UNIVERSIDADE ESTADUAL DA PARAÍBA
CAMPUS VII – GOVERNADOR ANTÔNIO MARIZ
CENTRO DE CIÊNCIAS EXATAS E SOCIAIS APLICADAS
CURSO DE LICENCIATURA PLENA EM MATEMÁTICA

GUSTAVO DOS SANTOS AZEVEDO OLIVEIRA

OS TEOREMAS DE SYLOW E APLICAÇÕES

PATOS
2022

GUSTAVO DOS SANTOS AZEVEDO OLIVEIRA

OS TEOREMAS DE SYLOW E APLICAÇÕES

Trabalho de Conclusão de Curso (Monografia) apresentado ao Curso de Licenciatura Plena em Matemática do Centro de Ciências Exatas e Sociais Aplicadas da Universidade Estadual da Paraíba, como requisito parcial para a obtenção do título de Licenciado em Matemática.

Área de concentração: Matemática

Orientador: Prof. Drª Kelyane Barboza de Abreu

PATOS
2022

O48t Oliveira, Gustavo dos Santos Azevedo.
Os Teoremas de Sylow e Aplicações [manuscrito] / Gustavo dos Santos Azevedo Oliveira. - 2022.
49 p.

Digitado.
Trabalho de Conclusão de Curso (Graduação em Matemática) - Universidade Estadual da Paraíba, Centro de Ciências Exatas e Sociais Aplicadas , 2022.
"Orientação : Profa. Dra. Kelyane Barboza de Abreu , Departamento de Matemática - CCT."

1. Ensino da Matemática. 2. Teorema de Lagrange. 3. Teoremas de Sylow. 4. Grupos. I. Título

21. ed. CDD 372.7

Elaborada por Edson M. Almeida - CRB - CRB 15/743 BSC 7

GUSTAVO DOS SANTOS AZEVEDO OLIVEIRA

OS TEOREMAS DE SYLOW E APLICAÇÕES

Trabalho de Conclusão de Curso, na modalidade Monografia, apresentado ao Curso de Licenciatura Plena em Matemática – CCEA – UEPB, como requisito parcial para obtenção do título de Licenciado em Matemática.

Área de concentração: Matemática

Aprovado em: 06.04.2022

BANCA EXAMINADORA

Prof. Drª Kelyane Barboza de Abreu (Orientadora)
Universidade Estadual da Paraíba (UEPB)

Prof. Dr. Arlandson Matheus Silva Oliveira
Universidade Estadual da Paraíba (UEPB)

Prof. Drª Josefa Genyle do Nascimento Santana
Universidade Estadual da Paraíba (UEPB)

AGRADECIMENTOS

Agradeço primeiramente a Deus, por tudo que ele me concede mesmo não sendo digno de tanto. A toda a minha família que foi minha base em todos os momentos e em especial minha mãe Maria Geane e a minha irmã Elizabete Neta.

A minha orientadora Kelyane Barboza, pelas horas dedicadas e por todo apoio. Ao primeiro contato já sabia que seria minha orientadora. A senhorita é sensacional.

Aos colegas de sala, por todo apoio e incentivo durante a minha graduação. Vocês foram essenciais nessa conquista.

Por fim, agradeço a todos os meus professores por todos os conhecimentos passados.

"A sabedoria é um paradoxo. O homem que mais sabe é aquele que mais reconhece a vastidão da sua ignorância."

(Friedrich Nietzsche)

RESUMO

Seja G um grupo. Definimos a ordem de G como sendo o número de elementos que ele possui e representamos por $|G|$. Quando essa ordem é finita, segue do Teorema de Lagrange que se H é um subgrupo de G, então $|H|$ divide $|G|$. Por outro lado, os Teoremas de Sylow nos propõe um caminho inverso. Consideramos um grupo G de ordem finita. A partir da sua ordem podemos determinar e classificar os seus subgrupos. Sabendo da grande importância dos Teoremas de Sylow dentro da teoria de grupos, o presente trabalho tem como objetivo apresentá-los e demonstrá-los. Para alcançarmos o nosso objetivo, destacamos alguns conceitos e resultos básicos da teoria de grupos e em seguida, introduzimos a teoria de representação de um grupo de permutações. Por fim, enuciamos e demonstramos os teoremas base do nosso trabalho. Além disso, concluímos com alguns exemplos e aplicações desses resultados.

Palavras-Chave: Grupos. Teorema de Lagrange. Teoremas de Sylow.

ABSTRACT

Let G be a group. We define the order of G as the number of elements it has and represent it by $|G|$. When this order is finite, it follows from Lagrange's Theorem that if H is a subgroup of G, then $|H|$ divides $|G|$. On the other hand, Sylow's Theorems propose an inverse path . We consider a group G of finite order. From their order we can determine and classify their subgroups. Knowing the great importance of Sylow's Theorems within the theory of groups, the present work aims to present and demonstrate them. To achieve our goal, we highlight some basic concepts and results of group theory and then introduce the theory of representation of a group of permutations. Finally, we enunciate and prove the base theorems of our work. Furthermore, we conclude with some examples and applications of these results.

Keywords: Groups. Lagrange's Theorem. Sylow's Theorems.

SUMÁRIO

1 Introdução

Dentro da Matemática Moderna, a Teoria de Grupos é sem dúvidas, um de seus pilares. Sua aplicabilidade passeia por diversas áreas, e não somente da Matemática. Podemos destacar, inclusive, aplicações em física e química, como na teoria quântica de campos, nas estruturas atômica e molecular, na cristalografia, dentre outros. Além disso, podemos citar sua enorme contribuição na criptografia - na decodificação de dados computacionais.

Foi o matemático francês Évariste Galois (1811-1832), o primeiro a estudar a ideia de grupo, quando em seus trabalhos em torno das equações polinomiais, ele estudou a solubilidade dessas equações por radicais. Segundo Boyer [2], ele mostrou que uma equação polinomial pode se relacionar com um dado grupo finito, em que a solubilidade de uma equação polinomial por radical está sujeita ao fato do grupo a qual é relativo é solúvel ou não. Galois tentou inúmeras vezes submeter seus artigos a respeito de suas descobertas sobre os grupos, mas eles eram sempre recusados. Somente quando Liouville (1809 - 1882) teve acesso ao seu trabalho, em 1846, alguns anos após seu falecimento, sua obra foi reconhecida e publicada. Hoje, suas contribuições são tidas como uma das mais importantes para a Álgebra Abstrata.

No decorrer dos séculos muitos outros matemáticos foram se destacando e contribuindo para a Teoria de Grupos. Podemos citar alguns nomes importantes como o noruêgues Niels Henrik Abel (1802 - 1829), Augustin-Louis Cauchy (1789 - 1857), Arthur Cayley (1821 - 1895), o britânico Georg Frobenius (1848 - 1917), Henri Poincaré (1854 - 1912) e outros que foram fundamentais para o seu desenvolvimento. Inclusive, o matemático Arthur Cayley foi o primeiro a definir grupos por meio de leis. É dele a famosa frase: "Um grupo é definido por meio de leis que combinam seus elementos". De acordo com Quaresma, (2009, p.27 apud Aleksandrov, Kolmogorov e Laurentiev) “a teoria dos grupos nasceu da necessidade de encontrar-se um método para se estudar propriedades importantes do mundo real, como por exemplo, a simetria”. No entanto, o estudo de grupos só tomou lugar de evidência quando surgiram os primeiros resultados sobre grupos infinitos, classificação de grupos finitos e representações de grupos. Aqui, destacamos o matemático Peter Ludwig Mejdell Sylow, que desenvolveu os resultados base para o nosso trabalho.

Dado um grupo finito G e um subgrupo H, segue como corolário do Teorema de Lagrange que a ordem de H divide a ordem de G. Mas será que vale a recíproca do Teorema de Lagrange? Considere um grupo finito G de ordem n e seja k um divisor de n. Existem subgrupos de G de ordem k? A resposta nem sempre é afirmativa, por exemplo se considerarmos o grupo alternado A_4 de ordem 12, ele não possui subgrupo de ordem 6. Os Teoremas de Sylow são os que mais se aproximam de uma recíproca para o Teorema de Lagrange. Além disso, eles são resultados importantíssimos no estudo da classificação de grupos finitos. Nesse sentido, o nosso trabalho tem como objetivo apresentar esses brilhantes Teoremas e a partir deles classificar alguns grupos de ordem finita. Ele está dividido da seguinte forma: No primeiro capítulo, fazemos um passeio pelas definições e resultados básicos da estrutura de grupos. No capítulo

dois dissertamos sobre as representações de grupos via permutação, em seguida apresentamos e demonstramos os Teoremas de Sylow e por fim, aplicamos os resultados em alguns grupos de ordem finita. Nosso trabalho teve como base livros clássicos da teoria de grupos, a citar [3], [4].

2 Teoria básica de grupos

Neste capítulo, algumas definições, teoremas, exemplos e resultados que servirão de base para o nosso principal objetivo, os Teoremas de Sylow, no qual exibiremos no segundo capítulo. Tal Teoria adveio do trabalho do matemático Évariste Galois (1811-1832) e recebeu influências de diversos matemáticos. Para uma leitura mais aprofundada sobre os assuntos apresentados neste capítulo, pode-se consultar os livros [3] e [4].

2.1 Relação de equivalência e relação de congruência

Nesta seção, definiremos duas importantes relações que irão nos acompanhar ao longo do nosso trabalho.

Definição 2.1. (Relação de equivalência) Seja A um conjunto não vazio e $\mathfrak{R}$ uma relação. Dizemos que $\mathfrak{R} \subset A \times A$ é uma relação de equivalência em A se as propriedades a seguir são satisfeitas para quaisquer $a, b, c \in A$:

(i) $a \,\mathfrak{R}\, a$

(ii) Se $a \,\mathfrak{R}\, b$ então $b \,\mathfrak{R}\, a$

(iii) Se $a \,\mathfrak{R}\, b$ e $b \,\mathfrak{R}\, c$ então $a \,\mathfrak{R}\, c$

As propriedades (i), (ii) e (iii) são chamadas, respectivamente, de reflexiva, simétrica e transitiva.

Usaremos a notação $\sim$ ao invés de $\mathfrak{R}$, para representar uma relação de equivalência.

Exemplo 2.1. A relação de paralelismo definida para as retas de um espaço A euclidiano é uma relação de equivalência. De fato, dadas às retas x, y, z de A, tem-se:

(i) $x \parallel x$

(ii) $x \parallel y \Rightarrow y \parallel x$

(iii) $x \parallel y,\ y \parallel z \Rightarrow x \parallel z$

Definição 2.2. (Classe de equivalência) Seja A um conjunto não vazio e $\sim$ uma relação de equivalência em A. Considere o elemento $x \in A$. É chamado classe de equivalência de x o conjunto dos elementos de A que estão relacionados com x. Deste modo, a classe de equivalência de $x \in A$ é o subconjunto de A estabelecido por $\overline{x} = \{y \in A \mid y \sim x\}$.

Observação 2.1. Visto que $\sim$ é uma relação de equivalência em A tem-se que $x \sim x$, assim $x \in A$ e $x \in \overline{x}$. Logo $\overline{x}$ não pode ser um conjunto vazio.

Proposição 2.1. Seja $\sim$ uma relação de equivalência em um conjunto A não vazio. Tem-se:

(i) $\overline{x} = \overline{y} \Leftrightarrow x \sim y;\ \forall x, y \in A$

(ii) $\overline{x} \neq \overline{y} \Rightarrow \overline{x} \cap \overline{y} = \varnothing;\ \forall x, y \in A$

(iii) $\bigcup_{x \in A} \overline{x} = A;\ \forall\ x \in A$

Demonstração. (i) ($\Rightarrow$): Sejam $x, y \in A$ e $\overline{x} = \overline{y}$. Vamos provar que $x \sim y$. Se $\overline{x} = \overline{y}$, então dado $x \in \overline{x}$, temos que $x \in \overline{y}$. Disto, segue que $x \sim y$.

($\Leftarrow$): Sejam $x, y \in A$ e $x \sim y$. Vamos provar que $\overline{x} = \overline{y}$ e para isso temos que provar que $\overline{x} \subset \overline{y}$ e $\overline{y} \subset \overline{x}$.

Primeiramente vamos provar que $\overline{x} \subset \overline{y}$.

Seja $z \in \overline{x}$. Logo $z \sim x$. Como $x \sim y$, a propriedade transitiva nos garante que $z \sim y$ e portanto $z \in \overline{y}$. Logo, $\overline{x} \subset \overline{y}$. Agora, se $x \sim y$ temos por simetria que $y \sim x$ e de maneira análoga a anterior chegamos à inclusão $\overline{y} \subset \overline{x}$ o que implica $\overline{x} = \overline{y}$.

(ii) Suponhamos $x, y \in A$ e $\overline{x} \neq \overline{y}$. Se existisse algum elemento $z \in \overline{x} \cap \overline{y}$ teríamos $z \sim x$ e $z \sim y$ e, usando a simetria, seguiria $x \sim z$ e $y \sim z$ e pela transitividade teríamos $x \sim y$ e pelo item (i) dessa proposição $\overline{x} = \overline{y}$ o que contraria a nossa hipótese, assim $\overline{x} \cap \overline{y} = \varnothing$.

(iii) Inicialmente temos que $\overline{x} \subset A,\ \forall\ x \in A$. Logo, $\bigcup_{x \in A} \subset A$. Agora, se $x \in A$. Como, $\sim$ é uma relação de equivalência em A, então pela propriedade reflexiva temos que $x \sim x$, isto é, $x \in \overline{x}$. Sabendo que, $\overline{x} \subset \bigcup_{x \in A} \overline{x}$, tem-se que $x \in \bigcup_{x \in A} \overline{x}$ e, com isso, $A \subset \bigcup_{x \in A} \overline{x} = A$.

□

A relação a seguir é de grande relevância para a Teoria dos Números.

Definição 2.3. (Relação de congruência módulo n) Uma relação de equivalência em $\mathbb{Z}$ é definida do seguinte modo: $x, y \in \mathbb{Z},\ x \sim y \Leftrightarrow x - y$ é um múltiplo inteiro de n. Assim, temos que $x - y = nk,\ k \in \mathbb{Z}$. Essa relação é indicada por $\equiv mod\ n$ e é definida por $x \equiv y\ mod\ n$.

Definição 2.4. (Conjunto quociente) Seja $\sim$ uma relação de equivalência em um conjunto A não vazio. Chama-se de conjunto quociente de A pela relação de equivalência $\sim$ o conjunto formado por todas as classes de equivalência dos elementos de A, denotado por

$$A / \sim\ = \{\overline{x} \mid x \in A\}.$$

2.2 Grupos e Subgrupos

Na presente seção estudaremos os grupos, que são estruturas algébricas dotadas de apenas uma operação. Além disso, trataremos de conceitos importantes para o nosso trabalho. Dentre eles, podemos destacar os subgrupos, grupos cíclicos e a ordem de um grupo e de um elemento.

Definição 2.5. (Grupo) Seja G um conjunto não vazio munido por uma operação

$$\cdot : G \times G \longrightarrow G$$

$$(a, b) \longmapsto a \cdot b$$

Dizemos que $(G, \cdot)$ é um grupo se as condições abaixo são satisfeitas para quaisquer que sejam $a, b, c \in G$

(i) A operação é associativa, ou seja,

$$a \cdot (b \cdot c) = (a \cdot b) \cdot c$$

(ii) Existe um elemento neutro, ou seja,

$$\exists \ e \in G \ \text{ tal que } \ e \cdot a = a \cdot e = a$$

(iii) Existe elemento inverso para todo elemento de G, ou seja,

$$\forall \ a \in G, \ \exists \ b \in G \ \text{ tal que } \ a \cdot b = b \cdot a = e$$

Além disso, o grupo é abeliano (ou comutativo) se:

(iv) A operação $\cdot$ é comutativa, ou seja,

$$a \cdot b = b \cdot a$$

Importante lembrar que nem todos os grupos são abelianos. Mais adiante veremos um exemplo de um grupo multiplicativo não abeliano. Além disso, com a finalidade de simplificar as notações, muitas vezes deixaremos de indicar a operação do grupo, escrevendo G para denotar um grupo $(G, \cdot)$. Também, quando não existir ambiguidade, escreveremos ab no lugar de $a \cdot b$.

Observação 2.2. (i) Seja $(G, \cdot)$ um grupo. O elemento neutro de G é único. De fato, se $e, e' \in G$ são elementos neutros de G, então

$$e = e \cdot e' \ \text{ pois } \ e' \ \text{ é elemento neutro,}$$

$$= e' \ \text{ pois } \ e \ \text{ é elemento neutro.}$$

(ii) O elemento inverso é único. De fato, seja $a \in G$, e sejam $b, b' \in G$ dois elementos inversos de a; temos

$$b = b \cdot e = b \cdot (a \cdot b') \text{ pois } b' \text{ é inverso de } a,$$

$$= (b \cdot a) \cdot b' = e \cdot b' = b' \text{ pois } b \text{ é inverso de } a.$$

Denotaremos o único elemento inverso de a por a^{-1}.

(iii) Da unicidade do inverso de um elemento $a \in G$, obtém-se o fato mais geral seguinte: Se $a, b \in G$, então a equação $X \cdot a = b$ tem uma única solução em G, a saber $b \cdot a^{-1}$. Por outro lado, a equação $a \cdot X = b$ do mesmo modo tem uma única solução em G, a saber $a^{-1} \cdot b$.

(iv) Em decorrência da observação anterior, para mostrar que um elemento $f \in G$ é igual ao elemento neutro do grupo, basta mostrar que $f \cdot a = a$ para algum elemento $a \in G$.

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

Exemplo 2.2. O conjunto dos números inteiros $\mathbb{Z}$ munido da operação de soma usual é um grupo abeliano. Em notação $(\mathbb{Z}, +)$. Com efeito, dados $a, b, c \in \mathbb{Z}$, temos que:

(i) $(a + b) + c = a + (b + c)$;

(ii) Existe $0 \in \mathbb{Z}$, tal que $a + 0 = 0 + a = a$;

(iii) Para todo $a \in \mathbb{Z}$, com $a \neq 0$, existe $(-a) \in \mathbb{Z}$ tal que $a + (-a) = -a + a = 0$;

(iv) $a + b = b + a$.

Analogamente, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$ são grupos abelianos aditivos.

Exemplo 2.3. O conjunto dos números racionais sem o zero $\mathbb{Q} - \{0\}$ munido da operação multiplicação usual é um grupo abeliano. De fato, para quaisquer $x, y, z \in \mathbb{Q} - \{0\}$, temos que:

(i) $(x \cdot y) \cdot z = x \cdot (y \cdot z)$;

(ii) Existe $1 \in \mathbb{Q} - \{0\}$, tal que $x \cdot 1 = 1 \cdot x = x$;

(iii) Para todo $z \in \mathbb{Q} - \{0\}$, com $z \neq 1$, existe $z^{-1} \in \mathbb{Q} - \{0\}$, tal que $z \cdot z^{-1} = z^{-1} \cdot z = 1$.

Analogamente, $(\mathbb{R} - \{0\}, \cdot)$, $(\mathbb{C} - \{0\}, \cdot)$ são grupos abelianos multiplicativos.

Exemplo 2.4. O conjunto $GL_n(\mathbb{R}) = \{A \in M_n(\mathbb{R}) \mid det(A) \neq 0\}$ munido da operação de multiplicação usual constitui um grupo.

(i) $A(BC) = (AB)C$, $\forall\ A, B, C \in GL_n(\mathbb{R})$

(ii) Existe $I_n \in GL_n(\mathbb{R})$, tal que $AI_n = I_nA = A$, $\forall A \in GL_n(\mathbb{R})$;

(iii) Toda matriz $A \in GL_n(\mathbb{R})$ possui um inverso A^{-1}, pois toda matriz quadrada que possui determinante diferente de zero é inversível. Assim, $AA^{-1} = A^{-1}A = I_n$

Logo, $GL_n(\mathbb{R})$ é um grupo chamado de grupo linear de grau n sobre $\mathbb{R}$. Além disso, podemos verificar que ele não é comutativo.

Exemplo 2.5. O conjunto $(S^1, \cdot)$ definido como $S^1 = \{z \in \mathbb{C} \mid |z| = 1\}$ munido da multiplicação complexa, é um grupo multiplicativo.

Exemplo 2.6. O conjunto A_n é um grupo e iremos defini-lo assim

$$A_n = \{\alpha \in S_n \mid \alpha \text{ é par}\},$$

o conjunto das permutações pares de S_n. A_n é denominado de grupo alternado de grau n.

Definição 2.6. (Subgrupos) Sejam $(G, \cdot)$ um grupo e H um subonjunto não vazio de G. Diz-se que H é um subgrupo de G (notação: $H \leq G$) se H for um grupo munido da operação $\cdot$ do grupo G, ou seja, quando satisfaz as condições a seguir:

(i) $h_1 \cdot h_2 \in H$, $\forall\ h_1, h_2 \in H$

(ii) $h_1 \cdot (h_2 \cdot h_3) = (h_1 \cdot h_2) \cdot h_3$, $\forall\ h_1, h_2, h_3 \in H$

(iii) $\exists\ e_H \in H$ tal que $e_H \cdot h = h \cdot e_H = h$, $\forall\ h \in H$.

(iv) Para cada $h \in H$, existe $k \in H$ tal que $h \cdot k = k \cdot h = e_H$.

Observação 2.3. 1) A condição (ii) é sempre satisfeita, pois a igualdade $g_1 \cdot (g_2 \cdot g_3) = (g_1 \cdot g_2) \cdot g_3$ é válida para todos os elementos de G.

2) O elemento neutro e_H de H é necessariamente igual ao elemento neutro e de G. De fato, tomando $a \in H \subseteq G$, temos $e_H \cdot a = a$; multiplicando os dois lados por a^{-1} à direita, obtemos $e_H = e$.

3) Dado $h \in H$, o inverso de h em H é necessariamente igual ao inverso de h em G. De fato, se k é o inverso de h em H, então $h \cdot k = k \cdot h = e_H$, logo $h \cdot k = k \cdot h = e$ pois $e_H = e$, e portanto k é o inverso de h em G.

Proposição 2.2. Seja H um subconjunto não vazio do grupo G. Diremos que H é um subgrupo de G se, e somente se, são satisfeitas as seguintes condições:

(i) $h_1 \cdot h_2 \in H$, $\forall\ h_1, h_2 \in H$.

(ii) $h^{-1} \in H$, $\forall \in H$.

Demonstração. Suponhamos que H seja um subgrupo de G. Só precisamos verificar que $h^{-1} \in H$, $\forall \in H$. Mas isso é verdade uma vez que, pela observação anterior, o inverso de todo $h \in H$ coincide com o inverso de $h \in G$, ou seja, é necessariamente igual a h^{-1}, logo $h^{-1} \in H$. Reciprocamente, note que $e_H \in H$. Dado $h \in H$, já temos $h^{-1} \in H$ e portanto pela condição (i), $e_H = hh^{-1} \in H$. Além disso, a condição de que para cada $h \in H$, existe $k \in H$ tal que $h \cdot k = k \cdot h = e_H$ segue direto da condição (ii). □

Exemplo 2.7. Se G é um grupo, então $\{e\}$ e G são subgrupos de G, denominados subgrupos triviais de G.

Exemplo 2.8. O conjunto de todos os números pares $(2\mathbb{Z}, +)$ munido da adição usual dos inteiros, é um subgrupo de $(\mathbb{Z}, +)$.

Exemplo 2.9. O conjunto $H = \{\overline{0}, \overline{3}, \overline{6}, \overline{9}, \overline{12}\}$ é um subgrupo de $G = (\mathbb{Z}_{15}, +)$.

Exemplo 2.10. O Grupo Linear Especial $SL_n(\mathbb{R}) = \{M \in GL_n(\mathbb{R}) \mid det(M) = 1\}$ é um subgrupo do grupo $GL_n(\mathbb{R})$.

Definição 2.7. (Subgrupo próprio) Sejam G um grupo e H um subconjunto não vazio de G. Diz-se que H é um subgrupo próprio ou não trivial de G se H é um subgrupo de G em que $H \neq G$ e $H \neq \{e\}$.

Definição 2.8. (**Centro de um grupo**) Seja G um grupo. Chamamos de centro de G o subconjunto definido por

$$Z(G) = \{x \in G \mid xg = gx, \ \forall \ g \in G\}.$$

Ele será denotado por $Z(G)$.

Proposição 2.3. Se G é um grupo, então $Z(G)$ é um subgrupo de G.

Demonstração. (i) Sejam $x, y \in Z(G)$. Para todo $g \in G$ temos:

$$(xy)g = x(yg) = x(gy) = (xg)y = (gx)y = g(xy).$$

Logo,

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

(ii) Se $x \in Z(G)$, então $x^{-1} \in Z(G)$. Isto porque, para todo $g \in G$ temos

$$x^{-1}g = x^{-1}ge = x^{-1}(gx)x^{-1} = x^{-1}(xg)x^{-1} = egx^{-1} = gx^{-1}.$$

Portanto, $Z(G)$ é um subgrupo de G.

□

Observação 2.4. G é um grupo abeliano se e somente se $Z(G) = G$.

Definição 2.9. (Subgrupo gerado por um subconjunto) Dado um subconjunto não vazio S de um grupo G, o conjunto $\{a_1a_2...a_n;\ n \in \mathbb{N}, a_i \in S \text{ ou } a_i \in S^{-1}\}$ será denotado por $\langle S\rangle$. Provaremos adiante que ele é um subgrupo de G chamado de subgrupo gerado pelo subconjunto S. Quando o conjunto é finito, digamos $S = \{\alpha_1, \alpha_2, ...\alpha_r\}$, empregaremos a notação $\langle \alpha_1, \alpha_2, ...\alpha_r\rangle$ para designar $\langle\{\alpha_1, \alpha_2, ...\alpha_r\}\rangle$.

Veja que se $g \in G$, então $\langle g\rangle = \{..., (g^{-1})^2, g^{-1}, e, g, g^2, ...\}$; com frequência, quando $r \in \mathbb{N}$, escrevemos g^{-r} para denotar o elemento $(g^{-1})^r$; assim, com estas notações, temos $\langle g\rangle = \{g^t \mid t \in \mathbb{Z}\}$.

Proposição 2.4. Sejam G um grupo e S um subconjunto não vazio de G. Então o conjunto $\langle S\rangle$ é um subgrupo de G.

Demonstração. É necessário provar:

(i) $\forall x, y \in \langle S\rangle$, temos $xy \in \langle S\rangle$.

(ii) $\forall x \in \langle S\rangle$, temos $x^{-1} \in \langle S\rangle$.

Sejam $x, y \in \langle S\rangle$. Temos

$$x = a_1a_2...a_n, \text{ com } a_i \in S \text{ ou } a_i \in S^{-1}, \forall\ i$$

$$y = b_1b_2...b_m, \text{ com } b_j \in S \text{ ou } b_j \in S^{-1}, \forall\ j.$$

Logo, $xy = a_1a_2...a_nb_1b_2...b_m$ e $x^{-1} = a_n^{-1}a_{n-1}^{-1}...a_2^{-1}a_1^{-1}$ estão também em $\langle S\rangle$. □

Definição 2.10. Sejam G um grupo e S um subconjunto não vazio de G. Então $\langle S\rangle$ é o subgrupo gerado por S.

Observação 2.5. Dado um elemento $g \in G$, temos que para todo $n, m \in \mathbb{Z}$ vale que $g^n \cdot g^m = g^{n+m}$ e $(g^n)^{-1} = g^{-n}$. Essa observação nos permite fazer a seguinte definição.

Definição 2.11. (Grupo cíclico) Um grupo G é denominado cíclico quando ele pode ser gerado por um elemento, ou seja, se existir $g \in G$ tal que $G = \langle g\rangle$.

Exemplo 2.11. $(\mathbb{Z}, +)$ é um grupo cíclico gerado por 1, isto é, $\mathbb{Z} = \langle 1\rangle$. De fato, todo número inteiro é multiplo de 1.

Proposição 2.5. Todo grupo cíclico é abeliano.

Demonstração. Seja G um grupo cíclico e $g \in G$, em que $G = \langle g\rangle$. Assim, utilizando $x, y \in G$ temos,

$$x = g^n \text{ e } y = g^m,$$

para $n, m \in \mathbb{Z}$. Deste modo, $x \cdot y = g^n \cdot g^m = g^{n+m} = g^{m+n} = g^m \cdot g^n = y \cdot x$. Logo, se G é grupo cíclico isso implica que G é abeliano. □

Definição 2.12. (Subgrupo dos comutadores) O subgrupo dos comutadores de G é definido por

$$G' := [x, y] := \langle \{xyx^{-1}y^{-1} \mid x, y \in G\} \rangle.$$

Ele será denotado por G'. Note que G é abeliano se e somente se $G' = e$.

Definição 2.13. (Ordem de um grupo) A ordem de um grupo G é definida como sendo o número de elementos em G e é indicada por $|G|$. Se $x \in G$, a ordem de x é a ordem do subgrupo gerado por x; ela será denotada por $o(x)$.

$$o(x) = |\langle x \rangle|$$

Exemplo 2.12. O conjunto $\mathbb{Z}$ é infinito. Assim, $|\mathbb{Z}| = \infty$.

Exemplo 2.13. O conjunto $\mathbb{Z}_n$ possui n elementos. Portanto, $|\mathbb{Z}_n| = n$

Proposição 2.6. Sejam $x \in G$ e $\langle x \rangle$ o subgrupo gerado por x. Então as seguintes condições são equivalentes:

(i) A ordem $|\langle x \rangle|$ é finita.

(ii) Existe $t \geq 1$ tal que $x^t = e$.

Neste caso, denotando por n a ordem de x, temos

$$\{t \geq 0 \mid x^t = e\} = \{0, n, 2n, ...\} \text{ e } \langle x \rangle = \{e, x, ..., x^{n-1}\}.$$

Demonstração. (i) $\Rightarrow$ (ii) Como $\langle x \rangle = \{x^m \mid m \in \mathbb{Z}\}$, e como, por hipótese, o grupo $\langle x \rangle$ é finito, existem $p, q \in \mathbb{Z}$, $p \neq q$ tais que $x^p = x^q$. Sem perda de generalidade, podemos supor que $p > q$. Como $x^p = x^q$, então $x^{p-q} = e$, e portanto existe $t > 0$ tal que $x^t = e$.

(ii) $\Rightarrow$ (i) Consideramos o inteiro $r := \min\{t \geq 1;\ x^t = e\}$. Queremos mostrar que $r = n$. Para isto, basta claramente provar o lema seguinte: □

Lema 2.1. $\langle x \rangle = \{e, x, x^2, ..., x^{r-1}\}$ e os elementos $e, x, x^2, ..., x^{r-1}$ são todos distintos.

Demonstração. Suponhamos que $x^p = x^q$ com $0 \leq p,\ \ q \leq r-1,\ \ p \neq q$; podemos supor $p > q$. Temos $x^{p-q} = e$ com $0 < p - q < r$ e isso contradiz a minimalidade de r. Logo $e, x, x^2, ..., x^{r-1}$ são elementos distintos de G. Para provar que $\langle x \rangle = \{e, x, x^2, ..., x^{r-1}\}$, devemos mostrar que $\forall\ m \in \mathbb{Z},\ x^m = x^\ell$ para algum $0 \leq \ell < r$. Ora, pelo algorítmo de Euclides, existem $q, \ell \in \mathbb{Z}$ tais que $m = qr + \ell$ com $0 \leq \ell < r$, e portanto temos que $x^m = x^{qr+\ell} = (x^r)^q \cdot x^\ell = e^q \cdot x^\ell = x^\ell$. □

2.3 Classes laterais e o Teorema de Lagrange

Vamos apresentar nesta seção o Teorema de Lagrange, o qual é uma das contribuições do matemático italiano Joseph Louis Lagrange (1736-1813) para a teoria dos grupos. O Teorema nos ajuda a identificar se um dado subconjunto de G é um subgrupo do mesmo. A título de exemplo, seja $K = \{\overline{0}, \overline{3}, \overline{6}, \overline{9}\}$ um subconjunto de $G = \mathbb{Z}_{15}$. Conforme o Teorema de Lagrange K não é um subgrupo de G, pois o subconjunto K apresenta ordem 4 e 15 não é divisível por 4. Antes de enunciar o Teorema, vamos definir algumas ferramentas importantes.

Definição 2.14. Seja G um grupo e seja H um subgrupo de G. Sobre G, defina a relação de equivalência $\sim_E$ da maneira seguinte:

$$y \sim_E x \Leftrightarrow \exists \ h \in H \ \text{ tal que } \ y = xh.$$

Proposição 2.7. A relação $\sim_E$ acima é de equivalêcia.

Demonstração. Para quaisquer $x, y, z \in G$, considera-se.

($\sim_E$ **é reflexiva**) Como $y = ye$, onde $e \in H$, então $y \sim_E y$.

($\sim_E$ **é simétrica**) Se $y \sim_E x$. Então, por definição, $\exists\ h \in H$ tal que $y = xh$. Assim, $yh^{-1} = x \Rightarrow x = yh^{-1}$ onde $h^{-1} \in H$. Logo, $x \sim_E y$.

($\sim_E$ **é transitiva**) Se $y \sim_E x$ e $x \sim_E z$, então $\exists\ h, h' \in H$ tais que $y = xh$ e $x = zh'$. Veja que $y = xh = (zh')h = z(h'h)$, onde $h'h \in H$. Logo, $y \sim_E z$.

Portanto, a relação $\sim_E$ é de equivalência. □

Definimos então a classe de x como sendo

$$\overline{x} = \{y \in G \mid y \sim_E x\} = \{xh \mid h \in H\} = xH.$$

Observação 2.6. Chamaremos o conjunto xH de classe lateral à esquerda de H em G que contém x. Quando não houver confusão possível, chamaremos simplesmente esta classe lateral de x à esquerda. Em particular, H é a classe lateral do elemento neutro e à esquerda. Observe que $y \in xH \Leftrightarrow yH = xH$.
Analogamente, poderíamos definir a relação de equivalência seguinte:

$$y \sim_D x \Leftrightarrow \exists \ h \in H; \ \ y = hx.$$

Obteríamos então as classes laterais à direita de H em G; a classe lateral de x à direita seria $Hx = \{hx \mid h \in H\}$.

Definição 2.15. A cardinalidade do conjunto das classes laterias à esquerda é o índice de H em G, ele será denotado por $(G : H)$.

Observação 2.7. O índice de H em G também é a cardinalidade do conjunto das classes laterias à direita de H em G, pois a aplicação φ abaixo é uma bijeção bem definida.

$$\begin{aligned}\varphi: \quad \{\text{classes laterais à esquerda}\} &\longrightarrow \{\text{classes laterias à direita}\}\\ xH &\longmapsto Hx^{-1}.\end{aligned}$$

Proposição 2.8. Sejam G um grupo e H um subgrupo de G. Então:

(i) G é igual a união das classes laterais aH, ou seja,

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

(ii) Duas classes laterais à esquerda (à direita) de H em G são disjuntas ou iguais.

Demonstração. A demonstração segue pela proposição 2.1. □

Observação 2.8. O conjunto de todas as classes laterais à esquerda de H em G forma uma partição de G e será denotado por

$$\frac{G}{H} = \{aH \mid a \in G\}.$$

Proposição 2.9. Todas as classes laterais de H em G têm a mesma cardinalidade, igual à cardinalidade de H.

Demonstração. Primeiramente, definamos a seguinte função

$$\begin{aligned}\varphi: \quad H &\longrightarrow xH\\ h &\longmapsto xh\end{aligned}$$

Note que, para qualquer $y \in xH$, existe $h \in H$ tal que

$$y = xh = \varphi(h),$$

ou seja, $y \in Im(\varphi)$. Logo, $xH \subset Im(\varphi)$. Como, $Im(\varphi) \subset xH$, então $xH = Im(\varphi)$, isto é, a função φ é sobrejetiva.

Agora, se $h, h' \in H$ são tais que $\varphi(h) = \varphi(h')$, temos

$$xh = xh' \Rightarrow h = h'.$$

Assim, φ é injetiva e, consequentemente, bijetiva. Portanto, xH tem a mesma quantidade de elementos de H, isto é,

$$|xH| = |H|. \tag{2.1}$$

Agora, defina

$$\begin{aligned} \varphi: \quad H &\longrightarrow Hx \\ h &\longmapsto hx \end{aligned}$$

Argumentando como anteriormente, segue que φ é sobrejetiva e injetiva. Assim, φ é bijetiva e, consequentemente,

$$|Hx| = |H|. \tag{2.2}$$

Portanto, de 2.1 e 2.2 segue que $|xH| = |Hx|$. □

Teorema 2.1. (Teorema de Lagrange) Sejam G um grupo finito e H um subgrupo de G. Então $|G| = |H|(G : H)$, em particular, a ordem e o índice de H dividem a ordem de G.

Demonstração. Como G é finito, então claramente $(G : H)$ também é finito. Considere $(G : H) = n$, assim

$$(G : H) = \{x_1H, x_2H, ..., x_nH\},$$

onde $x_1, x_2, ..., x_n \in G$, o que pela Proposição 2.8, temos

$$G = x_1H \cup x_2H \cup ... \cup x_nH.$$

Ainda pela Proposição 2.8, as classes laterais x_iH e x_jH são disjuntas se $i \neq j$. Como a união acima é disjunta, temos

$$|G| = |x_1H| + |x_2H| + ... + |x_nH|.$$

.

A proposição anterior mostra que em cada uma dessas classes temos $|H|$ elementos. Assim,

$$|G| = |H| + |H| + ... + |H|$$

.

Como, por definição, o número de classes é $(G : H) = n$, temos

$$|G| = |H|n = |H|(G : H)$$

Portanto, $|G| = |H|(G : H)$. □

Corolário 2.1. Seja G um grupo finito e seja $x \in G$. Então a ordem de x divide a ordem de G.

Demonstração. Considere $n, k \in \mathbb{N}$, tais que $|G| = n$ e $o(x) = k$. Por definição, $o(x) = |\langle x \rangle| = k$. Como $\langle x \rangle$ é subgrupo do grupo finito G, então pelo Teorema de Lagrange

$$|G| = |\langle x\rangle|(G : \langle x\rangle)$$

Assim, $\exists\ r \in \mathbb{N}$ tal que

$$|G| = |\langle x\rangle|r = kr$$

.

Logo, $o(x) = k$ divide $|G|$. Por fim, temos que este corolário equivalentemente diz que

$$x^{|G|} = x^{kr} = (x^k)^r = e^r = e$$

.

Portanto, $x^{|G|} = e$. □

Os dois teoremas que seguem tem uma importância relevante na Teoria dos Números e são corolários do Teorema de Lagrange. Esses resultados também nos ajudam a calcular o resto de divisões entre potências de números muito grandes. Por exemplo, o resto da divisão de 3^{125} por 450.

Corolário 2.2. (Pequeno Teorema de Fermat) Seja p um número primo. Então:

$$a^{p-1} \equiv 1\ mod\ \ p, \forall\ \ a \in \mathbb{Z} \setminus p\mathbb{Z}.$$

Definição 2.16. Seja $n \in \mathbb{N}$. A função de Euler de n é a cardinalidade do conjunto formado pelos números inteiros primos com n entre 1 e $n - 1$. Iremos denotá-la como $\Phi(n)$.

Corolário 2.3. (Teorema de Euler) Sejam x e n dois inteiros relativamente primos. Então

$$x^{\Phi(n)} \equiv 1\ mod\ \ n,$$

onde Φ é a função de Euler.

Corolário 2.4. Seja G é um grupo de ordem prima. Então G é cíclico.

Demonstração. Sejam $|G| = p$, onde $p \in \mathbb{Z}$ é primo, $x \in G$ com $x \neq e$. Pelo Teorema de Lagrange, $|\langle x\rangle|$ divide $|G| = p$. Sendo p um número primo, então $|\langle x\rangle| = 1$ ou $|\langle x\rangle| = p$. Mas, como $x \neq e$, segue que $|\langle x\rangle| = p$, ou seja, $|\langle x\rangle| = |G|$. Portanto, $\langle x\rangle = G$. O que mostra que G é cíclico. □

Proposição 2.10. Seja G um grupo finito. Se H e K são subgrupos de G tais que $K \leq H \leq G$, então

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

Demonstração. Pelo Teorema de Lagrange,

$$H \leq G \Rightarrow |G| = |H|(G : H),$$

$$K \leq H \Rightarrow |H| = |K|(H : K).$$

Dessas duas igualdades, obtemos

$$|G| = |K|(H : K)(G : H) \Rightarrow \frac{|G|}{|K|} = (H : K)(G : H),$$

de modo que,

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

□

Observação 2.9. Se G é um grupo abeliano e se H é um subgrupo de G, então $Hx = xH, \ \forall \ x \in G$.

2.4 Subgrupos Normais e Grupos Quocientes

Sejam G um grupo e H um subgrupo de G. O objetivo dessa seção é dar condições necessárias e suficientes ao subgrupo H para que o conjunto

$$\frac{G}{H}$$

tenha estrutura de grupo.

Uma pergunta natural que podemos fazer é sob quais condições a operação de G induz de maneira natural uma operação sobre o conjunto $\frac{G}{H}$, isto é, que torna a operação

$$(xH, yH) \mapsto xH \cdot yH = xyH$$

bem definida, no sentido de não depender da escolha dos representantes x e y. Tentaremos ao longo da seção responder a essa pergunta.

Definição 2.17. (Subgrupo normal) Sejam G um grupo e H um subgrupo de G. Dizemos que H é um subgrupo normal de G se $ghg^{-1} \in H, \ \forall \ g \in G, \ \forall \ h \in H$.

Observação 2.10. Um subgrupo normal H de G será denotado por

$$H \lhd G.$$

Proposição 2.11. Seja H um subgrupo de um grupo G. As afirmações seguintes são equivalentes:

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

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

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

(iv) $gH = Hg, \ \forall \ g \in G.$

Demonstração. (i) $\Leftrightarrow$ (ii) Por definição.
(ii) $\Rightarrow$ (iii) Suponhamos que $gHg^{-1} \subseteq H, \ \forall \ g \in G$; queremos mostrar que $H \subseteq gHg^{-1}, \forall g \in G$. Sejam então $h \in H$ e $g \in G$; temos

$$h = ehe$$

$$h = (gg^{-1})h(gg^{-1})$$

$$h = g(g^{-1}hg)g^{-1}.$$

Logo, $h = g(g^{-1}hg)g^{-1} \in g(g^{-1}Hg)g^{-1} \subseteq gHg^{-1}$.
(iii) $\Rightarrow$ (iv) Para $g \in G$, seja $x \in gH$, digamos $x = gh$ para algum $h \in H$. Logo, por hipótese,

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

isto é, $xg^{-1} = h_1$, com $h_1 \in H$. Portanto, $x = h_1 g \in Hg$, de modo que $gH \subset Hg$.
Da mesma forma, prova-se que $Hg \subset gH$. Por conseguinte, $Hg = gH$.
(iv) $\Rightarrow$ (i) Sejam $g \in G$ e $h \in H$. Como $gH = Hg$, temos que $gh \in gH = Hg$. Segue que $gh = h'g$ para algum $h' \in H$, ou seja, $ghg^{-1} = h' \in H$. □

Observação 2.11. Se H é um subgrupo normal, então $gH = Hg$. Neste caso, as classes laterais à esquerda de H são iguais às classes laterias à direita de H; vamos chamá-las de classes laterais de H.

Exemplo 2.14. Seja G um grupo. Os subgrupos triviais G e $\{e\}$ são normais em G.

Exemplo 2.15. Seja G um grupo abeliano. Então, os subgrupos de G são todos normais. De fato, sejam $g \in G$ e $h \in H$, temos

$$ghg^{-1} = (gh)g^{-1} = hgg^{-1} = he = h \in H.$$

Exemplo 2.16. O centro $Z(G)$ de um grupo G é normal.

Proposição 2.12. Sejam G um grupo e H um subgrupo. Se $(G : H) = 2$, então $H \lhd G$.

Demonstração. Para mostrar isso, vamos mostrar que $xH = Hx, \ \forall \ x \in G$. Se $x \in H$ então $xH = H = Hx$. Se $x \notin H$ temos

$$xH \neq H \ \text{ e } \ Hx \neq H.$$

Como $(G : H) = 2$, existem exatamente duas classes laterais à esquerda, xH e H. Agora, uma relação de equivalência num espaço decompõe o espaço na união disjunta de suas classes de equivalência; assim $xH = G \setminus H$. Da mesma forma, $Hx = G \setminus H$. Desse modo, $xH = G \setminus H = Hx$. Portanto, $H \lhd G$. □

Proposição 2.13. Sejam G um grupo e H um subgrupo de G. Então H é um subgrupo normal de G se, e somente se, a operação sobre $\frac{G}{H}$ definida por $xH \cdot yH = xyH$ está bem definida para $x, y \in G$.

Demonstração. Considere a igualdade $(xH, yH) = (aH, bH)$ com $x, y, a, b, \in G$, ou seja, $xH = aH$ e $yH = bH$. Se H for um subgrupo normal segue que

$$xyH = x(yH) = x(bH) = x(Hb),$$

$$xyH = (xH)b = (aH)b = (Ha)b = Hab = abH.$$

e isso implica que a operação está bem definida. Reciprocamente, temos que $eH = H = hH$ com $h \in H$. Logo

$$g^{-1}H = eg^{-1}H = (eH) \cdot (g^{-1}H) = hH \cdot (g^{-1}H) = hg^{-1}H.$$

Assim, $hg^{-1} \in g^{-1}H$, ou seja, $ghg^{-1} \in H$. Portanto, $H \lhd G$. □

Corolário 2.5. Seja G um grupo e seja H um subgrupo normal de G. Então o conjunto das classes laterais é um grupo munido com a seguinte operação:

$$\begin{aligned} \cdot : \ & G/H \times G/H \longrightarrow G/H \\ & (xH,\ yH) \longmapsto (xy)H \end{aligned}$$

Demonstração. Consideremos $xH, yH, zH \in G/H$ onde $x, y, z \in G$. Resta verificar que a operação é associativa e que $\frac{G}{H}$ possui elemento neutro e inverso.

(i) Associatividade:

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

(ii) Como G é grupo, G possui elemento neutro e e, evidentemente, $eH = H$. Temos

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

Logo, H é o elemento neutro da operação em G/H.

(iii) Como G é grupo, todo $x \in G$ possui elemento inverso x^{-1}. Temos

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

Desse modo, $x^{-1}H$ é o inverso de xH em G/H.

Portanto, G/H é um grupo.

□

Proposição 2.14. Sejam H e K subgrupos de um grupo G. Se H ou K for normal em G, então KH é um subgrupo de G.

Demonstração. Vamos considerar o caso em que $H \lhd G$ e $K \leq G$; o outro caso é totalmente análogo. Vamos mostrar que $HK = KH$. Dado $x = hk \in HK$, temos

$$x = hk = kk^{-1}hk = k\alpha,$$

com $\alpha = k^{-1}hk \in H$, pois $H \lhd G$. Assim, $x = k\alpha \in KH$, ou seja $HK \subseteq KH$. Para provar a inclusão contrária, basta notar que se $y = kh \in KH$, então

$$y = kh = khk^{-1}k = \beta k,$$

no qual $\beta = khk^{-1} \in H$ pois $H \lhd G$; portanto $y = \beta k \in HK$. □

Definição 2.18. (Grupo Quociente) 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 $\dfrac{G}{H}$.

Proposição 2.15. Sejam G um grupo e G' seu subgrupo dos comutadores. Então,

(i) G/G' é abeliano.

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

Demonstração. (i) Consideremos $xG', yG' \in G/G'$ onde $x, y \in G$.

Como $x^{-1}y^{-1}xy \in G'$ então

$$(x^{-1}y^{-1}xy)G' = G'$$

$$(x^{-1}y^{-1})G' \cdot (xy)G' = G'$$

$$(yx)^{-1}G' \cdot (xy)G' = G'$$

$$(xy)G' = (yx)G'.$$

(ii) Sejam $x, y \in G$. Como G/H é abeliano então

$$xH \cdot yH = yH \cdot xH$$

$$(xy)H = (yx)H$$

$$(xy)H \cdot (yx)^{-1}H = H$$

$$(xy)H \cdot (x^{-1}y^{-1})H = H$$

$$(xyx^{-1}y^{-1})H = H$$

$$[x, y]H = H$$

Assim, $[x, y] \in H$. Portanto, $G' \subseteq H$.

□

Proposição 2.16. Seja G um grupo e seja $Z(G)$ seu centro. Se o quociente $G/Z(G)$ é cíclico, então $Z(G) = G$. Em particular, $(G : Z(G))$ nunca é um número primo.

Demonstração. Seja $\overline{z} \in G/Z(G)$ tal que $G/Z(G) = \langle \overline{z} \rangle$. Então, $\forall\ g \in G, \exists\ i$ tal que $\overline{g} = \overline{z}^i$, logo tal que $g = z^i h$ 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 , $Z(G) = G$. □

2.5 Homomorfismo de Grupos

Nesta seção estudaremos as funções entre grupos que preservam suas operações. Denominamos essas funções de homomorfismo de grupos. Quando elas são bijetoras, chamamos de isomorfismo. Grupos isomorfos preservam algumas propriedades, e deste modo, é possível obter informações algébricas de um determinado grupo por meio de outro já conhecido.

Definição 2.19. (Homomorfismo) Sejam $(G, *)$ e $(H, \cdot)$ grupos. Chama-se homomorfismo a função $f : G \longrightarrow H$ quando

$$f(x * y) = f(x) \cdot f(y), \forall\ x, y \in G.$$

Observação 2.12. Se $f : G \longrightarrow H$ é um homomorfismo e $x_1, x_2, ..., x_n \in G$, então por indução temos que

$$f(x_1 * x_2 * ... * x_n) = f(x_1) \cdot f(x_2) \cdot ... \cdot f(x_n).$$

Exemplo 2.17. Seja $H \lhd G$, assim $\pi : G \longrightarrow G/H$ definida por $\pi(x) = xH$, é um homomorfismo sobrejetor, chamado de projeção canônica. Visto que para todo $x, y \in G$, então

$$\pi(xy) = xyH = (xH) \cdot (yH) = \pi(x)\pi(y).$$

Exemplo 2.18. Sejam $n \in \mathbb{Z}$ fixo e $\varphi_n : (\mathbb{Z}, +) \longrightarrow (\mathbb{Z}, +)$ definida por $\varphi_n(x) = nx$. Se $x, y \in \mathbb{Z}$, então

$$\varphi_n(x + y) = n \cdot (x + y) = n \cdot x + n \cdot y = \varphi_n(x) + \varphi_n(y),$$

isto é, φ_n é um homomorfismo.

Exemplo 2.19. Sejam os grupos $(\mathbb{R}_+, \cdot)$ e $(\mathbb{R}, +)$. A função

$$\begin{array}{rccc} f: & \mathbb{R}_+ & \longrightarrow & \mathbb{R} \\ & x & \longmapsto & f(x) = log(x) \end{array}$$

deste modo definida é um homomorfismo. De fato, para todo $x, y \in \mathbb{R}_+$, então

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

Proposição 2.17. Seja $f : (G, *) \longrightarrow (H, \cdot)$ um homomorfismo de grupos. Então,

(i) $f(e_G) = e_H$

(ii) $f(x^{-1}) = f(x)^{-1}$

(iii) $kerf := \{x \in G \mid f(x) = e_H\}$ é um subgrupo normal de G chamado núcleo do homomorfismo f.

(iv) $Im(f) := \{y \in H \mid y = f(g)$ para algum $g \in G\}$ é um subgrupo de H, chamado Imagem de f.

(v) f é injetiva $\Leftrightarrow kerf = \{e_G\}$.

(vi) Se $o(x) < \infty$ então $o(f(x))$ divide $o(x)$.

(vii) Se K é um subgrupo de G, então $f(K)$ é um subgrupo de H e $f^{-1}(f(K)) = K(kerf)$.

(viii) Se D é um subgrupo de H, então $f^{-1}(D)$ é um subgrupo de G contendo $kerf$ e temos que $f(f^{-1}(D)) = D \cap Im(f)$.

Demonstração. (i) De fato,

$$f(e_G) = f(e_G * e_G) = f(e_G) \cdot f(e_G).$$

Logo, $f(e_G) = e_H$.

(ii) Para todo $x \in G$, $x * x^{-1} = e_G$. Assim,

$$f(x \cdot x^{-1}) = f(e_G) = e_H \text{ pelo item anterior,}$$

ou seja,

$$f(x) \cdot f(x^{-1}) = e_H \Rightarrow f(x^{-1}) = f(x)^{-1}.$$

(iii) Inicialmente veremos que $kerf \leq G$. Dados $x, y \in kerf$, temos:

$$f(x * y) = f(x) \cdot f(y) = e_H \cdot e_H = e_H,$$

$$f(x^{-1}) = f(x)^{-1} = e_H^{-1} = e_H;$$

desse modo $kerf \leq G$. Para provar que $kerf \lhd G$ devemos mostrar que:

$$gxg^{-1} \in ker\ f, \forall\ g \in G \text{ e } \forall\ x \in ker\ f.$$

De fato, temos

$$f(gxg^{-1}) = f(g) \cdot f(x) \cdot f(g^{-1}) = f(g) \cdot e_H \cdot f(g)^{-1} = f(g) \cdot f(g)^{-1} = e_H.$$

Portanto, $kerf$ é subgrupo normal de G.

(iv) Sendo $f(e_G) = e_H$, segue que $e_H \in Im(f)$. Agora, dados $x, y \in Im(f)$, existem $a, b \in G$ tais que $f(a) = x$ e $f(b) = y$. Assim,

$$f(a * b) = f(a) \cdot f(b) = x \cdot y \in Im(f).$$

Por fim, dado $y \in Im(f)$, existe $x \in G$ tal que $f(x) = y$. Note que

$$y \cdot f(x^{-1}) = f(x) \cdot f(x^{-1}) = f(x * x^{-1}) = f(e_G) = e_H$$

$$f(x^{-1}) \cdot y = f(x^{-1}) \cdot f(x) = f(x^{-1} * x) = f(e_G) = e_H$$

Logo $y^{-1} = (f(x))^{-1} = f(x^{-1}) \in Im(f)$.

(v) ($\Rightarrow$) $\{e_G\} \subseteq kerf$. Reciprocamente, seja $x \in kerf$ temos,

$$f(x) = e_H = f(e_G)$$

e como f é injetora então $x = e_G$. Portanto, $kerf = \{e_G\}$.

($\Leftarrow$) Sejam $x, y \in G$ tais que $f(x) = f(y)$. Temos que

$$f(x) \cdot (f(y))^{-1} = e_H$$

$$f(x) \cdot f(y^{-1}) = e_H$$

$$f(x * y^{-1}) = e_H$$

$$x * y^{-1} \in kerf = \{e_G\}$$

$$x * y^{-1} = e_G \Rightarrow x = y.$$

Logo, f é injetiva.

(vi) Seja $n = o(x)$. Temos $x^n = e_G$, logo

$$e_H = f(e_G) = f(x^n) = (f(x))^n$$

e portanto

$$o(f(x)) \mid n \Rightarrow o(f(x)) \mid o(x).$$

(vii) Vamos assumir que $f(K)$ é um subgrupo de H. Agora, iremos provar que $f^{-1}(f(K)) = K(kerf)$. Queremos provar primeiramente que $K(kerf) \subseteq f^{-1}(f(K))$. Dado $x \in K(kerf)$, existem $a \in K$ e $b \in kerf$ tais que $x = ab$. Logo

$$f(x) = f(a * b) = f(a) \cdot f(b) = f(a) \cdot e_H = f(a) \in f(K).$$

Assim, $x \in f^{-1}(f(K))$. Agora, provaremos a inclusão contrária. Seja $x \in f^{-1}(f(K))$, por definição temos que $f(x) \in f(K)$ e existe $y \in K$ tal que

$$f(x) = f(y) \Rightarrow f(y^{-1} * x) = e_H.$$

Tomemos $w = y^{-1} \cdot x \in kerf$. Assim, $x = y \cdot w \in K(kerf)$.

(viii) Assumiremos que $f^{-1}(D)$ é um subgrupo de G contendo $kerf$. Verifiquemos a igualdade $f(f^{-1}(D)) = D \cap Im(f)$. Como $f(f^{-1}(D)) \subseteq D$ e $f(f^{-1}(D)) \subseteq Im(f)$, então $f(f^{-1}(D)) \subseteq D \cap Im(f)$. Nos resta agora provar a inclusão oposta. Seja $y \in D \cap Im(f)$; existe $z \in G$ tal que $y = f(z)$, pois $y \in Im(f)$. Como $f(z) = y \in D$, então $z \in f^{-1}(D)$ e assim $y = f(z) \in f(f^{-1}(D))$.

□

Observação 2.13. Quando $f : G \longrightarrow H$ é um homomorfismo sobrejetor temos

$$f(f^{-1}(D)) = D.$$

Definição 2.20. (Isomorfismo) Seja $f : G \longrightarrow H$ um homomorfismo. Dizemos que f é um isomorfismo se existir um homomorfismo $g : H \longrightarrow G$ tal que $f \circ g = id_H$ e $g \circ f = id_G$. Iremos denotar $G \simeq H$.

Proposição 2.18. Seja $f : (G, *) \longrightarrow (H, \cdot)$ um homomorfismo de grupos. Então, f é um isomorfismo se e somente se f é uma bijeção.

Demonstração. ($\Rightarrow$) trivial.

($\Leftarrow$) Para provar isto, mostraremos que se f é um homomorfismo bijetivo, então f^{-1} é um homomorfismo, isto é,

$$f^{-1}(\alpha \cdot \beta) = f^{-1}(\alpha) * f^{-1}(\beta), \forall\ \alpha, \beta \in H.$$

Sejam então $\alpha, \beta \in H$, e sejam $a = f^{-1}(\alpha)$ e $b = f^{-1}(\beta)$; temos

$$f^{-1}(\alpha \cdot \beta) = f^{-1}(f(a) \cdot f(b)) = f^{-1}(f(a * b)) = a * b = f^{-1}(\alpha) * f^{-1}(\beta).$$

□

Observação 2.14. Dado $f : G \longrightarrow H$ um homomorfismo injetivo de grupos temos que

$$o(f(x)) = o(x),\ \forall\ x \in G$$

Teorema 2.2. (Teorema do isomorfismo) Seja $f : (G, *) \longrightarrow (H, \cdot)$ um homomorfismo de grupos. Então,

i) A função induzida

$$\overline{f} : \frac{G}{ker f} \longrightarrow f(G)$$
$$g(ker f) \longrightarrow f(g)$$

é um isomorfismo.

ii) As seguintes funções

$$\begin{array}{rcl} \{\text{subgrupos de } G \text{ que contêm } ker\ f\} & \longleftrightarrow & \{\text{subgrupos de } f(G)\} \\ K & \longmapsto & f(K) \\ f^{-1}(D) & \longleftarrow\!\shortmid & D, \end{array}$$

são bijeções, inversas uma da outra. Além disso, estas bijeções levam subgrupos normais, isto é:

a) $K \lhd G \Rightarrow f(K) \lhd f(G)$.

b) $D \lhd f(G) \Rightarrow f^{-1}(D) \lhd G$.

Demonstração. i) Primeiramente, devemos verificar que $\overline{f}$ é uma função bem definida, isto é, se $g(kerf) = \widetilde{g}(kerf)$ então temos $f(g) = f(\widetilde{g})$. Mas, $g(kerf) = \widetilde{g}(kerf)$ implica que $g = \widetilde{g} * k$, para algum $k \in kerf$ e, portanto,

$$f(g) = f(\widetilde{g} * k) = f(\widetilde{g}) \cdot f(k) = f(\widetilde{g}) \cdot e_H = f(\widetilde{g}).$$

Agora, $\overline{f}$ é claramente uma função sobrejetora e, para $g, g' \in G$, obtemos

$$\overline{f}(g(kerf) * g'(kerf)) = \overline{f}((gg')kerf) = f(g * g')$$

$$= f(g) \cdot f(g') = \overline{f}(g(kerf)) \cdot \overline{f}(g'(kerf));$$

assim $\overline{f}$ é um homomorfismo. Agora,

$$ker\overline{f} = \{g(kerf) \mid f(g) = e_H\} = \{g(kerf) \mid g \in kerf\} = kerf;$$

assim $ker\overline{f} = \{e_{G/kerf}\}$ ou seja, a função $\overline{f}$ é injetiva.

ii) Pela proposição 2.15. sabemos que $f^{-1}(f(K)) = K(kerf), \ \forall \ K \leq G$, e além disso $f(f^{-1}(D)) = D \cap f(G), \ \forall \ D \leq H$. Daí, se $kerf \subseteq K$ então $f^{-1}(f(K)) = K$, e se $D \subseteq f(G)$ então $f(f^{-1}(D)) = D$. Portanto, as funções são uma inversa da outra. Nos resta provar que essas funções levam subgrupos normais em subgrupos normais.

a) Sejam $y \in f(G)$ e $x \in f(K)$, queremos mostrar que $yxy^{-1} \in f(K)$. Existem $g \in G$ e $k \in K$ tais que $y = f(g)$ e $x = f(k)$. Como $K \lhd G$ então $gkg^{-1} \in K$. Logo,

$$yxy^{-1} = f(g) \cdot f(k) \cdot (f(g))^{-1} = f(g \cdot k \cdot g^{-1}) \in f(K).$$

b) Sejam $g \in G$ e $x \in f^{-1}(D)$. Queremos mostrar que $gxg^{-1} \in f^{-1}(D)$. Daí, $f(g) \in f(G)$ e $f(x) \in D$, como $D \lhd f(G)$ então

$$f(g) \cdot f(x) \cdot (f(g))^{-1} \in D \Rightarrow f(gxg^{-1}) \in D$$

e portanto temos que $gxg^{-1} \in f^{-1}(D)$.

□

Corolário 2.6. Seja $H \lhd G$. Então a função

$$\begin{array}{ccc} \{\text{subgrupos (normais) de } G \text{ que contêm } H\} & \longleftrightarrow & \{\text{subgrupos (normais) de } \dfrac{G}{H}\} \\ K & \longmapsto & K/H \end{array}$$

é uma bijeção.

Demonstração. Considere o homomorfismo φ abaixo,

$$\begin{array}{rccc} \varphi: & G & \longrightarrow & \dfrac{G}{H} \\ & g & \longmapsto & gH \end{array}$$

Notoriamente, φ é um homomorfismo sobrejetor e $ker\varphi = H$. Utilizando a parte (ii) do teorema dos isomorfismos no homomorfismo φ, obtemos o corolário. □

Corolário 2.7. Sejam $H \lhd G$ e $K \leq G$. Então,

$$\frac{K}{H \cap K} \simeq \frac{KH}{H}.$$

Demonstração. Já que $H \lhd G$, sabemos que KH é um subgrupo de G e que $HK = KH$. Claramente, $H \lhd G \Rightarrow H \lhd KH$ e, portanto, faz sentido considerar o grupo quociente KH/H. Considere o homomorfismo canônico $\varphi : KH \longrightarrow KH/H$ e seja $\varphi|_K$ a sua restrição ao subgrupo $K \leq KH$, isto é:

$$\begin{array}{rccc} \varphi|_K: & K & \longrightarrow & \dfrac{KH}{H} \\ & k & \longmapsto & kH. \end{array}$$

Claramente, $ker(\varphi|_K) = \{k \in K \mid kH = H\} = H \cap K$. Seja agora $\alpha \in KH/H$; temos $\alpha = (kh)H$ para algum $k \in K$ e algum $h \in H$; logo

$$\alpha = (kh)H = (kH) \cdot (hH) = (kH) \cdot (eH) = kH = \varphi|_K(k)$$

e portanto $\varphi|_K$ é sobrejetor. Aplicando agora a parte $1)$ do teorema dos isomorfismo ao homomorfismo $\varphi|_K$, obtemos o corolário. □

Corolário 2.8. Sejam $K \leq H \leq G$ com $K \lhd G$ e $H \lhd G$. Então,

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

Demonstração. Considere o homomorfismo

$$\begin{aligned} \psi : \quad \frac{G}{K} &\longrightarrow \frac{G}{H} \\ gK &\longmapsto gH. \end{aligned}$$

A função ψ é bem definida; de fato $gK = \widetilde{g}K$ implica que $g = \widetilde{g}k$ para algum $k \in K$, e portanto vemos que $gH = \widetilde{g}kH = \widetilde{g}H$ pois temos $k \in K \subseteq H$. Claramente, ψ é sobrejetor e $ker\ \psi = H/K$. Pela parte $1)$ do teorema dos isomorfismos,

$$\frac{G/K}{H/K} = \frac{G/K}{Ker\ \psi} \simeq Im(\psi) = \frac{G}{H},$$

como queríamos demonstrar. □

Definição 2.21. (Automorfismo) Seja G um grupo. Um isomorfismo $f : G \longrightarrow G$ é chamado de automorfismo. O conjunto dos automorfismos de G será denotado por $Aut(G)$. É fácil verificar que a composição de dois automorfismos de G é um automorfismo de G e que $(Aut(G), \circ)$ é um grupo, onde "$\circ$" denota a operação composição de funções.

Proposição 2.19. Sejam G um grupo e $g \in G$. Então a função

$$\begin{aligned} I_g : \quad G &\longrightarrow G \\ x &\longmapsto gxg^{-1} \end{aligned}$$

é um automorfismo de G, chamado automorfismo interno. O conjunto dos automorfismo internos de G será denotado por $I(G)$; assim

$$I(G) := \{I_g \mid g \in G\} \subseteq Aut(G).$$

Proposição 2.20. Seja G um grupo.

(i) Se $g_1, g_2 \in G$ então $I_{g_1} \circ I_{g_2} = I_{g_1 g_2}$.

(ii) $I_e = id_G$.

(iii) Se $g \in G$ então $(I_g)^{-1} = I_{g^{-1}}$.

Demonstração. (i) Seja $x \in G$. Note que

$$I_{g_1} \circ I_{g_2}(x) = I_{g_1}(g_2 x g_2^{-1}) = g_1(g_2 x g_2^{-1})g_1^{-1}$$

$$= (g_1 g_2)x(g_1 g_2)^{-1} = I_{g_1 g_2}(x).$$

(ii) Para todo $x \in G$, temos

$$I_e(x) = exe^{-1} = exe = x = id_G(x).$$

Assim,

$$I_e = id_G.$$

(iii) Pelo item (i) temos

$$I_g \circ I_{g^{-1}} = I_{gg^{-1}} = I_e.$$

Logo, $(I_g)^{-1} = I_{g^{-1}}$.

□

Proposição 2.21. $(I(G), \circ)$ é um subgrupo normal de $(Aut(G), \circ)$.

Demonstração. Segue da proposição anterior que $I(G)$ é um subgrupo de $Aut(G)$. Agora, iremos mostrar que $I(G) \lhd (Aut(G), \circ)$, isto é, dados $\sigma \in Aut(G)$ e $g \in G$ quaisquer, temos $\sigma \circ I_g \circ \sigma^{-1} \in I(G)$. Para todo $x \in G$, temos:

$$\sigma \circ I_g \circ \sigma^{-1}(x) = \sigma \circ I_g(\sigma^{-1}(x)) = \sigma(g\sigma^{-1}(x)g^{-1})$$

$$= \sigma(g)x\sigma(g)^{-1} = I_{\sigma(g)}(x);$$

assim, $\sigma \circ I_g \circ \sigma^{-1} = I_{\sigma(g)} \in I(G)$. □

Definição 2.22. Dados H subgrupo de G e $\sigma \in Aut(G)$. Pode-se dizer que H é estável por σ se $\sigma(H) \subseteq H$.

Observação 2.15. Sejam G um grupo e H um subgrupo de G. Então,

1) Um elemento $g \in G$ comuta com todos os elementos de G se e só se $I_g = id$. Logo, o grupo G será abeliano se e somente se $I(G) = \{id\}$.

2) $H \lhd G \Leftrightarrow I_g(H) \subseteq H, \ \forall \ g \in G$.

3 Os teoremas de Sylow

A recíproca do Teorema de Lagrange nem sempre é válida. Por exemplo, se considerarmos o grupo alternado A_4 de ordem 12. Ele não possui subgrupo de ordem 6, embora 6 seja um divisor de 12. O resultado mais geral que se aproxima de uma recíproca para o Teorema de Lagrange são os Teoremas de Sylow. Desse modo, apresentaremos neste capítulo os Teoremas de Sylow, suas demonstrações e aplicações. A primeira seção deste capítulo será dedicada a representações de grupos por permutação, uma vez que alguns resultados apresentados serão de grande importância para a continuidade do nosso trabalho. Os livros [3] e [4] serviram de base para o desenvolvimento deste capítulo.

3.1 Representação de um Grupo por Permutações

Lembremos que um grupo de permutação de um dado conjunto C é o conjunto de todas as bijeções de C em C munido com a operação binária de composição de funções, ou seja, $P(C) = \{f : C \to C \mid f \text{ é bijetora}\}$.

Definição 3.1. Sejam G um grupo, C um conjunto e $P(C)$ o grupo de permutações de C. Uma *representação* de G no grupo de permutações de C é um homomorfismo ρ de G em $P(C)$, i.e.

$$\rho(g_1 g_2) = \rho(g_1) \circ \rho(g_2),$$

para cada $g_1, g_2 \in G$.

Observação 3.1. Utilizaremos o símbolo G_0 para designar o conjunto G, evitando assim conflitos de entendimento com o grupo G.

Exemplo 3.1. Sejam G um grupo e G_0 um conjunto. Veja que $I : G \longrightarrow P(G_0)$ definida da seguinte forma

$$\begin{aligned} I: \ & G \longrightarrow P(G_0) \\ & g \longmapsto I_g : \quad G_0 \to G_0 \\ & \qquad\qquad\ \ x \mapsto gxg^{-1} \end{aligned}$$

é uma representação de G em $P(G_0)$. De fato, como I_g é um homomorfismo, dados $g_1, g_2 \in G$, temos que $I(g_1 g_2) = I_{g_1 g_2} = I_{g_1} \circ I_{g_2} = I(g_1) \circ I(g_2)$, ou seja, I é um homomorfismo.

Exemplo 3.2. Sejam G um grupo e H um subgrupo normal de G. Considere a aplicação

$$\begin{aligned} I: \ & G \longrightarrow P(H_0) \\ & g \longmapsto I_g : \quad H_0 \to H_0 \\ & \qquad\qquad\ \ h \mapsto ghg^{-1}. \end{aligned}$$

Sabe-se que I é um homomorfismo, assim esta aplicação é uma representação de G no grupo das permutações do conjunto $H_0 = H$.

Exemplo 3.3. Seja G um grupo e seja G_0 um conjunto. Temos que

$$\begin{aligned} T: \ G &\longrightarrow P(G_0) \\ g \longmapsto T_g: \quad & G_0 \to G_0 \\ & x \mapsto gx \end{aligned}$$

é um homomorfismo. Visto que para todo $g_1, g_2 \in G$ e $x \in G_0$, temos

$$T_{g_1 g_2}(x) = (g_1 g_2)x = g_1(g_2 x) = T_{g_1}(T_{g_2} x) = T_{g_1} \circ T_{g_2}(x);$$

assim

$$T_{g_1 g_2} = T_{g_1} \circ T_{g_2}.$$

Portanto, será também uma representação de G em $P(G_0)$.

Exemplo 3.4. Sejam G um grupo e seja C o conjunto formado pelos subgrupos de G. Considere a aplicação

$$\begin{aligned} I: \ G &\longrightarrow P(C) \\ g \longmapsto I_g: \quad & C \to C \\ & H \mapsto gHg^{-1}. \end{aligned}$$

Para todo $g \in G$ podemos ver que a função dada é uma permutação de C e que a aplicação I é um homomorfismo. Portanto, a aplicação acima é uma representação de G em $P(C)$.

Definição 3.2. Sejam G um grupo, C um conjunto e $\rho : G \to P(C)$ uma representação de G. Podemos definir uma relação de equivalência sobre o conjunto C da seguinte forma

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

Definição 3.3. (Órbita) A órbita de x, em que $x \in C$, é o conjunto

$$\mathfrak{O}(x) := \{y \in C \mid y \sim x\} = \{\rho(g)(x) \mid g \in G\}.$$

Observação 3.2. Quando $C = \mathfrak{O}(x)$, para algum $x \in C$, dizemos que a representação ρ é transitiva.

Definição 3.4. (Estabilizador) Seja $x \in C$. O estabilizador de x, denotado por $E(x)$, é o conjunto

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

Observação 3.3. O estabilizador $E(x)$ é um subgrupo de G.

O teorema que segue é de extrema importância, uma vez que ele nos possibilidade calcular a ordem da classe de conjugação de x a partir do índice do seu centralizador.

Teorema 3.1. (Órbita-estabilizador) Sejam $\rho : G \to P(C)$ uma representação do grupo G no grupo de permutações do conjunto C e $x \in C$. Logo, a aplicação ψ a seguir é uma bijeção.

$$\begin{aligned} \psi : \quad \mathfrak{O}(x) \quad &\longrightarrow \{\text{Classes laterais à esquerda de } E(x) \text{ em } G\} \\ \rho(g)(x) \quad &\longmapsto gE(x). \end{aligned}$$

Demonstração. Primeiramente, vamos verificar se a aplicação ψ está bem definida. De fato, dados $g_1, g_2 \in G$ tais que $\rho(g_1)(x) = \rho(g_2)(x)$; aplicando $\rho(g_2^{-1})$ em ambos os lados e como ρ é um homomorfismo, conseguimos obter $\rho(g_2^{-1}g_1)(x) = x$. Assim, temos $g_2^{-1}g_1 \in E(x)$, logo $g_1 \in g_2E(x)$ e $g_1E(x) = g_2E(x)$.

Agora, vamos verificar que ψ é injetiva. Sejam $y_1 = \rho(g_1)(x)$ e $y_2 = \rho(g_2)(x)$ elementos de $\mathfrak{O}(x)$ tais que $\psi(y_1) = \psi(y_2)$, ou seja, tais que $g_1E(x) = g_2E(x)$. Assim, temos que $g_1^{-1}g_2 \in E(x)$, logo $\rho(g_1^{-1}g_2)(x) = x$, ou seja, $\rho(g_1^{-1}) \circ \rho(g_2)(x) = x$ e, portanto,

$$y_2 = \rho(g_2)(x) = \rho(g_1) \circ \rho(g_1^{-1}) \circ \rho(g_2)(x) = \rho(g_1)(x) = y_1.$$

Por fim, ψ é sobrejetora pois, se $gE(x)$ é uma classe lateral à esquerda de $E(x)$ em G, logo temos que $gE(x) = \psi(y)$ com $y = \rho(g)(x)$. □

Observação 3.4. Em decorrência do teorema anterior, se G é um grupo finito segue que:

a) $|\mathfrak{O}(x)| = (G : E(x))$

b) $|\mathfrak{O}(x)|$ divide $|G|$.

Vamos voltar aos exemplos do início do capítulo, agora destacando a órbita e o estabilizador referente a cada representação dada.

Exemplo 3.5. Sejam G um grupo e G_0 um conjunto. Considere

$$\begin{aligned} I : \quad G &\longrightarrow P(G_0) \\ g \longmapsto I_g : \quad &G_0 \to G_0 \\ &x \mapsto gxg^{-1}. \end{aligned}$$

Para cada $x \in G_0$, obtemos

1) A órbita $\mathfrak{O}(x) = \{I_g(x) \mid g \in G\} = \{gxg^{-1} \mid g \in G\}$ de um elemento x nesta representação por conjugação se chama *a classe de conjugação de* x, e é denotado da seguinte forma $Cl(x)$. Os elementos de $Cl(x)$ se chamam *os conjugados de* x *em* G. Observe que temos $Cl(x) = \{x\} \Leftrightarrow gxg^{-1} = x, \ \forall \ g \in G \Leftrightarrow x \in Z(G)$.

2) O estabilizador $E(x) = \{g \in G \mid I_g(x) = x\} = \{g \in G \mid gxg^{-1} = x\} = \{g \in G \mid gx = xg\}$ de um elemento x nesta representação por conjugação se chama *o centralizador de* x, e é denotado da seguinte forma $Z(x)$.

Pela observação 3.4 a ordem da classe de conjungação de x é exatamente o índice do centralizador de x. Ou seja,

$$|Cl(x)| = \#\{\text{conjugados de } \ x \ \text{ em } \ G\} = (G : Z(x)).$$

Naturalmente, G_0 é igual à união, disjunta, das classes de conjugação. Escolhendo um representante x_α, em cada classe de conjugação, temos que $|G| = \sum_\alpha |Cl(x_\alpha)|$, e portanto,

$$|G| = |Z(G)| + \sum_{x_\alpha \notin Z(G)} |Cl(x_\alpha)|.$$

A igualdade acima se chama a **equação das classes de conjugação**.

Segue da equação das classes de conjugação os seguintes resultados.

Proposição 3.1. Sejam p um número primo e G um grupo de ordem p^n com $n \geq 1$. Portanto, $Z(G)$ tem no mínimo p elementos.

Demonstração. Temos $|G| = |Z(G)| + \sum_{x_\alpha \notin Z(G)} |Cl(x_\alpha)|$. Para $x_\alpha \notin Z(G)$, temos

$$|Cl(x_\alpha)| > 1.$$

Pelo Teorema de Lagrange sabemos que

$$(G : Cl(x_\alpha)) \mid |G| \Rightarrow |Cl(x_\alpha)| \mid |G| \Rightarrow |Cl(x_\alpha)| \mid p^n.$$

Logo, $|Cl(x_\alpha)|$ é um múltiplo de p. Deste modo,

$$p \mid |Cl(x_\alpha)| \Rightarrow p \mid (\sum_{x_\alpha \notin Z(G)} |Cl(x_\alpha)|).$$

Como

$$p \mid |G| \Rightarrow p \mid (|G| - \sum_{x_\alpha \notin Z(G)} |Cl(x_\alpha)|) \Rightarrow p \mid |Z(G)|.$$

De outra forma, já que o elemento neutro pertence a $Z(G)$, temos $|Z(G)| \neq 0$. Portanto, o centro $Z(G)$ tem pelo menos p elementos. □

Proposição 3.2. Dado p um número primo. Desse modo todo grupo G de ordem p^2 é abeliano.

Demonstração. Pela proposição anterior, temos $|Z(G)| = p$ ou p^2; por outro lado, sabemos pela Proposição 2.15 que o índice do centro no grupo nunca pode ser um número primo. Logo,

$$|Z(G)| = p^2 = |G| \Rightarrow Z(G) = G$$

e isso implica que G é abeliano. □

Exemplo 3.6. Sejam G um grupo e C o conjunto formado pelos subgrupos de G. Considere a aplicação a seguir

$$\begin{aligned} I: \ G &\longrightarrow P(C) \\ g \longmapsto I_g: \quad & C \to C \\ & H \mapsto gHg^{-1}. \end{aligned}$$

1) A órbita $\mathfrak{O}(H) = \{I_g(H) \mid g \in G\} = \{gHg^{-1} \mid g \in G\}$ de um subgrupo H chama-se *a classe de conjugação de* H, e seus elementos chamam-se *os subgrupos conjugados de* H. Veja que temos $\mathfrak{O}(H) = \{H\} \Leftrightarrow H \lhd G$.

2) O estabilizador $E(H) = \{g \in G \mid I_g(H) = H\} = \{g \in G \mid gHg^{-1} = H\}$ chama-se *o normalizador de* H *em* G, e será denotado por $N_G(H)$.

Pela observação 3.4, a cardinalidade do conjunto dos conjugados de H em G é exatamente o índice do normalizador de H em G. Ou seja,

$$\#\{\text{conjugados de } \ H \ \text{ em } \ G\} = (G : N_G(H)).$$

Proposição 3.3. Seja H um subgrupo de G. Desse modo,

a) $H \lhd N_G(H)$.

b) $N_G(H)$ é o maior subgrupo de G em que H é normal.

c) $H \lhd G \Leftrightarrow N_G(H) = G$.

Demonstração. a) Dados $g \in N_G(H)$ e $h \in H$. Logo, $gHg^{-1} = H$. Como $h \in H$ então

$$ghg^{-1} \in gHg^{-1} = H \Rightarrow ghg^{-1} \in H.$$

Consequentemente, $H \lhd N_G(H)$.

b) Para provar isto, mostraremos que seja Q um subgrupo de G e $H \lhd Q$, então $Q \subseteq N_G(H)$. Seja $q \in Q$. Como $H \lhd Q$ então

$$qHq^{-1} = H \Rightarrow q \in N_G(H).$$

Portanto, $Q \subseteq N_G(H)$.

c) ($\Rightarrow$) Como $H \lhd G$ então pelo item anterior temos $G \subseteq N_G(H)$. Sabemos que $N_G(H) \leq G$, assim, $N_G(H) \subseteq G$. Logo, $N_G(H) = G$.

($\Leftarrow$) Suponhamos que $N_G(H) = G$. Pelo item a) tem-se que

$$H \lhd N_G(H) \Rightarrow H \lhd G.$$

□

Exemplo 3.7. Seja G um grupo. Sejam $K \leq G$ e C o conjunto formado pelos subgrupos de G. Considere

$$\begin{aligned} I: \quad K &\longrightarrow P(C) \\ k &\longmapsto I_k: \quad C \to C \\ & \qquad\quad H \mapsto kHk^{-1}. \end{aligned}$$

1) A aplicação acima é uma restrição para K da representação do Exemplo 3.6.

2) A órbita $\mathfrak{O}(H) = \{I_k(H) \mid k \in K\} = \{kHk^{-1} \mid k \in K\}$ de um subgrupo H chama-se *K-classe de conjugação de* H, e seus elementos chamam-se os *K-conjugados de* H.

3) O estabilizador é

$$E(H) = \{k \in K;\ kHk^{-1} = H\} = K \cap N_G(H).$$

Novamente, pela observação 3.4, segue que,

$$\#\{\text{K-conjugados de } H\} = (K : K \cap N_G(H)).$$

3.2 Teoremas de Sylow

Iniciaremos agora uma das seções mais interessantes do nosso trabalho, que trata da demonstração dos Teoremas de Sylow. Ainda nesta seção, estudaremos algumas noções de p-Grupos, no qual o símbolo p indicará sempre um inteiro primo. Alguns lemas terão suas demonstrações omitidas, mas podem ser consultadas na referência [3].

Lema 3.1. (Cauchy) Sejam G um grupo abeliano finito e p um número primo que divide $|G|$. Então existe $x \in G$ de ordem p.

Demonstração. Vamos provar esse resultado por indução sobre $|G|$.

Se $|G| = 1$, não existe nada para mostrar.

Suponha que $|G| > 1$ e que, como hipótese de indução, o lema é válido para todos os grupos abelianos de ordem menor que $|G|$. Pretendemos provar que o lema é válido do mesmo modo para o grupo G.

Suponha que $|G| = p$. Assim, G é cíclico e qualuqer gerador de G tem ordem p. Provando o que queríamos.

Suponha que $|G| \neq p$. Assim, afirmamos primeiramente que existe um subgrupo H tal que $1 < |H| < |G|$. De fato, tome $y \in G$, $y \neq e$. Se $\langle y \rangle \neq G$, então $H = \langle y \rangle$ satisfaz $1 < |H| < |G|$. Se $\langle y \rangle = G$, então $y^p \neq e$ e $H = \langle y^p \rangle$ também satisfaz, visto que $|H| = o(y^p) = |G|/p < |G|$.

Agora, se $p \mid |H|$ então, pela hipótese de indução, existe $x \in H \subseteq G$ com $o(x) = p$, concluindo o que queriamos mostrar.

Caso p não divida $|H|$ então pelo Teorema de Lagrange temos a igualdade $|G| = |H||G/H|$ e como G é abeliano temos que $H \lhd G$. Pela igualdade anterior vemos que $p \mid |G/H|$ e que $|G/H| < |G|$; logo, pela hipótese de indução, o grupo G/H admite um elemento $\overline{z}$ de ordem p. Considere o homomorfismo canônico, onde $z \in G$,

$$\begin{aligned} \varphi : \quad G &\longrightarrow G/H \\ z &\longmapsto \overline{z} \end{aligned}$$

Seja r a ordem de z; temos $z^r = e$ logo $\varphi(z^r) = \varphi(e)$, ou seja, $\overline{z^r} = \overline{e}$ e, portanto, r é um múltiplo da ordem de $\overline{z}$, isto é, r é um múltiplo de p, digamos $r = kp$ com $k \geq 1$. Então, z^k é um elemento de G de ordem p.

□

Teorema 3.2. (1º Teorema de Sylow) Sejam p um número primo e G um grupo com $|G| = p^m b$, com $(p, b) = 1$. Então, para cada $n \in \{0, ..., m\}$ existe um subgrupo H de G tal que $|H| = p^n$.

Demonstração. Vamos provar por indução em $|G|$.

Se $|G| = 1$, não existe nada para mostrar.

Suponha que $|G| > 1$ e que, como hipótese de indução, o teorema é válido para todos os grupos de ordem menor que $|G|$. Pretendemos provar que o teorema é válido do mesmo modo para o grupo G.

Seja $n \in \mathbb{Z}_+$ tal que $p^n \mid |G|$. Vamos dividir em dois casos.

Caso 1: Suponha que existe um subgrupo próprio H de G tal que p^n divida a ordem de H. Diante disso, pela hipótese de indução, temos que H possui um subgrupo de ordem p^n. Logo, G também o possui.

Caso 2: Suponha que não existe um subgrupo próprio H de G tal que p^n divida a sua ordem. Diante disso, considere a equação das classes de conjugação:

$$|G| = |Z(G)| + \sum_{x_\alpha \notin Z(G)} |Cl(x_\alpha)| = |Z(G)| + \sum_{x_\alpha \notin Z(G)} (G : Z(x_\alpha)).$$

Para $x_\alpha \notin Z(G)$ segue que $Z(x_\alpha) \subsetneq G$. Logo, $Z(x_\alpha)$ é um subgrupo próprio de G e por hipótese temos que p^n não divide $|Z(x_\alpha)|$, e portanto p divide $(G : Z(x_\alpha))$. Como p divide $|G|$, obtemos

$$p \mid (|G| - \sum_{x_\alpha \notin Z(G)} (G : Z(x_\alpha))) \Rightarrow p \mid |Z(G)|.$$

Visto que $Z(G)$ é um grupo abeliano finito, pelo lema de Cauchy, $Z(G)$ admite um elemento y de ordem p. Como $y \in Z(G)$ então $\langle y\rangle \subseteq Z(G) \Rightarrow \langle y\rangle \lhd G$. Assim, podemos considerar o grupo quociente $G/\langle y\rangle$. Naturalmente, $|G/\langle y\rangle| < |G|$ e p^{n-1} divide $|G/\langle y\rangle|$. Da indução, o grupo $G/\langle y\rangle$ possui um subgrupo K' de ordem p^{n-1}. Considere o homomorfismo canônico $\varphi : G \to G/\langle y\rangle$ e tome $K := \varphi^{-1}(K')$. Então K é um subgrupo de G que contém $\langle y\rangle$ e pelo teorema do isomorfismo segue que $\dfrac{K}{ker\varphi} \simeq K'$. Assim, segue que

$$|K| = |ker\ \varphi||K'| = |\langle y\rangle||K'| = p^n.$$

□

Corolário 3.1. (Generalização do lema de Cauchy) Sejam G um grupo finito e p um número primo que divide a ordem de G. Então G admite um elemento de ordem p.

Corolário 3.2. Sejam G um grupo finito e p um número primo. Seja p^m a maior potência de p que divide a ordem de G. Logo, existe um subgrupo de G de ordem p^m.

Definição 3.5. Sejam G um grupo finito, p um número primo e p^m a maior potência de p que divide a ordem de G. Os subgrupos de G que possuem ordem p^m são chamados de p-subgrupos de Sylow de G.

Observação 3.5. Se p é um número primo que não divide a ordem de G, isso implica que $\{e\}$ é o único p-subgrupo de Sylow de G.

Corolário 3.3. Sejam G um grupo finito e p um número primo. Então a ordem de G é igual a uma potência de p se, e somente se, todo elemento de G tem sua ordem igual a uma potência de p.

Demonstração. ($\Rightarrow$) Seja $x \in G$ e, por hipótese, $|G| = p^t$. Pelo Teorema de Lagrange, $o(x) \mid p^t$ e, portanto, é uma potência de p.

($\Leftarrow$) Se $|G|$ não é uma potência de p, existe um número primo q tal que $q \neq p$ e q divide a ordem de G. Pelo Corolário 3.1 temos que

$$\exists\ x \in G \text{ tal que } o(x) = q.$$

□

Definição 3.6. Sejam G um grupo, não necessariamente finito, e p um número primo. Dizemos que G é um p-grupo se cada elemento de G tem sua ordem igual a uma potência de p.

Lema 3.2. Sejam G um grupo finito e p um número primo. Sejam S um p-subgrupo de Sylow de G e P um p-subgrupo qualquer de G. Assim, $P \cap N_G(S) = P \cap S$.

Teorema 3.3. (2º Teorema de Sylow) Sejam G um grupo finito, p um número primo tal que $p \mid |G|$ e n_p o número de p-subgrupos de Sylow de G. Portanto:

a) Todos os p-subgrupos de Sylow de G são conjugados entre si.

b) Se P é um p-subgrupo de G, logo existe um p-subgrupo de Sylow S de G em que $P \subseteq S$.

c) Se S é um p-subgrupo de Sylow, então temos que

$$n_p = (G : N_G(S)).$$

Demonstração. Dado S um p-subgrupo de Sylow qualquer de G, considere os conjuntos $C = \{\text{conjugados de } S\} = \{gSg^{-1}; g \in G\}$ e $D = \{\text{subgrupos de } G\}$. Por definição, o conjunto C é a órbita de S na representação por conjugação $I : G \longrightarrow P(D)$. Logo, pelo exemplo 3.6,

$$|C| = (G : N_G(S)). \tag{3.1}$$

Para mostrar os itens a) e b) basta verificar que um p-subgrupo P qualquer de G está contido em um conjugado de S em G.

Seja P um p-sugrupo de G e considere a representação abaixo:

$$\begin{aligned} I: \quad & P \longrightarrow P(C) \\ & a \longmapsto I_a: \quad C \to C \\ & \qquad\qquad\quad gSg^{-1} \mapsto agSg^{-1}a^{-1}. \end{aligned}$$

Sejam $\mathfrak{O}_1, ..., \mathfrak{O}_k$ as órbitas duas a duas distintas dessa representação, ou seja,

$$\mathfrak{O}_i = \{aS_ia^{-1}; a \in G; \quad S_i = g_iSg_i^{-1}\}$$

Para cada $\mathfrak{O}_i$ escolha um representante S_i dentro de $\mathfrak{O}_i$. Podemos perceber que $|C| = \sum_{i=1}^{k} |\mathfrak{O}_i|$ e pela Observação 3.4, temos $|\mathfrak{O}_i| = (P : E(S_i)) = (P : P \cap N_G(S_i))$ e, pelo Lema 3.2, temos $(P : P \cap N_G(S_i)) = (P : P \cap S_i)$. Assim, obtemos

$$|C| = \sum_{i=1}^{k} (P : P \cap S_i). \tag{3.2}$$

Portanto, de 3.1 e 3.2 segue que

$$(G : N_G(S)) = \sum_{i=1}^{k} (P : P \cap S_i). \tag{3.3}$$

Como P é um p-grupo, pelo teorema de Lagrange temos que cada parcela $(P : P \cap S_i)$ é igual a 1 ou a um múltiplo de p. Além disso, o primo p não divide $(G : S)$ visto que S é um

p-subgrupo de Sylow. Sabendo que $S \leq N_G(S) \leq G$, pela Proposição 2.9 temos que

$$(G : S) = (G : N_G(S))(N_G(S) : S).$$

Com isso, p não divide $(G : N_G(S))$. Dessa forma, existe j tal que p não divide $(P : P \cap S_j)$ e portanto $(P : P \cap S_j) = 1$.

Assim, temos que

$$(P : P \cap S_j) = 1 \Rightarrow P = P \cap S_j \Rightarrow P \subseteq S_j = g_j S g_j^{-1}.$$

Em particular, se $|P| = p^m = |S_j|$, então $P = S_j$. Isso implica que $P \in C$.

Logo,

$$\{p\text{-subgrupos de Sylow}\} = \{\text{conjugados de } S\} = C.$$

c) Pelo item a), segue que

$$n_p = |C| = (G : N_G(S)).$$

□

Corolário 3.4. Sejam G um grupo finito, p primo em que $p \mid |G|$ e S um p-subgrupo de Sylow de G. Como caso particular do item a) do teorema anterior, temos que $S \lhd G$ se e somente se S é o único p-subgrupo de Sylow de G.

Demonstração. ($\Rightarrow$) Considere C o conjunto formado pelos conjugados de S. Pelo 2º teorema de Sylow, temos que

$$\{p\text{-subgrupos de Sylow de } G\} = C = \{gSg^{-1} \mid g \in G\} = \{S\}.$$

Assim, S é o único p-subgrupo de Sylow de G.

($\Leftarrow$) Imediato. □

O terceiro teorema de Sylow traz uma propriedade aritmética do índice $(G : N_G(S))$, sendo S um p-subgrupo de Sylow de G.

Teorema 3.4. (3º Teorema de Sylow) Sejam p um número primo e G um grupo finito tal que $|G| = p^m b$, onde $(p, b) = 1$. Se n_p é o número de p-subgrupos de Sylow de G então

$$n_p \mid b \text{ e } n_p \equiv 1 \ mod \ p.$$

Demonstração. Seja S um p-subgrupo de Sylow de G. Assim, temos que $(G : S) = b$. Como $S \leq N_G(S) \leq G$, então pela Proposição 2.9 obtemos

$$(G : S) = (G : N_G(S))(N_G(S) : S).$$

Do 2º Teorema de Sylow, temos que $n_p = (G : N_G(S))$. Então $n_p \mid b$.

Agora, consideramos a expressão 3.3 para $(G : N_G(S))$ estabelecida ao longo da prova do 2º Teorema de Sylow. Utilizando S no lugar de P, obtemos

$$(G : N_G(S)) = \sum_{i=1}^{k} (S : S \cap S_i),$$

em que $S_1, ..., S_k$ são representantes das distintas órbitas $\mathfrak{O}_1, ..., \mathfrak{O}_k$ da representação seguinte

$$I : S \longrightarrow P(C),$$

e C é o conjunto dos p-subgrupos de Sylow de G. Nitidamente, podemos tomar $S_1 = S$; com esta escolha nos resta provar que $p \mid (S : S \cap S_i), \forall\ i \in \{2, ..., k\}$.
De fato, dado $i \in \{2, ..., k\}$ por meio do Teorema de Lagrange temos que

$$|S| = (S : S \cap S_i)|S \cap S_i| \Rightarrow (S : S \cap S_i) \mid |S| \Rightarrow (S : S \cap S_i) \mid p^m.$$

Assim, $(S : S \cap S_i) = p^r$, com $r \in \mathbb{Z}^+$. Se $r = 0$, então $S_1 = S_i \Rightarrow i = 1$, absurdo. Com isso, $r \geq 1 \Rightarrow p \mid (S : S \cap S_i)$.

Sabendo que $n_p = (G : N_G(S))$, obtemos

$$n_p = (S : S \cap S) + \sum_{i=2}^{k} (S : S \cap S_i) \equiv 1\ mod\ p.$$

□

3.3 Aplicações

Agora vamos aplicar os resultados obtidos para alguns grupo finitos.

Exemplo 3.8. Dado G um grupo de ordem $380 = 2^2 \cdot 5 \cdot 19$, vamos mostrar que necessariamente ambos n_5 e n_{19} são iguais a 1.

Demonstração. Pelo 3º Teorema de Sylow, somente 1 e 76 satisfazem as condições expostas para n_5. As condições estabelecidas pelo teorema citado são

$$n_5 \equiv 1\ mod\ 5 \text{ e } n_5 \text{ divide } 2^2 \cdot 19.$$

Assim, temos $n_5 = 1$ ou 76. Do mesmo modo, o 3º Teorema de Sylow nos fornece $n_{19} = 1$ ou 20. Sejam H um 5-subgrupo de Sylow de G e K um 19-subgrupo de Sylow de G. Para provar que n_5 e n_{19} são necessariamente iguais a 1, vamos buscar propriedades dos normalizadores de cada subgrupo em G.

Primeiro, afirmamos que n_5 ou n_{19} é igual a 1; com efeito, caso contrário, G possuiria $(5 - 1) \cdot 76 = 304$ elementos de ordem igual a 5 e também possuiria $(19 - 1) \cdot 20 = 360$

elementos de ordem 19 (É retirado de cada subgrupo o elemento neutro). Isso é um absurdo, pois G possuiria ao todo 664 elementos e sabemos que $|G| = 380$. Deste modo, um dos subgrupos H ou K é normal em G (pois $n_5 = 1$ ou $n_{19} = 1$) e, em todo caso, o conjunto HK é um subgrupo de G; temos que $|HK| = 5 \cdot 19 = 95$ visto que, nitidamente, $H \cap K = \{e\}$. Agora, aplicando o 3º Teorema de Sylow ao grupo HK, vemos que HK possui somente um subgrupo de ordem 5 (que necessariamente deve ser H) e somente um subgrupo de ordem 19 (que necessariamente deve ser K). Portanto, H é normal em HK e equivalentemente, temos $HK \subseteq N_G(H)$; logo $n_5 = (G : N_G(H)) \leq (G : HK) = 2^2$ e, portanto, $n_5 = 1$, pois já sabíamos que n_5 era igual a 1 ou 76. Do mesmo modo, K é normal em HK e equivalentemente, temos $HK \subseteq N_G(K)$; logo $n_{19} = (G : N_G(K)) \leq (G : HK) = 2^2$ e, portanto, $n_{19} = 1$, pois já sabíamos que n_{19} era igual a 1 ou 20. □

Exemplo 3.9. Seja G um grupo e sejam p e q números primos. Se $|G| = pq$, então G possui um subgrupo normal não-trivial.

Demonstração. Se $p = q$, então $|G| = p^2$. Pela Proposição 3.1, G é abeliano, como decorrência, todo subgrupo de G é normal nele. Agora, se $p \neq q$, podemos supor sem perda de generalidade que $p > q$. Denotando por n_p o número de p-subgrupos de Sylow de G. Fazendo uso do 3º Teorema de Sylow obtemos,

$$n_p \equiv 1 \; mod \; p \text{ e } n_p \text{ divide } q.$$

Logo, $n_p = 1$ visto que $p > q$. Portanto, possuímos um único p-subgrupo de Sylow de G e este é normal em G. □

Exemplo 3.10. Se G é um grupo de ordem $364 = 2^2 \cdot 7 \cdot 13$, então G possui um subgrupo normal de ordem 13.

Demonstração. Seja n_{13} o número de 13-subgrupos de Sylow de G. Por meio do 3º Teorema de Sylow, obtemos

$$n_{13} \equiv 1 \; mod \; 13 \text{ e } n_{13} \text{ divide } 2^2 \cdot 7.$$

Assim, temos $n_{13} = 1$ ou 14. Seja S um 13-subgrupo de Sylow de G. Desejamos informações sobre $(G : N_G(S))$; para tal procuramos subgrupos entre S e $N_G(S)$, ou seja, buscamos subgrupos nos quais S é normal. Pelo 3º Teorema de Sylow, temos $n_7 = 1$; seja então K o único 7-subgrupo de Sylow de G. Como $K \lhd G$, visto que $n_7 = 1$, o produto KS é um subgrupo de G; temos que $|KS| = 7 \cdot 13$, pois $K \cap S = \{e\}$. Aplicando o 3º Teorema de Sylow ao grupo KS, vemos que $S \lhd KS$. Logo, $n_{13} = (G : N_G(S)) \leq (G : KS) = 2^2$. Portanto, temos $n_{13} = 1$. □

O resultado abaixo nos fornece um caso particular onde podemos concluir se um grupo é cíclico.

Proposição 3.4. Seja G um grupo e sejam p, q números primos tais que $p < q$ e p não divide $q - 1$. Se $|G| = pq$, então G é cíclico.

Demonstração. Pelo 3º Teorema de Sylow, temos

$$n_p \equiv 1 \; mod \; p \text{ e } n_p \mid q; \; n_q \equiv 1 \; mod \; q \text{ e } n_q \mid p.$$

Com isso, $n_p = 1$ ou q. Temos uma contradição, pois para que $n_p = q$ é necessário que $p \mid q - 1$ e por hipótese temos que p não divide $q - 1$, logo $n_p = 1$. Similarmente, $n_q = 1$ ou p. Novamente há uma contradição, pois na medida em que temos $n_q = p$ implica que $q \mid p - 1$ e isso exige que $p > q$; por hipótese dispomos de $p < q$ e assim $n_q = 1$. Sejam H o único p-subgrupo de Sylow de G e K o único q-subgrupo de Sylow de G. Como $n_p = 1$ e $n_q = 1$, $H \lhd G$ e $K \lhd G$. Além disso, como são grupos de ordem primo, são cíclicos. Então existem $a, b \in G$ tais que $H = \langle a \rangle$ e $K = \langle b \rangle$. Visto que H e K são normais em G, $aba^{-1} \in K$ e $ba^{-1}b^{-1} \in H$, logo

$$aba^{-1}b^{-1} \in H \cap K.$$

Por outro lado, dado que p e q são primos distintos, $H \cap K = \{e\}$ o que implica que $G = HK$, onde e é o elemento neutro de G. Então,

$$ab = ba \Rightarrow G = \langle ab \rangle.$$

Em particular, grupos de ordem $33, 51, 65, ...$ são cíclicos. □

Exemplo 3.11. Se G é um grupo de ordem $182 = 2 \cdot 7 \cdot 13$, então G contêm no máximo 91 elementos de ordem 2.

Demonstração. Seja n_2 o número de 2-subgrupos de Sylow de G. Mediante o 3º Teorema de Sylow, obtemos

$$n_2 \equiv 1 \; mod \; 2 \text{ e } n_2 \mid 91.$$

Logo, $n_2 = 1$ ou 91. Deste modo, G possui no máximo 91 elementos de ordem 2. □

4 Conclusão

Ao desenvolver este trabalho pude me aprofundar mais sobre os conteúdos presentes na disciplina de Estruturas Algébricas I, conteúdos esses de grande relevância devido a generalidade que proporcionam.

Em meio a todos os resultados expostos no presente trabalho, destacamos os Teoremas de Sylow que constituem uma parte fundamental da teoria dos grupos finitos. Estes teoremas são importantíssimos no estudo da classificação de grupos finitos e por meio deles conseguimos nos aproximar de uma recíproca para o Teorema de Lagrange.

REFERÊNCIAS

Aleksandrov, A. D; kolmogorov, A. N; Laurentiev, M. A. **La matemática: su contenido, métodos y significado.** Vol 3. Madrid. Alianza Editorial, 1994.

Boyer, C.B. **História da matemática.** Tradução: Elza F. Gomide. São Paulo, Edgard Blucher, Ed. da Universidade de São Paulo, 1974.

Garcia, A; Lequain, Y. **Elementos de Álgebra.** Rio de Janeiro, IMPA, 2010.

Gonçalves, A. **Introdução à Álgebra.** Rio de Janeiro, IMPA, 2008.

Quaresma, J. C. B; **Uma análise histórico-epistemológica do conceito de grupo.** Tese de doutorado. UFRN (2009).

Souza, J. A; **Uma nota sobre a teoria dos grupos: A teoria de Galois à teoria de Gauge.** Revista brasileira de história da matematíca. Vol 12, nº24.