualdade entre as classes laterais sobre um subgrupo H e suas consequências sobre o grupo.

3.4.1 Subgrupos Normais

Definição 3.3. Seja G um grupo. Um subgrupo H de G chama-se normal quando

$$ghg^{-1} \in H, \text{ para todo } g \in G \text{ e para todo } h \in H,$$

ou equivalentemente,

$$gHg^{-1} \subset H, \text{ para todo } g \in G.$$

Como $g \in G$ é qualquer, a expressão $ghg^{-1} \in H$ é equivalente $g^{-1}hg \in H$. O mesmo vale para as expressões $gHg^{-1} \subset H$ e $g^{-1}Hg \subset H$.

Notação: Um subgrupo normal H de um grupo G, também é dito invariante, e será indicado por $H \lhd G$.

Exemplo 3.6. Para um grupo G qualquer, tem-se que G e $\{e\}$ são subgrupos normais de G.

Exemplo 3.7. Se G é um grupo abeliano, então todo subgrupo H de G é normal.

Solução: De fato, se $g \in G$ e $h \in H$, então

$$ghg^{-1} = gg^{-1}h = eh = h \in H.$$

Exemplo 3.8. Seja um subgrupo H de S_3 dado por

$$H = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \right\}.$$

Para os elementos,

$$\beta = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \in S_3 \quad \text{e} \quad \alpha = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \in H,$$

temos que

$$\beta\alpha\beta^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \neq H.$$

Portanto, H não é um subgrupo normal de S_3

Proposição 3.2. 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 (2013, p. 232). ■

O teorema a seguir caracteriza os subgrupos normais.

Teorema 3.9. Seja H um subgrupo de um grupo G. Então, as seguintes condições são equivalentes:

1. $H \lhd G$.
2. $gHg^{-1} = H$, para todo $g \in G$.
3. $gH = Hg$, para todo $g \in G$.

Demonstração.

- (1) $\Rightarrow$ (2). Por hipótese, para cada $g \in G$, tem-se naturalmente a inclusão $gHg^{-1} \subset H$. Agora, dado $h \in H$,
$$h = g^{-1}(ghg^{-1})g \in H.$$
Pois $ghg^{-1} \in H \lhd G$. Isso significa que $H \subset gHg^{-1}$ e, portanto, $gHg^{-1} = H$.

- (2) $\Rightarrow$ (3). Para $g \in G$, seja $x \in gH$, digamos $x = gh$ para algum $h \in H$. Logo, por hipótese,
$$xg^{-1} = ghg^{-1} \in gHg^{-1} = H,$$
ou seja, $xg^{-1} = h_1$, como $h_1 \in H$. Portanto, $x = h_1 g \in Hg$, de modo que $gH \subset Hg$. Da mesma maneira, prova-se que $Hg \subset gH$. Consequentemente $Hg = gH$.

- (3) $\Rightarrow$ (1). Sejam $g \in G$ e $h \in H$. Como $gH = Hg$ e $gh \in Hg$. Segue que $gh = h_2 g$ para algum $h_2 \in H$, isto é, $ghg^{-1} = h_2 \in H$. Portanto, $H \lhd G$.

■

Observação 3.4. H é um subgrupo normal de G, se ele satisfaz as condições equivalentes do teorema anterior. Neste caso, toda classe lateral à esquerda é também uma classe lateral à direita e vice-versa. Desse modo,
$$aH = \{gH;\ g \in G\} = \{Hg;\ g \in G\} = Ha.$$
Neste sentido, quando H for um subgrupo normal de G, representaremos os conjuntos das classes laterais (aH ou Ha) por G/H ou $\frac{G}{H}$, ou seja,
$$G/H = \{gH;\ g \in G\}.$$

Proposição 3.3. Se H é um subgrupo de um grupo G tal que $(G : H) = 2$, então $H \lhd G$.

Demonstração. Conforme o Teorema 3.9, é suficiente mostrar que $gH = Hg$ para todo $g \in G$. Já sabemos que o próprio H é uma classe lateral à esquerda. Como $(G : H) = 2$, então aH contém exatamente duas classes laterais à esquerda e, sendo ele uma partição de G, $G - H$ é a outra classe lateral à esquerda. Se $g \in H$, então $gH = H = Hg$. Por outro lado, para $g \notin H$,
$$gH \notin H \ \ e \ \ Hg \neq H.$$
Por isso, $gH = G - H$. Similarmente, $Hg = G - H$. Desse modo, $gH = Hg$ para todo $g \in G$. Portanto, $H \lhd G$. ■

A proposição mencionada anteriormente se apresenta como uma ferramenta de grande utilidade quando se busca a determinação de subgrupos normais em grupos finitos, mesmo que a sua aplicabilidade seja um tanto quanto restrita. Por exemplo, no grupo S_3, todo subgrupo de H de ordem três é certamente normal, pois $(S_3 : H) = 2$. Essa condição, na verdade, simplifica significativamente o árduo processo de identificação de todos os subgrupos normais contidos em S_3.

3.4.2 Grupos Quocientes

Após a introdução do conceito de subgrupo normal e a discussão de alguns resultados relacionados, agora exploraremos sua aplicação para apresentar grupos quocientes. Sendo assim, o teorema subsequente garante que, com base na operação em G, é possível definir uma segunda operação sobre G/H, transformando-o em um grupo.

Teorema 3.10. Sejam $(G,\cdot)$ um grupo e H um subgrupo normal de G. Então,

$$\begin{array}{rcl} \cdot : G/H \times G/H & \longrightarrow & G/H \\ (xH, yH) & \longmapsto & (xH)\cdot(yH) = xyH \end{array}$$

define uma operação sobre G/H. Além disso, G/H é um grupo com esta operação.

Demonstração. Para verificarmos se " $\cdot$ " está bem definida sobre G/H, precisamos mostrar que o resultado independem dos representantes [1] das classes. Especificamente, se $x_1H = x_2H$ e $y_1H = y_2H$, com $x_1, x_2, y_1, y_2 \in G$, então

$$x_1H \cdot y_1H = x_2H \cdot y_2H.$$

Para $x_1H = x_2H$ e $y_1H = y_2H$, temos

$$x_1 \sim x_2 \quad \text{e} \quad y_1 \sim y_2 \Leftrightarrow x_1^{-1}x_2 = h_1 \in H \quad \text{e} \quad y_1^{-1}y_2 = h_2 \in H.$$

Portanto,

$$\begin{array}{rcl} y_1^{-1}x_1^{-1}x_2y_2 & = & y_1^{-1}h_1y_2 \quad (pois\ \ x_1^{-1}x_2 = h_1) \\ & = & h_2y_2^{-1}h_1y_2. \quad (pois\ \ y_1^{-1} = h_2y_2^{-1}) \end{array}$$

Como $H \lhd G$, então $y_2^{-1}h_1y_2 = h_3 \in H$. Assim,

$$\begin{array}{rcl} y_1^{-1}x_1^{-1}x_2y_2 & = & h_1h_2 \in H \\ & \Leftrightarrow & (x_1y_1)^{-1}(x_2y_2) \in H \\ & \Leftrightarrow & x_1y_1H = x_2y_2H, \end{array}$$

ou seja, $x_1H \cdot y_1H = x_2H \cdot y_2H$. Por conseguinte, "$\cdot$" é uma operação que está bem definida sobre G/H. Consideremos agora xH, yH, $zH \in G/H$. Desse modo, como a operação em G é associativa,

$$\begin{array}{rcl} xH \cdot (yH \cdot zH) & = & xH \cdot (yz)H \\ & = & x(yz)H \\ & = & (xy)zH \\ & = & (xyH) \cdot zH \\ & = & (xH \cdot yH) \cdot zH, \end{array}$$

[1] Isso faz necessário, visto que uma classe lateral pode ter mais do que um representante, isto é, g_1, $g_2 \in G$, $g_1 \neq g_2$, com $g_1H = g_2H$.

isto é, "$\cdot$" é associativa. Agora, é claro que

$$(xH)\cdot(eH) = (eH)\cdot(xH) = xH.$$

Por isso, H é o elemento neutro da operação em G/H. Para finalizar,

$$(xH)\cdot(x^{-1}H) = (x^{-1}H)\cdot(xH) = eH = H.$$

Desse modo, $x^{-1}H$ é o inverso de xH em G/H. Logo, $(G/H,\cdot)$ é um grupo. ■

A partir desse teorema podemos definir grupos quocientes.

Definição 3.4. 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; ele será denotado por G/H ou por $\frac{G}{H}$.

Note que considerando um grupo G e um subgrupo H de G, é possível estabelecer uma relação entre a ordem de H e a ordem do grupo quociente G/H. Sendo assim, de acordo com as definições 3.2 e 3.4 podemos escrever $|G/H| = (G:H)$, dessa forma, a ordem de G, é dada por $|G| = |H|(G:H)$.

Observação 3.5. É importante destacar que se G for aditivo e H um subgrupo normal de G, então representaremos a operação do grupo quociente G/H de forma aditiva. Com isso, para $\overline{x} = x+H$ e $\overline{y} = y+H$ em G/H,

$$\overline{x}+\overline{y} = (x+H)+(y+H) = (x+y)+H = \overline{x+y}.$$

Também, no grupo $(G/H,\cdot)$, dados $xH \in G/H$ e $n \in \mathbb{Z}$, temos que

$$(xH)^n = x^nH,$$

e no grupo $(G/H,+)$,

$$n(x+H) = nx+H.$$

Proposição 3.4. Sejam G um grupo e $H \lhd G$.

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

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

Demonstração. (1) Para $xH, yH \in G/H$,

$$\begin{aligned}(xH)\cdot(yH) = (xy)H &= (yx)H \quad \text{(pois G é abeliano)}\\ &= (yH)\cdot(xH),\end{aligned}$$

isto é, G/H é abeliano.

(2) Suponhamos que $G = \langle a \rangle$ e seja $xH \in G/H$. Como $x \in G$, existe $n \in \mathbb{Z}$ tal que $x = a^n$. Assim,

$$xH = a^nH = (aH)^n \in \langle aH \rangle.$$

Logo, $G/H \subset \langle aH \rangle$, e como naturalmente $\langle aH \rangle \subset G/H$, então $G/H = \langle aH \rangle$.

■

É importante destacar que a recíproca dos itens da proposição anterior não é válida.

Exemplo 3.11. Seja H um subgrupo de um grupo G tal que $x^2 \in H$ para todo $x \in G$. Provar que $H \lhd G$ e G/H é abeliano.

Solução: Para $x \in G$,

$$xhx^{-1} = xhxhh^{-1}x^{-2} = (xh)^2h^{-1}(x^2)^{-1} \in H,$$

pois $(xh)^2$ e x^2 estão em H. Desse modo, $H \lhd G$. Por outro lado, dado $xH \in G/H$,

$$(xH)^2 = x^2H = H,$$

pois $x^2 \in H$. Portanto, todo elemento de G/H diferente da identidade, H, tem ordem dois. Sendo assim, item (3) da proposição 2.10. Concluímos que G é abeliano.

Vimos no capitulo 2 que, dado um grupo G arbitrário, o centro de G, representado como $Z(G)$, é um subgrupo de G. Além disso, é possível perceber que $Z(G)$ é um subgrupo normal de G. Portanto, podemos estabelecer a seguinte proposição.

Proposição 3.5. 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. Seja $\overline{z}$ um gerador do grupo $G/Z(G)$. Então, para todo $g \in G$, existe i tal que $\overline{g} = \overline{z}^i$, logo $g = z^ih$ com $h \in Z(G)$. Se $g_1 := z^{i_1}h_1$ e $g_2 := z^{i_2}h_2$ são dois elementos quaisquer de G, temos

$$g_1g_2 = z^{i_1}h_1z^{i_2}h_2 = z^{i_1+i^2}h_1h_2 = z^{i_2}h_2z^{i_1}h_1 = g_2g_1,$$

pois h_1 e h_2 comutam com qualquer elemento de G. Isto mostra que o grupo G é abeliano, ou seja, $Z(G) = G$. ■

Capítulo 4

Recíprocas para o Teorema de Lagrange

Neste capítulo, exploraremos a recíproca do Teorema de Lagrange. Para isso, apresentaremos quatro importantes teoremas: o Teorema de Cauchy e os três Teoremas de Sylow. Veremos que o Teorema de Cauchy é um caso particular do primeiro Teorema de Sylow.

4.1 Conceitos Essenciais

Antes de adentrarmos na análise detalhada dos Teoremas de Cauchy e Sylow, dedicaremos um momento para aprofundar nosso entendimento em relação a alguns conceitos essenciais que desempenham um papel fundamental na compreensão das demonstrações desses teoremas. Esses conceitos são: Ação de um Grupo em um Conjunto, Classe de Conjugação, Equação de Classes, Órbita, Estabilizador e P-Grupos. Portanto, iniciaremos com uma breve apresentação desses conceitos.

4.1.1 Ação de um Grupo em um Conjunto

A ação de um grupo em um conjunto é uma versão mais sofisticada do conceito de operação binária 2.1, como podemos observar no que segue:

Definição 4.1. Seja G um grupo e X um conjunto não vazio. Uma ação de G em X é uma aplicação,

$$\begin{array}{rcl} * : G \times X & \longrightarrow & X \\ (g,x) & \longmapsto & g * x. \end{array}$$

Tal que:

1. Para todo $x \in X$ tem-se $e * x = x$, onde $e \in G$ é o elemento neutro;
2. Para todo g_1, $g_2 \in G$ e $x \in X$ tem-se,

$$g_1 * (g_2 * x) = (g_1 * g_2) * x.$$

Nestas condições, X é chamado G-conjunto.

É comum usar a notação $G|X$ para representar a ação de um grupo G em um conjunto X.

Exemplo 4.1. A aplicação trivial, dada por $(g,x) \longmapsto x$ define uma ação de G em X.

Exemplo 4.2. Todo grupo G em si mesmo é um G-conjunto, onde a ação de $g_1 \in G$ sobre $g_2 \in G$ é dado pela multiplicação direta. Isto, é $g_1 * g_2 = g_1 g_2$. Se H é um subgrupo de G, também podemos considerar G como um H-conjunto onde $g * h = gh$.

Observe que esta ação do grupo G em si mesmo é chamada translação.

Exemplo 4.3. Seja X um conjunto qualquer e S_X o grupo contendo todas as permutações de X. Então, X é um S_X-conjunto onde para cada elemento $x \in X$ e permutação $\sigma \in S_X$, a ação de σ sobre x corresponde ao efeito da aplicação da permutação σ a x. Além disso, a condição 2 é satisfeita como uma consequência direta da definição da multiplicação de permutações, que se baseia na composição de funções. A condição 1 é imediatamente satisfeita devido à definição da permutação identidade. Em particular, podemos afirmar que $\{1,2,3,...,n\}$ é um S_n-conjunto.

Na subseção a seguir, estudaremos sobre a Classe de Conjugação e a Equação de Classes.

4.1.2 Classe de Conjugação e Equação de Classes

Dizemos que x e y são elementos conjugados em G e denotamos por, $x \sim_G y$ onde $\sim_G$ é uma relação de conjugação sobre G. Isto é, dizemos que y é conjugado de x em G, ou equivalentemente, $x \sim_G y$, se existe $g \in G$, tal que, $y = g^{-1}xg$. Podemos observar também, que esta relação é uma relação de equivalência, pois são válidas as seguintes propriedades:

(a) $x \sim_G x$. (reflexiva)

Demonstração. De fato, dado $e \in G$, temos $x = exe^{-1}$, para todo $x \in G$. ■

(b) $x \sim_G y$, então $y \sim_G x$. (simétrica)

Demonstração. De fato,

$$x \sim_G y \Rightarrow y = g^{-1}xg \Rightarrow gyg^{-1} = x \Rightarrow y \sim_G x.$$

■

(c) Se $x \sim_G y$ e $y \sim_G z$ então $x \sim_G z$. (transitiva)

Demonstração. De fato, $x \sim_G y \Rightarrow g^{-1}xg = y$ e $y \sim_G z \Rightarrow h^{-1}yh = z$. Deste modo,

$$\begin{aligned} z = h^{-1}yh &= h^{-1}(g^{-1}xg)h \\ &= (h^{-1}g^{-1})x(gh) \\ &= (gh)^{-1}x(gh) \end{aligned}$$

considerando $gh = w$,

$$= \quad w^{-1}xw.$$

Portanto, $x \sim_G z$. ■

Definição 4.2. A classe definida por $Ha = \{y \in G;\ x \sim_G y\} = \{g^{-1}xg;\ g \in G\}$ é chamada classe de conjugação (em G) determinada pelo elemento $x \in G$, ou seja, é o conjunto dos elementos de G que são conjugados de x.

Vamos denotar a classe de conjugação Ha por C_x. Observe que Ha representa uma classe lateral (à direita) de H em G.

Exemplo 4.4. Encontre a classe de conjugação de R_M em $D_4 = \{e, R_{\frac{\pi}{2}}, R_\pi, R_{\frac{3\pi}{2}}, R_M, R_N, R_1, R_2\}$.

Solução: Para determinar a classe de conjugação de R_M, simplesmente o conjugamos com todos os elementos de D_4. Assim, analisando a tábua de multiplicação do grupo D_4,

Tabela 4.1: Tábua de multiplicação do grupo D_4

$\cdot$	e	$R_{\frac{\pi}{2}}$	R_π	$R_{\frac{3\pi}{2}}$	R_M	R_N	R_1	R_2
e	e	$R_{\frac{\pi}{2}}$	R_π	$R_{\frac{3\pi}{2}}$	R_M	R_N	R_1	R_2
$R_{\frac{\pi}{2}}$	$R_{\frac{\pi}{2}}$	R_π	$R_{\frac{3\pi}{2}}$	e	R_2	R_1	R_M	R_N
R_π	R_π	$R_{\frac{3\pi}{2}}$	e	$R_{\frac{\pi}{2}}$	R_N	R_M	R_2	R_1
$R_{\frac{3\pi}{2}}$	$R_{\frac{3\pi}{2}}$	e	$R_{\frac{\pi}{2}}$	R_π	R_1	R_2	R_N	R_M
R_M	R_M	R_1	R_N	R_2	e	R_π	$R_{\frac{3\pi}{2}}$	$R_{\frac{\pi}{2}}$
R_N	R_N	R_2	R_M	R_1	R_π	e	$R_{\frac{\pi}{2}}$	$R_{\frac{3\pi}{2}}$
R_1	R_1	R_N	R_2	R_M	$R_{\frac{\pi}{2}}$	$R_{\frac{3\pi}{2}}$	e	R_π
R_2	R_2	R_M	R_1	R_N	$R_{\frac{3\pi}{2}}$	$R_{\frac{\pi}{2}}$	R_π	e

Fonte: Autoria própria

obtemos que $C_{R_M} = \{R_M, R_N\}$, pois

- $e \cdot R_M \cdot e^{-1} = R_M$.
- $R_{\frac{\pi}{2}} \cdot R_M \cdot {R_{\frac{\pi}{2}}}^{-1} = R_2 \cdot R_{\frac{3\pi}{2}} = R_N$.
- $R_\pi \cdot R_M \cdot {R_\pi}^{-1} = R_N \cdot R_\pi = R_M$.
- $R_{\frac{3\pi}{2}} \cdot R_M \cdot {R_{\frac{3\pi}{2}}}^{-1} = R_1 \cdot R_{\frac{\pi}{2}} = R_N$.
- $R_M \cdot R_M \cdot {R_M}^{-1} = e \cdot R_M = R_M$.
- $R_N \cdot R_M \cdot {R_N}^{-1} = R_\pi \cdot R_N = R_M$.
- $R_1 \cdot R_M \cdot {R_1}^{-1} = R_{\frac{\pi}{2}} \cdot R_1 = R_M$.

- $R_2 \cdot R_M \cdot {R_2}^{-1} = R_{\frac{3\pi}{2}} \cdot R_2 = R_M$.

Definição 4.3. Se G é um grupo finito e existem n classes de conjugação (em G) com representantes $x_1, x_2, ..., x_n$, então,

$$G = C_{x_1} \cup C_{x_2} \cup ... \cup C_{x_n}.$$

Ou seja, G é igual à união (disjunta) das classes de conjugação, e assim chegamos a chamada equação de classes:

$$|G| = |C_{x_1}| + |C_{x_2}| + ... + |C_{x_n}|. \tag{4.1}$$

Proposição 4.1. Sejam G um grupo e $x \in Z(G)$. Então, $C_x = \{x\}$.

Demonstração. De fato, $C_x = \{g^{-1}xg;\ g \in G\}$. Como $x \in Z(G)$, temos $xg = gx$, para todo $g \in G$. Deste modo, $g^{-1}xg = x$. Portanto, $G_x = \{x\}$. ■

Dessa proposição, concluímos que se um elemento está no centro do grupo, então ele se relaciona apenas com ele mesmo, na relação de conjugação. Note que, $g^{-1}xg = x$ é equivalente a $xg = gx$. no caso de x conjugar apenas com ele mesmo, o elemento de G tomado foi a identidade. A partir da proposição anterior a equação de classes torna-se:

$$|G| = |Z(G)| + \sum_{x_i \notin Z(G)} |C_{x_i}|. \tag{4.2}$$

Isto é, o número de elementos de G é igual a quantidade de elementos do seu centro adicionado ao somatório de cada classe de conjugação dos elementos que não estão no centro.

Proposição 4.2. Sejam G um grupo finito e $x \in G$. Então, o índice $(G : C_{G(x)})$ é igual ao número de elementos $|C_x|$ da classe de conjugação C_x. Em particular, $|C_x|$ é um divisor de $|G|$ para todo $a \in G$.

Demonstração. Ver Adilson Gonçalves (1999, p. 137). ■

4.1.3 Estabilizador e Órbita

Na Teoria de Grupos, o estabilizador é, basicamente, o conjunto de elementos do grupo que fixam o elemento x numa conjugação.

Definição 4.4. Sejam G um grupo agindo sobre um conjunto X e $x \in X$. O conjunto

$$E(x) := \{g \in G;\ g^{-1}xg = x\} \subseteq G,$$

é chamado de estabilizador de x em G.

Ou seja, o estabilizador é o conjunto dos elementos do grupo que comutam com o elemento dado, x.

Observação 4.1. O Estabilizador é um subgrupo do grupo. De fato, Pela definição de ação de um grupo em um conjunto 4.1, temos que $e^{-1}xe = x$, ou seja, $e \in E(x)$. Isso significa que $E(x)$ não é vazio. Mais ainda, se $g, h \in E(x)$, então:

$$(gh)^{-1}x(gh) = h^{-1}(g^{-1}xg)h = h^{-1}xh = x.$$

Além disso,

$$g^{-1} * x = g^{-1} * (g * x) = (g^{-1}g) * x = e * x = x.$$

Portanto, gh, $g^{-1} \in E(x)$. Isto é, para todo $x \in X$, $E(x) \leqslant G$.

Observe que, a partir de uma ação e dos estabilizadores de todos os elementos do conjunto X, podemos construir subgrupos do grupo G. Em toda ação, o estabilizador é um subgrupo do grupo. Se pensarmos na última proposição 4.1 da seção anterior, onde $x \in Z(G)$, sabemos que x comuta com todos os elementos de G, logo $E(x) = G$.

Observação 4.2.

1. Se G age sobre si mesmo por conjugação, então o estabilizador de $x \in G$ é o subgrupo de G dado por:

   $$E(x) = \{a \in G;\ axa^{-1} = x\} = \{a \in G;\ ax = xa\}.$$

   Neste caso particular de ação, o estabilizador de $x \in G$ é chamado de normalizador ou centralizador de $x \in G$ e representado por $N(x)$.

2. Se G sobre $\mathcal{P}(G)$ (conjunto das partes de G) por conjugação, então o estabilizador de $S \in \mathcal{P}(G)$ é o subgrupo de G dado por,

   $$E(S) = \{a \in G;\ aSa^{-1} = S\}.$$

   Neste caso particular de ação, o estabilizador de $S \in \mathcal{P}(G)$ é chamado de normalizador de S em G e denotado por $N_G(S)$.

A órbita na Teoria de Grupos refere-se ao conjunto de todos os elementos obtidos ao aplicar a ação de um grupo em um elemento particular do conjunto.

Definição 4.5. Sejam G um grupo agindo sobre um conjunto X e $x \in X$. O conjunto

$$\mathcal{O}(x) := \{g * x;\ g \in G\} \subseteq X,$$

é chamado a órbita de x em G.

Note que os estabilizadores são subgrupos do grupo G, enquanto que as órbitas são subconjuntos do conjunto X.

Observação 4.3.

1. Considere G agindo sobre si mesmo por translação. A órbita de $x \in G$ é dada por:

$$\mathcal{O}(x) = \{ax;\ a \in G\} = G.$$

2. Quando consideramos a ação de G sobre si mesmo por conjugação, a órbita de $x \in G$ é dada por:

$$\mathcal{O}(x) = \{a^{-1}xa;\ a \in G\},$$

chamada a classe de conjugação de x e denotada por C_x.

Para compreender o próximo teorema, é fundamental ter a definição de representação de um grupo por permutações.

Definição 4.6. Sejam G um grupo, C um conjunto e $\mathcal{P}(C)$ o grupo de permutações de C. Uma representação de G no grupo de permutações de C é um homomorfismo $p : G \to \mathcal{P}(C)$, isto é, uma função tal que $p(g_1g_2) = p(g_1 \circ g_2)$. Diz-se também que o grupo G opera sobre o conjunto C.

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

$$\text{Para todo } x,y \in C,\ x \sim y \text{ se, e somente, existe } g \in G \text{ tal que } p(g)(x) = y.$$

O teorema seguinte enfatiza a estreita conexão entre a órbita de um elemento e o seu estabilizador.

Teorema 4.5. Sejam $p : G \to \mathcal{P}(C)$ uma representação do grupo G no grupo de permutações do conjunto C, e $x \in C$. Então a aplicação β abaixo é uma bijeção:

$$\begin{array}{rcl} \beta : \mathcal{O}(x) & \longrightarrow & \{\text{Classe laterias à esquerda de } E(x) \text{ em } G\} \\ p(g)(x) & \longmapsto & gE(x). \end{array}$$

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

Demonstração. Ver Garcia e Lequain (2014, p.255). ■

A seguir vamos definir P-Grupos que refere-se a um grupo no qual a ordem de todos os seus elementos é uma potência de um número primo p.

4.1.4 P-Grupos

Seja p um número primo e G um grupo. Se $|G| = p^n$, $n \in \mathbb{N}$, dizemos que G é um p-grupo. Pelo Teorema de Lagrange 3.5 um subgrupo de um p-grupo é também um p-grupo.

Proposição 4.3. 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. Pela equação de classes temos,

$$|G| = |Z(G)| + \sum_{x_i \notin Z(G)} |C_{x_i}|.$$

Para elementos $x_i \notin Z(G)$, temos $|C_x| > 1$. Pelo teorema 4.5, sabemos que $|C_x|$ divide $|G|$, isto é, divide p^n; portanto, $|C_x|$ é um múltiplo de p,

$$\sum_{x_i \notin Z(G)} |C_{x_i}|$$

é um múltiplo de p e logo

$$|Z(G)| = |G| - \sum_{x_i \notin Z(G)} |C_{x_i}|.$$

é um múltiplo de p. Por outro lado, já que o elemento neutro pertence a $Z(G)$, temos $|Z(G)| \neq 0$. Portanto, o centro $Z(G)$ tem pelo menos p elementos. ■

Corolário 4.1. Se p é um número primo e $|G| = p^2$ então G é um grupo abeliano.

Demonstração. Pela proposição anterior 4.3, temos $|Z(G)| = p$ ou p^2; por outro lado, já sabemos pela proposição 3.5 que o centro de um grupo nunca pode ter índice no grupo igual a um primo. Logo, $|Z(G)| = p^2$ e portanto, o grupo G é abeliano.

■

Note que demonstramos no capítulo anterior que se $|G| = p$ então G é cíclico e agora acabamos de demonstrar que se $|G| = p^2$, então G é abeliano.

Nas seções subsequentes, dedicaremos nosso foco ao estudo detalhado do Teorema de Cauchy e dos Teoremas de Sylow. Conforme já discutimos no capítulo 3, reconhecemos que a recíproca do Teorema de Lagrange não é válida, em geral. Para estabelecer a validade dessa recíproca em determinados casos, recorremos à exploração dos Teoremas de Cauchy e Sylow, os quais fornecerão a base necessária para alcançar esse objetivo.

4.2 Teorema de Cauchy

Figura 4.1: Augustin Louis Cauchy



Fonte: Google Imagens

Augustin-Louis Cauchy (1789-1857) foi um eminente matemático francês que deixou numerosas e significativas contribuições para matemática, com um enfoque notável na Teoria de Grupos. Ele percebeu a importância intrínseca dos grupos de permutações, levando a publicar uma série de artigos sobre o tema no período de 1844-1846. Além disso, seus trabalhos exerceram uma influência profunda em muitos matemáticos da época, incluindo Cayley, que inspirado por essas contribuições, foi o pioneiro a formular a noção geral implícita no caso particular.

A seguir iremos estudar o Teorema de Cauchy, sendo um caso particular do primeiro Teorema de Sylow, onde, inicialmente, exploraremos o cenário abeliano e, posteriormente, o caso geral que será reduzido ao caso abeliano.

Lema 4.1. Sejam G um grupo abeliano finito e p um número primo tal que $p\big||G|$. Então, existe $a \in G$ de ordem p. Portanto $\langle a \rangle$ é um subgrupo de ordem p.

Demonstração. Considere $|G| = pm$, a prova será feita por indução sobre m.

- Se $m = 1$, então $|G| = p$ e assim G é cíclico.
- Se $m > 1$, considere $x \in G/\{e\}$ tal que $Ord(x) = r$. Logo, pelo Teorema de Lagrange 3.5 $r\big||G| = pm$.

Se $p|r$, então existe $r = ps$ para algum s, sendo assim, $Ord(x^{r/p}) = p$, pois $(x^{\frac{r}{p}})^p = x^{\frac{r}{p}\cdot p} = x^r = e$, então $x^{\frac{r}{p}}$ é elemento de ordem p, assim podemos construir subgrupo cíclico gerado por ele, isto é, $\langle x^{\frac{r}{p}} \rangle$. Se $p \nmid r$, então são primos entre si e com $r\big|pm$, r dividirá m. Como G é abeliano, todo subgrupo é normal a G, logo tomando $\langle x \rangle$, temos $\langle x \rangle \trianglelefteq G$ e $G/\langle x \rangle$ é um grupo quociente tal que

$$\left|\frac{G}{\langle x \rangle}\right| = \frac{|G|}{|\langle x \rangle|} = \frac{pm}{r} = p \cdot \frac{m}{r} < pm = |G|.$$

Logo, pela hipótese de indução o grupo $\frac{G}{\langle x\rangle}$ possui um elemento, digamos que $\overline{y} \in \frac{G}{\langle x\rangle}$, tal que $\overline{y}$ tenha ordem p e $y^p \in \langle x\rangle$. Pois, como $Ord(x) = r$. Então,

$$e = (y^p)^r = y^{pr} = (y^r)^p,$$

e portanto $Ord(y^r) = p$. ■

Teorema 4.6. Sejam G um grupo finito e p um número primo tal que $p\big||G|$. Então, existe $a \in G$ de ordem p.

Demonstração. Seja $|G| = pm$, a prova será feita novamente por indução sobre m.

- Se $m = 1$, então $|G| = p$ e assim G é cíclico de ordem p e não há o que demostrar.
- Se $m > 1$, temos pela equação de classes de conjugação que:

$$|G| = |Z(G)| + \sum_{x_i \notin Z(G)} |C_{x_i}|.$$

Se para todo $x_i \notin Z(G)$, $P\big||C_{x_i}|$, então $p\big||Z(G)|$, uma vez que $p\big||G|$. Como $Z(G)$ é abeliano, o lema anterior garante a existência de algum elemento de $Z(G)$ com ordem p. Agora, suponha que existe $x_i \notin Z(G)$ tal que $p \nmid |C_{x_i}|$. Como

$$|G| = |C_{x_i}|(G : C_{x_i}) = |C_{x_i}| \cdot \frac{|G|}{|C_{x_i}|},$$

e $p\big||G|$, concluímos que $p\big||C_{x_i}|$.

Observe que $C_{x_i} \leqslant G$ e $C_{x_i} < |G|$, então pela hipótese de indução, C_{x_i} possui algum elemento de ordem p. ■

4.3 Teoremas de Sylow

Figura 4.2: Peter Ludwig Mejdell Sylow



Fonte: Google Imagens

Peter Ludwig Mejdell Sylow (1832-1918) destacou-se como um eminente matemático norueguês, exercendo um papel essencial na Teoria de Grupos. No ano de 1872, Sylow publicou um conjunto de teoremas que atualmente são identificados como os Teoremas de Sylow. Esses teoremas fundamentais detalham as características dos subgrupos p-máximos de um grupo finito, agora reconhecidos como os subgrupos p de Sylow.

No capítulo três, ao final da seção sobre o Teorema de Lagrange, exploramos a recíproca desse teorema. Em outras palavras, questionamos se, dada a ordem n de um grupo G, sempre há um subgrupo de ordem d quando d divide n? Os Teoremas de Sylow é um dos resultados que torna essa recíproca verdadeira. Na seção anterior, discutimos o Teorema de Cauchy, e agora estamos prestes a estudar os três Teoremas de Sylow.

Sabemos pelo Teorema Fundamental da Aritmética que, se $|G| \geqslant 2$, $|G| = p_1^{t_1} \cdot p_2^{t_2}, \cdots, p_r^{t_r}$. O primeiro Teorema de Sylow mostra que, para cada i conseguimos H_i, tal que $|H_i| = p_i^{t_i}$, onde $i \in \{0,1,...,t_i\}$. Por exemplo, se $|G| = 36$, como $36 = 6^2 = (2\cdot 3)^2 = 2^2 \cdot 3^2$, então $|G| = 2^2 \cdot 3^2$, e assim, o primeiro Teorema de Sylow nos garante que, temos pelo menos um subgrupo de G com ordem igual as possíveis potências obtidas, isto é, $2^0 = 3^0, 2^1$ e 2^2, 3^1 e 3^2. Veremos a demonstração, com todos os detalhes, a seguir:

Teorema 4.7 (Primeiro Teorema de Sylow). Sejam G um grupo finito, p um número primo e $|G| = p^m b$, onde $p \nmid m$ e $b \geq 1$. Então para cada $i = \{0,1,2,...,m\}$ existe H subgrupo de G tal que $|H| = p^i$.

Demonstração. Seja $|G| \geqslant 2$, a demonstração será feita por indução sobre G.

Para $|G| = 2 = 2^0 \cdot 2^1$ temos $\{e\}$ subgrupo de G de ordem 2^0 e G é um subgrupo de G com ordem 2^1. Agora, suponha que $|G| > 2$ e o resultado é verdadeiro para todo grupo K tal que, $|K| < |G|$. Seja $i \in \{0,1,2,...,m\}$, observe que o nosso objetivo é encontrar um subgrupo de ordem p^i. Assim, se $i = 0$, basta toma $H_j = \{e\} = \langle e \rangle$.

Agora, vamos supor que $i \in \{1,2,...,m\}$, então:

Considere que existe um subgrupo L próprio de G tal que $p^i \big| |L|$. Como $|L| < |G|$, pela hipótese de indução, existe $H \leqslant L$ tal que $|H| = p^i$. Logo $H \leqslant L$ com $|H| = p^i$. Suponha, agora, que para todo L subgrupo próprio de G, temos $p^i \nmid |L|$.

Afirmação: $p \big| |Z(G)|$.

Se G é abeliano, então $G = Z(G)$ e como $p \big| |G|$, em particular $p \big| |Z(G)|$. Suponha G não abeliano, tomando $T \subseteq G$ um conjunto com relação a ação de conjugação, obtemos a equação de classes de conjugação:

$$|G| = |Z(G)| + \sum_{x \notin Z(G)} (G : C_G(x)).$$

Para cada $x \in T \setminus Z(G)$, segue que $C_G(x) \subsetneqq G \Rightarrow p^i \nmid |C_G(x)|$, para todo $x \in T \setminus Z(G)$.

Afirmação 2: $p \mid (G : C_G(x))$, para todo $T \setminus Z(G)$.

De fato, se $p \nmid (G : C_G(x))$, para algum $x \in T \setminus Z(G)$, então $mdc(p,(G : C_G(x))) = 1 \Rightarrow mdc(p^i,(G : C_G(x))) = 1$, como $p^i \big| |G|$ e pelo Teorema de Lagrange 3.5 temos que $|G| = |C_G(x) \cdot (G : C_G(x))|$, então $p^i \big| |C_G(x)|$, absurdo!

Portanto, $p \big| (G : C_G(x))$ para todo $x \in T \setminus Z(G)$. Assim,

$$p \left| \left(\sum_{x \in T \setminus Z(G)} (G : C_G(x)) \right) \right.$$

e como $p \big| |G|$, então $p \big| |Z(G)|$.

Como $P \big| |Z(G)|$ e $Z(G)$ é um grupo finito e abeliano temos, pelo lema de Cauchy 4.1, que $Z(G)$ admite um elemento y com $ord(y) = p$. Como $y \in Z(G)$, então $\langle y \rangle \subseteq Z(G) \Rightarrow \langle y \rangle \trianglelefteq G$. Logo, podemos considerar o grupo quociente $\frac{G}{\langle y \rangle}$. Pelo Teorema de Lagrange 3.5,

$$\left| \frac{G}{\langle y \rangle} \right| = \frac{|G|}{|\langle y \rangle|} = \frac{|G|}{p} < |G|.$$

Além disso,

$$\left| \frac{G}{\langle y \rangle} \right| = \frac{|G|}{p} = \frac{p^m \cdot b}{p} = p^{m-1} \cdot b$$

com $i \in \{0,1,2,...,m-1\}$, então

$$p^{i-1} \left| \left| \frac{G}{\langle y \rangle} \right| \right.,$$

pela hipótese de indução $\frac{G}{\langle y \rangle}$ possui um subgrupo H' tal que $|H'| = p^{i-1}$. Agora, considere o morfismo quociente,

$$\begin{array}{rccc} \pi : G & \longrightarrow & \dfrac{G}{\langle y \rangle} \\ x & \longmapsto & x\langle y \rangle. \end{array}$$

Tomando a imagem inversa desse morfismo temos $H_i = \pi^{-1}(H')$ que é um subgrupo de G, que contém $\langle y \rangle$. Daí, $H' = \pi(H) = \frac{H}{\langle y \rangle} \Rightarrow \langle y \rangle \lhd G$ e H. Logo, pelo Teorema de Lagrange 3.5

$$|H| = |\langle y \rangle| \cdot \left| \frac{H}{\langle y \rangle} \right| = Ord(y) \cdot |H'| = p \cdot p^{i-1} = p^i.$$

■

Em posse deste teorema, podemos estudar algumas implicações.

Corolário 4.2. Sejam G um grupo finito e $p \in \mathbb{N}$ um número que divide $|G|$, então G admite um elemento de ordem p.

Demonstração. Por hipótese podemos escrever $|G| = p^m \cdot b$, com $b, m \in \mathbb{N}$ e $mdc(p,b) = 1$. Como $m \geqslant 1$, então pelo primeiro Teorema de Sylow4.7 existe H um subgrupo de G, onde $|H| = p^i = p$. Daí, H é cíclico e logo, existe $x \in H$ tal que $H = \langle x \rangle$. Portanto, $x \in G$ e $Ord(x) = |\langle x \rangle| = |H| = p$. ■

Observe que este corolário é equivalente ao Teorema de Cauchy, o que demonstra que o primeiro Teorema de Sylow é uma generalização do Teorema de Cauchy.

Definição 4.7. Sejam G um grupo finito, e $|G| = p^m \cdot b$, onde p é um número primo, $p \in \mathbb{N}$ e m, $b \in \mathbb{N}$ com $mdc(p,b) = 1$. Então dizemos que H é um p-subgrupo de G:

- Se H é um p-grupo;
- Se $|H| = p^k$, para algum $k \in \mathbb{N}$;
- E se H é um subgrupo de G.

Além disso, dizemos que H é um p-subgrupo de Sylow de G, se H é um subgrupo de G e $|H| = p^m$ (maior potência que divide $|G|$).

Corolário 4.3. Sejam G um grupo finito e $p \in \mathbb{N}$ um número primo. Então, G é um p-grupo se, e somente se, $Ord(x)$ é uma potência de p, para todo $x \in G$.

Demonstração. $(\Rightarrow)$ Seja $x \in G$. Por hipótese $|G| = p^t$, para algum $t \in \mathbb{N}$. Pelo Teorema de Lagrange 3.5,

$$Ord(x) \big| p^t \Rightarrow Ord(x) = p^i,$$

para algum $i \in \{0,1,2,...,t\}$.
$(\Leftarrow)$ Tome $x \in G, x \neq e$. Por hipótese $Ord(x) = p^t$, para algum $t \in \mathbb{N}$. Pelo Teorema de Lagrange 3.5, $Ord(x) \big| |G|$ e como $p \big| Ord(x)$, por transitividade $p \big| |G|$. Logo, podemos escrever $|g| = p^b \cdot b$, onde b, $m \in \mathbb{N}$ e $p \nmid b$.

Suponha, por absurdo, que $b > 1$. Pelo Teorema Fundamental da Aritmética existe $q \in \mathbb{N}$ primo tal que $q \big| b$. Logo, $q \neq p$. Pelo primeiro Teorema de Sylow como $q \big| |G|$, então existe $y \in G$ tal que $Ord(y) = q$, mas por hipótese todo elemento de G é potência de p, isto é, existe $r \in \mathbb{N}$ tal que $Ord(y) = y^r$. Portanto, $q = p^r \Rightarrow p \big| q$ e como p e q são primos, então $p = q$, absurdo. Logo, $b = 1$ e $|G| = p^m$, desta forma, G é um p-grupo. ■

Vejamos alguns exemplos de p-grupos.

Exemplo 4.8. $\frac{\mathbb{Z}}{4\mathbb{Z}}$ é um p-grupo de ordem $4 = 2^2$.

Exemplo 4.9. $\frac{\mathbb{Z}}{8\mathbb{Z}}$ é um p-grupo de ordem $8 = 2^3$.

Exemplo 4.10. $\frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{2\mathbb{Z}}$ é um p-grupo de ordem $8 = 2^3$.

Exemplo 4.11. $\frac{\mathbb{Z}}{9\mathbb{Z}}$ é um p-grupo de ordem $9 = 3^2$.

Agora, vamos examinar o segundo Teorema de Sylow, que enfatiza algumas características dos p-subgrupos.

Teorema 4.12 (Segundo Teorema de Sylow). Sejam G um grupo finito, p um número primo e n_p o número de p-subgrupos de Sylow de G. Então:

(a) Todos os p-subgrupos de Sylow de G são conjugados entre si.

(b) Se P é um p-subgrupo de G, existe um p-grupo de Sylow S de G tal que $P \subseteq S$.

(c) Se S é um p-subgrupo de Sylow, temos $n_p = (G : N_G(S))$.

Antes de iniciar a demostração do teorema, demostraremos o seguinte lema:

Lema 4.2. Sejam G um grupo finito e p um número primo. Sejam S p-subgrupo de Sylow de G e P um p-subgrupo qualquer de G. Então

$$P \cap N_G(S) = P \cap S.$$

Demonstração. Sabemos que $S \subseteq N_G(S) \Rightarrow P \cap S \subseteq P \cap N_G(S)$. Suponha por absurdo que $P \cap S \subsetneqq P \cap N_G(S)$. Daí, existe $x \in P \cap N_G(S)$, mas $x \notin P \cap S$. Em particular, $x \notin S$. Como $x \in P$ e P é um p-grupo, então existe $r \in \mathbb{Z}^+$ tal que $Ord(x) = p^r$. Como $x \notin S$, então $r \geqslant 1$. Como $S \trianglelefteq N_G(S)$, então $\langle x \rangle \cdot S$ é um subgrupo de $N_G(S)$. Assim,

$$|\langle x \rangle \cdot S| = \frac{|\langle x \rangle| \cdot |S|}{|\langle x \rangle \cap S|} = p^r \cdot \frac{|S|}{|\langle x \rangle \cap S|}.$$

Por hipótese, $|S| = p^m$, com $m \in \mathbb{N}$ onde $|G| = p^m \cdot b$, $b \in \mathbb{N}$ e $mdc(p,b) = 1$.

Como $\langle x \rangle \cap S$ é um subgrupo de S, então $|\langle x \rangle \cap S| = p^s$, para algum $s \in \mathbb{Z}^+$. Como $x \notin S$, então

$$\langle x \rangle \cap S \subsetneqq \langle x \rangle \Rightarrow |\langle x \rangle \cap S| < |\langle x \rangle| \Rightarrow p^s < p^r \Rightarrow s < r \Rightarrow r - s \in \mathbb{N}.$$

Logo,

$$|\langle x \rangle \cdot S| = |S| \cdot \frac{p^r}{p^s} = p^m \cdot p^{r-s} = p^{m+(r-s)},$$

com $r - s \geqslant 1$. Assim, pelo Teorema de Lagrange 3.5 temos que $p^{m+r-s} \big| |G|$. Então $m + r - s \leqslant m \Rightarrow r - s \leqslant 0$, absurdo!

Portanto, $P \cap S = P \cap N_G(S)$. ■

Agora, veremos a demonstração do segundo Teorema de Sylow.

Demonstração. Sejam S um p-subgrupo de Sylow de G e $C_s = \{gSg^{-1};\ g \in G\}$. Sabemos que $|C_s| = (G : E(S)) = (G : N_G(S))$.

Afirmação: Se P é um p-subgrupo de G, então existe $S' \in C_s$ tal que $P \subseteq S'$.

De fato, observe que se $a \in G$ e $K \in C_s$, então $aKa^{-1} \in C_s$. Logo,

$$\begin{aligned} \mathfrak{I} : P &\longrightarrow Bij(C_s) \\ a &\longmapsto \mathfrak{I}_a : C_s \to C_s \\ &\qquad K \mapsto aKa^{-1}. \end{aligned}$$

É uma representação do grupo P em $Bij(C_s)$. Sejam $\mathcal{O}_{\mathcal{I}}(S_1),...,\mathcal{O}_{\mathcal{I}}(S_t)$ as t órbitas duas a duas distintas da representação $\mathcal{I}$, e sendo t definido como a cardinalidade do conjunto de todas as órbitas de $\mathcal{I}$, isso implica que $S_1,...,S_t \in C_s$. Assim,

$$C_s = \bigcup_{i=1} \mathcal{O}_{\mathcal{I}}(Si) \Rightarrow |C_s| = \sum_{i=1}^{t} |\mathcal{O}_{\mathcal{I}}(Si)| = \sum_{i=1}^{t} (P : E_{\mathcal{I}}(S_i)) = \sum_{i=1}^{t} (P : P \cap N_G(S_i))$$

pelo lema 4.2 anterior temos:

$$\sum_{i=1}^{t} (P : P \cap N_G(S_i)) = \sum_{i=1}^{t} (P : P \cap S_i).$$

Logo,

$$(G : N_G(S)) = \sum_{i=1}^{t} (P : P \cap S_i).$$

Por hipótese $|S| = p^m$, onde $|G| = p^m \cdot b$ e b, $m \in \mathbb{N}$ tais que $mds(p,b) = 1$. Assim, pelo Teorema de Lagrange 3.5:

$$(G : S) = \frac{|G|}{|S|} = \frac{p^m \cdot b}{p^m} = p^{(m-m)} \cdot b = p^0 \cdot b = 1 \cdot b = b \Rightarrow p \nmid (G : S).$$

Como $S \subseteq N_G(S) \subseteq G$, então

$$(G : S) = \underbrace{(G : N_G(S))}_{p\nmid} \cdot \underbrace{(N_G(S) : S)}_{p\nmid} \Rightarrow p \nmid (G : N_G(S)) \Rightarrow p \nmid \sum_{i=1}^{t} (P : P \cap S_i),$$

então existe $j \in \{1,2,...,t\}$ tal que $p \nmid (P : P \cap S_j)$.

Por outro lado, pelo Teorema de Lagrange 3.5:

$$|P| = (P : P \cap S_j) \cdot |p \cap S_j| \Rightarrow (P : P \cap S_j) \big| |P|,$$

então existe $l \in \mathbb{Z}^+$ tal que $(P : P \cap S_j) = p^l$. Como $p \nmid (P : P \cap S_j)$, então $l = 0$. Isso implica que $(P : P \cap S_j) = 1 \Rightarrow P = P \cap S_j \Rightarrow P \subseteq S_j$. Tomando $S' = s_j$. Daí $S' \in C_s$ e $P \subseteq S'$.

Portanto, por essa afirmação o **item (b)** está demonstrado.

(a) Seja K um p-subgrupo de Sylow de G. Em particular, K é um p-subgrupo. Consequentemente pelo **item (b)** existe $S' \in C_s$ tal que $K \subseteq S'$. Como $|K| = P^m = |S'| \Rightarrow K = S' \Rightarrow K \in C_s$.

Logo: $\{p$-subgrupos de Sylow de $G\} = C_s$.

(c) Pelo **item (a)**, temos $\{p$-subgrupos de Sylow de $G\} = \{$conjugados de $S\}$. Assim, segue de imediato que $n_p = |C_s| = (G : N_G(S))$.

■

Agora, apresentaremos um corolário como resultado do segundo Teorema de Sylow.

Corolário 4.4. Sejam G um grupo finito, p um número primo onde $p\big||G|$ e S um p-subgrupo de Sylow de G são equivalentes:

(a) $S \trianglelefteq G$;

(b) S é o único p-subgrupo de Sylow de G;

(c) S é um subgrupo característico de G.

O Terceiro Teorema de Sylow demonstra que o número de p-subgrupos de Sylow de um grupo G é côngruo a 1 módulo p.

Teorema 4.13 (Terceiro Teorema de Sylow). Sejam p um número primo e G um grupo finito de ordem $p^m \cdot b$, com $mdc(p,b) = 1$. Seja n_p o número de p-subgrupos de Sylow de G. Então

$$\begin{cases} n_p \text{ divide } b \\ n_p \equiv 1 \mod p. \end{cases}$$

Demonstração. Tome S um p-subgrupo de Sylow de G. Assim, pelo segundo Teorema de Sylow, $n_p = (G : N_G(S))$. Vimos anteriormente que

$$b = (G : S) = (G : N_G(S)) \cdot (N_G(S) : S) = n_p \cdot (N_G(S) : S)$$

isso implica que $n_p\big|b$. Considere a representação

$$\begin{aligned} \mathcal{I} : S &\longrightarrow Bij(C_s) \\ a &\longmapsto \mathcal{I}_a : C_s \to C_s \\ &\qquad K \mapsto aKa^{-1}. \end{aligned}$$

com órbitas $\mathcal{O}_{\mathcal{I}}(S_1), ..., \mathcal{O}_{\mathcal{I}}(S_t)$ duas a duas, distintas, tais que

$$C_s = \bigcup_{i=1} \mathcal{O}_{\mathcal{I}}(Si),$$

$S_1 = S$ e $S_1, ..., S_t \in C_s$.

Analogamente ao que foi feito na demonstração do segundo Teorema de Sylow tem-se:

$$n_p = (G : N_G(S)) = \sum_{i=1}^{t} (S : S \cap S_i) = (S : S \cap S_i) + \sum_{i=2}^{t} (S : S \cap S_i)$$

sabemos que $S \cap S = S$, assim $(S : S \cap S) = (S : S)$ isso implica que $(S : S = 1)$, pois o índice de qualquer grupo nele mesmo é 1. Logo:

$$(S : S \cap S_i) + \sum_{i=2}^{t} (S : S \cap S_i) = 1 + \sum_{i=2}^{t} (S : S \cap S_i).$$

Afirmação: $p\big|(S : S \cap S_i)$, para todo $i \in \{2, ..., t\}$.

De fato, dado $i \in \{2,...,t\}$,

$$(S : S \cap S_i) \big| |S| \Rightarrow (S : S \cap S_i) \big| p^m \Rightarrow (S : S \cap S_i) = p^l,$$

com $l \in \mathbb{Z}^+$.

Se $l = 0$, então $(S : S \cap S_i) = p^0 = 1 \Rightarrow S = S \cap S_i \Rightarrow S \subseteq S_i$ e como $|S| = p^m = |S_i|$, então $S = S_i \Rightarrow i = 1$, absurdo. Assim, $l \geqslant 1 \Rightarrow p \big| (S : S \cap S_i)$.

Portanto,

$$p \left| \sum_{i=2}^{t} (S : S \cap S_i) \Rightarrow p \right| (n_p - 1) \Rightarrow n_p \equiv 1 \ \ mod p.$$

■

É importante destacar que se não tivermos nenhuma outra informação sobre o grupo G, então, em geral, o terceiro Teorema de Sylow não permite determinar o valor de n_p.

A seguir, veremos uma proposição que decorre do segundo e do terceiro Teorema de Sylow.

Proposição 4.4. Sejam G um grupo finito, p um número primo tal que $p \big| |G|$, S um p-subgrupo de Sylow de G e H um subgrupo de G com $N_G(S) \subseteq H$. Então:

(a) $N_G(H) = H$. Em particular $N_G(N_G(S)) = N_G(S)$;

(b) $(G : H) \equiv 1 \bmod p$.

Demonstração. Ver Garcia e Lequain (2014, p.266). ■

Os Teoremas de Sylow desempenham um papel fundamental na classificação de grupos finitos, além de ser uma ferramenta valiosa para determinar a existência de subgrupos normais em um grupo e elementos de ordem específica. Para concluir este capítulo, na próxima seção, exploraremos algumas aplicações cujas demonstrações dependem principalmente dos Teoremas de Sylow.

4.4 Aplicações dos Teoremas de Sylow

Nesta seção, p e q representam números primos. Além disso, um grupo G é denominado simples se não possui nenhum subgrupo normal não trivial, ou seja, além dos subgrupos $\{e\}$ e G. Essa definição é importante para entender duas das aplicações.

4.4.1 Grupos de ordem pq

Sejam G um grupo de ordem pq tal que $p \nmid q - 1$. Então, G é cíclico.

Consideremos o número de p-Sylow, denotado por n_p, que satisfaz $n_p = pk + 1 \mid q$. Isso implica que n_p é igual a 1 ou q. O segundo caso é descartado, pois resultaria em $p \mid q - 1$. Assim, há apenas um p-Sylow H, o qual é normal em G.

Analogamente, ao examinar o número de q-Sylow, denotado por n_q, onde $n_q = ql+1 \mid p$, e considerando que $q > p$, concluímos que n_q só pode ser 1. Portanto, há apenas um q-Sylow K, também normal em G.

Dado que p e q são primos, H e K são cíclicos, o que significa que existem elementos a e b em G tais que $H = \langle a \rangle$ e $K = \langle b \rangle$. Devido à normalidade de H e K em G, temos que $aba^{-1} \in K$ e $ba^{-1}b^{-1} \in H$, o que implica que $aba^{-1}b^{-1} \in K \cap H$.

Pelo Teorema de Lagrange (3.5),

$$|K \cap H| \big| |K| = q \text{ e } |K \cap H| \big| |H| = p.$$

Resultando em $|K \cap H| = 1$, uma vez que p e q são primos distintos. Portanto, $K \cap H = \{e\}$, onde e é o elemento neutro de G. Consequentemente, $ab = ba$, e a ordem de ab é $pq = |G|$. Assim, G é gerado por ab e é, portanto, cíclico.

Na subseção subsequente, iremos referir ao conjunto de 3-Sylows do grupo G como $Syl_3(G)$, e em certos momentos, utilizaremos $Syl_2(G)$ para referenciar o conjunto de 2-Sylows do grupo G.

4.4.2 Grupos de ordem p^2q não são simples

Analisaremos três casos.

Caso 1: Se $p = q$, então $|G| = p^3$. Nesse caso pela equação de conjugação o centro de G não é trivial e sabemos que o centro sempre é um subgrupo normal.

Caso 2: Se $p > q$. Então $n_p = 1$. Logo, o p-Sylow é normal.

Caso 3: Se $q > p$. Então $n_q \in \{1, p, p^2\}$. No primeiro caso o q-Sylow é normal. O segundo caso é impossível, pois $q > p$. Se $n_q = p^2$, então

$$q|p^2 - 1 = (p-1)(p+1) \Rightarrow q|p-1 \text{ ou } q|p+1 \overset{q>p}{\Longrightarrow} q = p+1.$$

Portanto $p = 2$ e $q = 3$, e $|G| = 12$. Nesse caso, mostraremos que G possui um 3-Sylow normal ou $G \cong A_4$, o caso em que possui 2-Sylow normal. Se $n_3 \neq 1$, então $n_3 = [G : N(P)] = 4$, onde $P \in Syl_3(G)$. Então $|N(P)| = 3$ consequentemente $P = N(P)$. A ação de G em $Syl_3(G)$ define um homomorfismo

$$\varphi : G \to S_4$$

cujo núcleo $\ker\varphi := K$ é um subgrupo de $P = N(P)$. Como P não é normal, K é trivial, isto é, φ é injetivo. Então

$$G \cong (G) \leqslant S_4.$$

Ou seja, $\varphi(G)$ é um subgrupo de S_4 com 12 elementos. Observem que G possui $4(3-1) = 8$ elementos de ordem 3. Lembrando que S_4 possui exatamente 8 elementos

de ordem 3, todos em A_4, concluímos que $|\varphi(G) \cap A_4| \geqslant 8$, logo $\varphi(G) = A_4$ e $G \cong A_4$. Seja $V \in Syl2(A_4)$, então $|V| = 4$, logo V contém todos os outros (não de ordem 3) elementos de A_4. Em particular há apenas um 2-Sylow, logo é normal.

Algumas observações desta demonstração:

- A_4 é o grupo das permutações pares de grau 4. Denotamos por A_n o subconjunto de S_n das permutações pares, ou seja, $A_n = \{\alpha \in S_n : \alpha \quad \text{é uma permutação par } \}$.
- S_4 é o grupo das permutações de grau 4.
- $N(P)$ é o normalizador de P em G, ou seja, $N(P)$ pode também ser representado por $N_G(P)$.
- A notação 2-Sylow indica que se trata de um grupo cuja ordem é uma potência de dois, sendo essa ordem precisamente a maior potência de dois encontrada na fatoração do grupo. Da mesma forma, para 3-Sylow.

Para concluir esta seção sobre as aplicações dos Teoremas de Sylow, vamos apresentar uma demonstração de que grupos de ordem 30 não são simples.

4.4.3 Grupos de ordem 30 não são simples

De fato, demonstraremos que um grupo G de ordem 30 contém um subgrupo de 15 elementos, com índice 2, e, consequentemente, é normal. Sejam S_1 pertencente ao conjunto de 5-Sylow do grupo G e S_2 pertencente ao conjunto de 3-Sylow do grupo G. Se pelo menos um deles for normal, então o produto $S_1 \cdot S_2$ forma um subgrupo de ordem 15. Caso contrário, de acordo com o Terceiro Teorema de Sylow 4.13, temos $n_5 = 6$ e $n_3 = 10$. Isso implica que G possui $6(5-1) = 24$ elementos de ordem 5 e $10(3-1) = 20$ elementos de ordem 3. No entanto, isso levaria a $|G| = 30 > 24 + 20 = 44$, uma contradição. Portanto, concluímos que G possui 5-Sylow ou 3-Sylow normal, o que implica na existência do subgrupo de 15 elementos.

Assim, finalizamos este capítulo, onde apresentamos duas das mais importantes recíprocas parciais do Teorema de Lagrange, bem como aplicações dos Teoremas de Sylow em algumas classificações de grupos, conforme objetivo deste trabalho.

Capítulo 5

Conclusão e Perspectivas

Neste trabalho, realizamos um estudo sobre as Recíprocas do Teorema de Lagrange. Este Teorema diz que sendo G um grupo finito e H um subgrupo de G, então a ordem de H divide a ordem de G. Naturalmente, podemos questionar se a recíproca desse teorema é verdadeira, isto é, dado um grupo finito G de ordem n, um inteiro positivo d que divide a ordem de G, existe um subgrupo H em G com ordem d?

Certamente, é verdade para grupos abelianos e grupos cíclicos. Se $G = \langle g \rangle$ tiver ordem n e d for um divisor de n, então a ordem de $g^{\frac{n}{d}}$ é d, e portanto, $H = \langle g^{\frac{n}{d}} \rangle$ é um subgrupo de ordem d. No entanto, em geral, a resposta é negativa, como é o caso do grupo das permutações pares A_4, que possui ordem igual a 12, porém não possui nenhum subgrupo de ordem 6.

Com esse propósito, o enfoque principal deste trabalho foi a apresentação de resultados que fornecessem respostas parciais à pergunta acima. Os três Teoremas de Sylow, especialmente o primeiro Teorema de Sylow, e o Teorema de Cauchy proporcionam respostas para essa indagação. Além disso, há outros resultados que garantem a recíproca do Teorema de Lagrange, envolvendo P-Grupos, Grupos Nilpotentes e Grupos Solúveis. Neste trabalho, contudo, concentramos exclusivamente nos três Teoremas de Sylow e no Teorema de Cauchy. Ficando os demais casos como possibilidade de estudo futuramente.

O Teorema de Cauchy estipula que dado um grupo abeliano finito G e um número primo p que divide a ordem de G, então existe um elemento $x \in G$ com ordem p. Usando a observação de que a ordem de x é igual à ordem do subgrupo gerado por x ($Ord(x) = |\langle x \rangle|$), chegamos a essa conclusão. Por outro lado, o primeiro Teorema de Sylow estabelece que, se p é um número primo e G é um grupo de ordem $p^m \cdot b$ com $mdc(p,b) = 1$, então para cada inteiro n no intervalo de $0 \leq n \leq m$, existe um subgrupo H de G com ordem p^n. Isso implica que em grupos finitos que atendem às condições do teorema, existem subgrupos cuja ordem é um divisor da ordem de G.

Além disso, podemos observar que ao longo deste trabalho, avançamos progressivamente na classificação de grupos abelianos finitos com ordens de p, p^2, pq e p^2q. Existem, entretanto, outros cenários a serem explorados. Sugerimos, portanto, que futuros trabalhos se concentrem na classificação desses casos adicionais. Também é importante enfatizar que durante o seu

desenvolvimento, notamos que o estudo das recíprocas do Teorema de Lagrange requer conhecimento de tópicos abordados no curso, especialmente na disciplina de Estruturas Algébricas. O que ressalta a sua relevância, visto que muitos desses conteúdos não são apresentados devido à falta de tempo.

A experiência ao explorar esse tema enriqueceu consideravelmente minha formação acadêmica. Este trabalho, além de sua relevância intrínseca, tem a finalidade de servir como um recurso valioso para estudantes interessados no assunto. Espera-se que este trabalho possa ser utilizado como referência de estudo sobre o tema e, igualmente, como fundamento para a realização de futuras pesquisas na área. Diante disso, busca-se não apenas contribuir com o conhecimento já existente, mas também inspirar e facilitar o desenvolvimento de estudos adicionais nesse campo de estudo.

Referências

DOMINGUES, H. H. *Fundamentos de aritmética*. São Paulo: Atual, 1981.

FILHO, E. de A. *Teoria elementar dos números*. [S.l.]: Nobel, 1981.

FILHO, E. de A. *Teoria dos Grupos*. [S.l.]: São Paulo: Edgard Blücher, 1985.

FRALEIGH, J. B.; LOPEZ, M. et al. Algebra abstracta: primer curso. Masachusetts: Addison-Wesley Iberoamericana, 1988.

GARCIA, A.; LEQUAIN, Y. *Elementos de álgebra*. 1. ed. Rio de Janeiro: Instituto de Matemática Pura e Aplicada, 2014.

GIL, A. C. Como elaborar projetos de pesquisa. são paulo: Atlas, 1993. gil, antônio carlos. *Como elaborar projetos de pesquisa. São Paulo: Atlas*, 2002.

GONÇALVES, A. *Introdução à álgebra*. [S.l.]: Projeto Euclides/Instituto de Matemática Pura e Aplicada, 1999.

HERNSTEIN, I. N. *Tópicos de Álgebra*. USA: Blaisdell, 1964.

IEZZI, G.; DOMINGUES, H. *Álgebra moderna: teoría y problemas*. [S.l.]: Saraiva Educação SA, 1970.

MINAYO, M. d. S. O desafio da pesquisa social. in. minayo, mc de s.(org.); deslandes; sf; gomes, r. *Pesquisa social: Teoria, método e criatividade. Petrópolis, RJ: Vozes*, 2001.

ROBINSON, D. J. *A Course in the Theory of Groups*. 2. ed. USA: Springer, 1996.

ROTMAN, J. J. *An Introduction to the Theory of Groups*. 4. ed. USA: Springer, 1934.

SALEHYAN, P. Teorema de sylow e aplicaçõs. 2010.

SANCHEZ, D. F. Joseph louis lagrange e o desenvolvimento da mecânica clássica. 2007.

SILVA, M. A. et al. Grupos finitos. 2002.

SOUZA, J. A. Uma nota sobre a teoria dos grupos: da teoria de galois à teoria de gauge. *Revista Brasileira de História da Matemática*, v. 12, n. 24, p. 71–81, 2012.

VIEIRA, V. L. Álgebra abstrata para licenciatura, 1ª edição. *Campina Grande-PB, EDUEPB*, 2013.

YARTEY, J. N. A. *Álgebra II*. Salvador - Bahia: UFBA, 2017.