UNIVERSIDADE DO ESTADO DA BAHIA
DEPARTAMENTO DE CIÊNCIAS EXATAS E DA TERRA II
COLEGIADO DE MATEMÁTICA

VILEMAR FRAGAS DOS REIS FILHO

Condição suficiente para a existência de um grupo finito gerado por dois elementos a e b satisfazendo as relações $a^n = e$, $b^m = a^u$ e $ba = a^s b$

ALAGOINHAS
2025

VILEMAR FRAGAS DOS REIS FILHO

Condição suficiente para a existência de um grupo finito gerado por dois elementos a e b satisfazendo as relações $a^n = e$, $b^m = a^u$ e $ba = a^s b$

Monografia apresentada ao Curso de Licenciatura em Matemática do Departamento de Ciências Exatas e da Terra - Campus II (DCET-II) da Universidade do Estado da Bahia (UNEB), como requisito parcial à obtenção do grau de licenciado em Matemática.
Área de concentração: Álgebra.

Orientador: Me. Luís Roque Rodrigues de Jesus.

ALAGOINHAS
2025

VILEMAR FRAGAS DOS REIS FILHO

Condição suficiente para a existência de um grupo finito gerado por dois elementos a e b satisfazendo as relações $a^n = e$, $b^m = a^u$ e $ba = a^s b$

Monografia apresentada ao Curso de Licenciatura em Matemática do Departamento de Ciências Exatas e da Terra - Campus II (DCET-II) da Universidade do Estado da Bahia (UNEB), como requisito parcial à obtenção do grau de licenciado em Matemática. **Área de concentração:** Álgebra.

Aprovada em: 16 de dezembro de 2025.

BANCA EXAMINADORA

Documento assinado digitalmente
gov.br
LUIS ROQUE RODRIGUES DE JESUS
Data: 27/02/2026 19:14:01-0300
Verifique em https://validar.iti.gov.br

Prof. Me. Luís Roque Rodrigues de Jesus
(Orientador)

Documento assinado digitalmente
gov.br
MARIDETE BRITO CUNHA FERREIRA
Data: 28/02/2026 18:11:24-0300
Verifique em https://validar.iti.gov.br

Prof.ª Dra. Maridete Brito Cunha Ferreira
Examinadora Interna (DCET-II/UNEB)

Prof.ª Ma. Glaene Santos Santiago Mendonça
Examinadora Externa (UFBA)

Documento assinado digitalmente
gov.br
GLAENE SANTOS SANTIAGO MENDONCA
Data: 27/02/2026 15:37:39-0300
Verifique em https://validar.iti.gov.br

ALAGOINHAS
2025

A caminho de Damasco,
Tive a perspectiva que me falta.
Vi o antes e o depois.
E isso não significava nada.

— Rogerio Skylab

Agradecimentos

Enfatizo meus agradecimentos exclusivamente àqueles que estão mais diretamente ligados à minha trajetória acadêmica, pois acredito que aqueles relacionados à minha vida pessoal sabem, de fato, em que medida sou grato a eles.

Assim, agradeço, inicialmente, a todos os professores que contribuíram para minha formação, compartilhando conhecimentos e despertando meu interesse pela matemática.

Devo um agradecimento especial ao meu ex-coordenador do Colegiado de Matemática do nosso campus, Erivelton Nonato, pelo incentivo e pelos constantes esforços em relação ao fornecimento de disciplinas e ao reajuste de horários, o que me permitiu agilizar o curso em um momento decisivo. Sou grato também ao meu atual coordenador, Mário Ferreira, pela sugestão do tema inicial que conduziu a este trabalho.

Agradeço aos colegas com quem pude estudar e discutir conteúdos, aprendendo diferentes perspectivas e consolidando meu conhecimento. Como são tantos, a fim de não esquecer alguém, prefiro não citá-los individualmente, mas deixo meu sincero agradecimento a todos.

Em especial, agradeço à professora Maridete Brito, por me apresentar a matemática como um sistema lógico-dedutivo e tornar tão interessante meu primeiro contato com demonstrações, despertando minha paixão permanente pela disciplina. À professora Grace Baqueiro, pelas aulas envolventes, pelas discussões proporcionadas e por incentivar minha participação em pesquisa e monitorias de ensino, além de compartilhar seus conhecimentos sobre educação matemática e oferecer orientações valiosas sobre ensino. Por fim, agradeço ao meu orientador, Luís Roque, por possibilitar o aprofundamento em temas que tanto almejava, pela disponibilidade constante, pelos desafios propostos e pelo incentivo a avançar em estudos que inicialmente me pareciam impossíveis.

A todos que participaram desta jornada, minha sincera gratidão.

Resumo

Este trabalho apresenta uma demonstração construtiva e didática para a existência de grupos finitos da forma $G = \langle a, b \rangle$ definidos pelas relações $a^n = e$, $b^m = a^u$ e $ba = a^s b$. O objetivo principal é provar a suficiência das condições de congruência $s^m \equiv 1 \pmod{n}$ e $u(s-1) \equiv 0 \pmod{n}$, as quais, como se sabe, são também necessárias para a existência de tais grupos (os quais são únicos, a menos de isomorfismos). A abordagem inicia-se com uma motivação detalhada que torna explícitas as idéias que conduzem naturalmente à escolha do grupo candidato e da sua operação binária. Em seguida, a construção é realizada explicitamente sobre um conjunto de pares ordenados, utilizando apenas ferramentas elementares da Teoria de Grupos e Teoria dos números, aritmética modular, indução e propriedades elementares de homomorfismos. Como consequência, obtém-se a garantia da existência dos grupos dos quatérnions generalizados Q_n e dos grupos diedrais D_n, além da classificação completa dos grupos de ordem $2p$, com p primo ímpar. Como desdobramento natural, aponta-se para a possibilidade de estender o método construtivo aqui desenvolvido ao caso de grupos gerados por três elementos, conforme sugerido, mas não demonstrado, na literatura consultada. O trabalho destaca-se, portanto, por oferecer uma prova completa, pedagogicamente orientada e motivada desde as escolhas construtivas iniciais, preenchendo uma lacuna expositiva na literatura.

Palavras-chave: Grupos finitamente gerados; Subgrupo gerado; Condição suficiente; Teorema de Existência; Demonstração Motivada.

Abstract

This work presents a constructive and didactic proof for the existence of finite groups of the form $G = \langle a, b \rangle$ defined by the relations $a^n = e$, $b^m = a^u$, and $ba = a^s b$. The main objective is to prove the sufficiency of the congruence conditions $s^m \equiv 1 \pmod{n}$ and $u(s-1) \equiv 0 \pmod{n}$, which, as is known, are also necessary for the existence of such groups (and which are unique up to isomorphism). The approach begins with a detailed motivation that makes explicit the ideas that naturally lead to the choice of the candidate group and its binary operation. Subsequently, the construction is explicitly carried out on a set of ordered pairs, using only elementary tools from Group Theory and Number Theory, modular arithmetic, induction, and basic properties of homomorphisms. As a consequence, the existence of the generalized quaternion groups Q_n and the dihedral groups D_n is guaranteed, in addition to the complete classification of groups of order $2p$, where p is an odd prime. As a natural continuation, the possibility of extending the constructive method developed here to the case of groups generated by three elements is pointed out, as suggested but not demonstrated in the consulted literature. This work thus stands out for offering a complete, pedagogically oriented, and motivationally grounded proof from the initial constructive choices, filling an expository gap in the literature.

Keywords: Finitely generated groups; Generated subgroup; Sufficient condition; Existence theorem; Motivated proof.

Sumário

1 Introdução

As estruturas algébricas constituem objetos de grande relevância em Álgebra e são definidas como conjuntos dotados de operações que satisfazem certas propriedades. Entre essas estruturas destacam-se os grupos, cujo conceito, como observa Milies (2022), envolve um elevado grau de abstração e figura entre os primeiros a serem formulados com tal generalidade, tendo suas raízes nos estudos históricos de grupos de permutações, os quais estavam ligados à resolução de equações algébricas por radicais.

No âmbito dos grupos finitos, aqueles gerados por um único elemento podem ser facilmente classificados. Contudo, como mencionam Garcia e Lequain (2022), o mesmo não ocorre com grupos finitos gerados por dois elementos, cuja estrutura pode se tornar significativamente mais complexa e de difícil descrição. Apesar disso, alguns casos particulares em que certas relações são satisfeitas tornam o trabalho com grupos gerados por dois elementos mais acessível e, ainda assim, conduzem a resultados relevantes. É precisamente nesse cenário que se insere o presente trabalho. Investigaremos grupos finitos da forma $G = \langle a, b\rangle$, submetidos às relações $a^n = e$, $b^m = a^u$ e $ba = a^s b$. Nosso objetivo é demonstrar um teorema que estabelece condições suficientes para a existência de grupos com essa configuração.

A motivação para esta investigação originou-se do estudo da obra de Garcia e Lequain (2022). Os autores, ao tratarem de grupos finitos gerados por dois elementos, apresentam condições de congruência envolvendo os inteiros n, m, s e u como necessárias e suficientes para a existência de um (único, a menos de isomorfismos) grupo satisfazendo as relações mencionadas anteriormente. No entanto, os autores apresentam a demonstração da suficiência apenas para o caso particular $u = 0$, justificando que a prova do caso geral seria excessivamente técnica. Além disso, mesmo para esse caso particular, precisam primeiro introduzir uma ferramenta mais avançada: o produto semidireto de grupos. Esta lacuna expositiva motivou a questão central que norteou este trabalho: seria possível, utilizando apenas as ferramentas elementares da teoria de grupos já disponíveis até aquele ponto, construir uma prova completa, acessível e bem motivada do caso geral?

A pertinência desta questão reforçou-se ao se consultar uma exposição alternativa, onde Garcia (1985) (inspirado em notas de aula do professor Yves Lequain) exibe um candidato ao grupo, porém sem apresentar a motivação subjacente à sua construção e sem, possivelmente devido a limitações de espaço, verificar em detalhes que tal objeto de fato satisfaz todas as relações impostas. Assim, o presente trabalho posiciona-se como uma contribuição de caráter didático e de síntese, preenchendo essa lacuna ao oferecer uma demonstração, apoiada exclusivamente nos recursos introduzidos até o ponto em que é apresentada, bem como explicitar a motivação que guiou sua formulação.

A demonstração do Teorema Principal foi construtiva. A motivação inicial permitiu descrever os raciocínios necessários para formular o grupo e a operação. Em seguida,

para estabelecer a suficiência, construímos explicitamente o grupo G como um conjunto de pares ordenados munido de uma operação cuidadosamente definida. A verificação de que esta operação, sobre o conjunto dado, define de fato um grupo que satisfaz as relações esperadas utilizou: indução, propriedades de homomorfismos, aritmética modular, propriedades sobre o quociente e o resto da divisão euclidiana de inteiros e outros resultados básicos sobre grupos.

A relevância deste resultado reside não apenas em seu valor didático. Na seção de aplicações, demonstramos como o Teorema Principal fornece um método alternativo e elegante para: (i) garantir a existência dos quatérnions generalizados Q_n e do grupo diedral D_n; (ii) classificar, de forma concisa, todos os grupos de ordem $2p$, em que p é um primo ímpar.

Este trabalho está organizado da seguinte forma: no Capítulo 2, revisamos os conceitos fundamentais de grupos, subgrupos e homomorfismos. No Capítulo 3, apresentamos resultados específicos sobre grupos finitos gerados por dois elementos e desenvolvemos tanto a motivação quanto a demonstração detalhada do Teorema Principal, encerrando o capítulo com três aplicações desse resultado. Por fim, nas Considerações Finais, sintetizamos as contribuições alcançadas e indicamos possíveis desdobramentos para estudos futuros.

2 Teoria Básica de Grupos

2.1 Grupos

Um grupo é uma estrutura algébrica composta por um conjunto não vazio G e uma operação binária que satisfaz certas propriedades fundamentais. Nesta seção, apresentamos precisamente a definição de grupo, introduzimos notações utilizadas ao longo deste trabalho, verificamos propriedades básicas decorrentes da definição e exibimos exemplos de grupos.

Definição 1. *Uma operação binária sobre um conjunto G é uma função*

$$\begin{aligned} \cdot : G \times G &\longrightarrow G \\ (a, b) &\longmapsto a \cdot b \end{aligned}$$

Exemplo 1. *Sejam $n \in \mathbb{N} - \{0\}$ e $z \in \mathbb{Z}$. Iremos utilizar a notação $r_n(z)$ para indicar o resto da divisão euclidiana de z por n. Assim, sobre o conjunto $\mathbb{Z}_n := \{0, 1, 2, \cdots, n-1\}$, definimos a operação*

$$\begin{aligned} \underset{n}{\oplus} : \mathbb{Z}_n \times \mathbb{Z}_n &\longrightarrow \mathbb{Z}_n \\ (a, b) &\longmapsto a \underset{n}{\oplus} b = r_n(a + b) \end{aligned}$$

Exemplo 2. *Sejam $n \in \mathbb{N} - \{0\}$ e $\mathbb{Z}_n^* := \{m : m \in \mathbb{Z}_n \wedge \text{mdc}(m, n) = 1\}$. Se $a, b \in \mathbb{Z}_n^*$, então $\text{mdc}(a, n) = 1$ e $\text{mdc}(b, n) = 1$. Pelo teorema de Bezout, existem $q, r, s, t \in \mathbb{Z}$ tais que $bs + nt = 1 = aq + nr$. Daí,*

$$\begin{aligned} 1^2 &= (bs + nt)(aq + nr) \\ &= bsaq + ntaq + bsnr + n^2tr \\ &= ab(qs) + n(taq + bsr + ntr) \end{aligned}$$

Pelo algoritmo da divisão, existem $p, r_n(ab) \in \mathbb{Z}$, com $0 \leq r_n(ab) < n$, tal que $ab = pn + r_n(ab)$. Logo,

$$\begin{aligned} 1 &= (pn + r_n(ab))(qs) + n(taq + bsr + ntr) \\ &= pqsn + r_n(ab)(qs) + n(taq + bsr + ntr) \\ &= r_n(ab)(qs) + n(taq + bsr + ntr + pqs) \end{aligned}$$

Pela recíproca do teorema de Bezout (que vale quando o máximo divisor comum entre dois números é um), obtemos que $\text{mdc}(r_n(ab), n) = 1$ e, portanto, $r_n(ab) \in \mathbb{Z}_n^*$. Logo, $\underset{n}{\odot}$ é uma operação sobre $\mathbb{Z}_n^*$, definida por $a \underset{n}{\odot} b = r_n(ab)$, para todos $a, b \in \mathbb{Z}_n^*$.

Definição 2. *Sejam P e Q pontos quaisquer. Denotaremos por $d(P,Q)$ a distância entre P e Q. Seja $\mathcal{F}$ uma figura geométrica (qualquer conjunto de pontos). Uma simetria de $\mathcal{F}$ é uma função $f : \mathcal{F} \longrightarrow \mathcal{F}$ que satisfaz as seguintes propriedades*

(1) f é bijetiva.

(2) f preserva a distância entre pontos de $\mathcal{F}$, i.e., $d(f(Q), f(P)) = d(P,Q); \forall P, Q \in \mathcal{F}$.

Exemplo 3. *Seja $\mathcal{F}$ uma figura geométrica e $S_{\mathcal{F}}$ o conjunto das simetrias da figura $\mathcal{F}$. Então, a composição de funções reestrita ao conjunto $S_{\mathcal{F}}$ é uma operação sobre $S_{\mathcal{F}}$.*

Com efeito, sendo $f, g \in S_{\mathcal{F}}$, então $f \circ g : \mathcal{F} \longrightarrow \mathcal{F}$ é bijetiva, pois a composição de funções bijetivas, é também uma função bijetiva. Além disso, dados $P, Q \in \mathcal{F}$, temos

$$\begin{aligned} d\left((f \circ g)(P), (f \circ g)(Q)\right) &= d\left((f(g(P)), f(g(Q))\right) \\ &\overset{(1)}{=} d\left((g(P)), g(Q))\right) \\ &\overset{(2)}{=} d(P,Q) \end{aligned}$$

As igualdades (1) e (2) decorrem, respectivamente, do fato de f e g serem simetrias de $\mathcal{F}$, aplicadas em pontos de $\mathcal{F}$. Logo, $f \circ g \in S_{\mathcal{F}}$ e, portanto, $\circ$ é uma operação sobre $S_{\mathcal{F}}$.

Definição 3. *Sejam G um conjunto e $\cdot$ uma operação binária sobre G. Dizemos que $(G, \cdot)$ é um grupo se*

(1) A operação é associativa, isto é, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$, para todo $a, b, c \in G$.

(2) O conjunto G admite elemento neutro relativamente a operação $\cdot$, i.e., $\exists e \in G$ tal que $g \cdot e = g = g \cdot e, \forall g \in G$.

(3) Todo elemento em G admite um inverso, i.e., $\forall a \in G, \exists b \in G$,tal que $a \cdot b = e = b \cdot a$

Além disso, dizemos que $(G, \cdot)$ é um grupo comutativo (ou abeliano) se, além das condições anteriores, é satisfeita

(4) A operação é comutativa, ou seja, $a \cdot b = b \cdot a$, para todos $a, b \in G$.

Observação 1. *Quando não houver ambiguidade, escreveremos G para denotar o grupo $(G, \cdot)$ e ab para denotar o composto $a \cdot b$ de dois elementos $a, b \in G$.*

Antes de darmos exemplos de grupos, vamos mostrar algumas propriedades que decorrem imediatamente da definição de grupo, e que nos serão úteis posteriormente.

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

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

Demonstração. (1) Sejam $(G, \cdot)$ um grupo e e, e' elementos neutro em G. Como e' é elemento neutro, temos que $e = ee'$. Mas do fato de e também ser elemento neutro, temos que $ee' = e'$. Portanto, $e = e'$. Isso mostra que e é o único elemento neutro de G.

(2) Sejam G um grupo, $g \in G$ e $b, b' \in G$ inversos do elemento g. Então, $gb = e = gb'$, donde segue-se ao se aplicar b à esquerda em ambos os membros da igualdade $gb = gb'$, que $b = b'$.

□

Observação 2. *Em virtude da unicidade do inverso de um elemento a em um grupo, denotaremos esse elemento por a^{-1} quando o grupo for multiplicativo, e por $-a$, quando o grupo for aditivo.*

Proposição 2. *(1) Se G é um grupo e $a, b \in G$, então a equação $x \cdot a = b$ (respectivamente, $a \cdot x = b$) tem uma única solução.*

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

Demonstração. (1) Evidentemente, ba^{-1} é uma solução da equação $x \cdot a = b$. Suponha que $c \in G$ é uma solução da equação. Então,

$$ca = b \Rightarrow caa^{-1} = ba^{-1} \Rightarrow ce = ba^{-1} \Rightarrow c = ba^{-1}$$

Portanto, ba^{-1} é a única solução da equação dada. De modo análogo mostra-se que $a^{-1}b$ é a única solução da equação $a \cdot x = b$.

(2) Sejam $a, b \in G$. Então, $(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = aea^{-1} = aa^{-1} = e$. De modo análogo, podemos concluir que $(b^{-1}a^{-1})(ab) = e$. Logo, $b^{-1}a^{-1}$ é o inverso do elemento ab, isto é, $(ab)^{-1} = b^{-1}a^{-1}$. □

Neste trabalho, iremos assumir que $(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +), (\mathbb{C}, +), (\mathbb{Q} - \{0\}, \cdot), (\mathbb{R} - \{0\}, \cdot)$ e $(\mathbb{C} - \{0\}, \cdot)$ são grupos abelianos. As provas desses fatos podem ser encontradas em (FERREIRA, 2022).

Exemplo 4. *Seja $n \in \mathbb{N} - \{0\}$. O conjunto $\mathbb{Z}_n := \{0, 1, 2, \cdots, n-1\}$ com a operação*

$$\begin{aligned} \underset{n}{\oplus} : \mathbb{Z}_n \times \mathbb{Z}_n &\longrightarrow \mathbb{Z}_n \\ (a, b) &\longmapsto a \underset{n}{\oplus} b = r_n(a + b) \end{aligned}$$

é um grupo abeliano.

De fato, dados $a, b, c \in \mathbb{Z}_n$,temos

$$(a \underset{n}{\oplus} b) \underset{n}{\oplus} c = r_n(a + b) \underset{n}{\oplus} c = r_n(r_n(a + b) + c)$$

Note que, sendo $k \in \mathbb{Z}_n$, temos que $r_n(k) = k$. Daí, segue-se que

$$\begin{aligned}(a \underset{n}{\oplus} b) \underset{n}{\oplus} c &= r_n(r_n(a+b) + r_n(c)) \\ &= r_n((a+b)+c)) \\ &= r_n(a+(b+c))) \\ &= r_n(r_n(a) + r_n(b+c)) \\ &= r_n(a+b \underset{n}{\oplus} c) \\ &= a \underset{n}{\oplus} (b \underset{n}{\oplus} c)\end{aligned}$$

Portanto, a operação $\underset{n}{\oplus}$ sobre $\mathbb{Z}_n$ é associativa. Além disso, temos

$$a \underset{n}{\oplus} b = r_n(a+b) = r_n(b+a) = b \underset{n}{\oplus} a$$

Isso prova a comutatividade da operação $\underset{n}{\oplus}$ sobre $\mathbb{Z}_n$.

É evidente que $0 \in \mathbb{Z}_n$ é o elemento neutro, relativamente a operação $\underset{n}{\oplus}$, pois $a \underset{n}{\oplus} 0 = r_n(a+0) = r_n(a) = a$, donde concluímos pela comutatividade da operação, que $a \underset{n}{\oplus} 0 = a = 0 \underset{n}{\oplus} a$.

Por fim, para mostrar que todo elemento de $a \in \mathbb{Z}_n$ é simetrizável (admite inverso aditivo), analisaremos dois casos:

1º Caso: $a = 0$. Neste caso, $a \underset{n}{\oplus} a = 0 \underset{n}{\oplus} 0 = r_n(0+0) = r_n(0) = 0$. Logo, $0 \in \mathbb{Z}_n$ é simetrizável e seu simétrico é ele próprio, isto é, $-0 = 0$.

2º Caso: $a \in \mathbb{Z}_n - \{0\}$. Neste caso, afirmamos que $-a = n - a$. Inicialmente, precisamos mostrar que $n - a \in \mathbb{Z}_n$, pois por definição, dado um elemento qualquer em um grupo, seu inverso também deve ser um elemento no grupo. Note que, sendo $a \in \mathbb{Z}_n - \{0\}$, então

$$1 \leq a < n \Rightarrow -n < -a \leq -1 \Rightarrow 0 < n - a \leq n - 1 < n$$

Portanto, $n - a \in \mathbb{Z}_n$. Além disso, $(n-a) \underset{n}{\oplus} a = r_n(n-a+a) = r_n(n) = 0$. Pela comutatividade da operação, obtemos $a \underset{n}{\oplus} (n-a) = 0$, o que concluí o segundo caso.

Como provamos que a operação $\underset{n}{\oplus}$ sobre $\mathbb{Z}_n$ é associativa, comutativa, admite elemento neutro e todo elemento é simetrizável, podemos concluir que $(\mathbb{Z}_n, \underset{n}{\oplus})$ é um grupo abeliano.

Exemplo 5. *Dado $n \in \mathbb{N} - \{0\}$. O conjunto $\mathbb{Z}_n^* := \{m : m \in \mathbb{Z}_n \bigwedge mdc(m,n) = 1\}$ com a operação $\underset{n}{\odot}$ é um grupo abeliano.*

A associatividade e comutatividade podem ser provadas de modo análogo ao exemplo anterior, com exceção de que utilizaremos a identidade $r_n(a \cdot b) = r_n(r_n(a) \cdot r_n(b))$, ao invés da identidade para o resto da soma de dois inteiros. Além disso, facilmente prova-se que 1 é o elemento neutro de $\mathbb{Z}_n$ relativamente a operação $\underset{n}{\odot}$. Mostraremos, que todo elemento em $\mathbb{Z}_n^*$ é simetrizável relativamente à operação $\underset{n}{\odot}$.

Seja $m \in \mathbb{Z}_n^*$. Então, $mdc(m,n) = 1$ e assim, pelo Teorema de Bezout, existem $x, y \in \mathbb{Z}$ tais que $mx + ny \overset{(*)}{=} 1$, ou seja, $mx \overset{(**)}{=} n(-y) + 1$ e, portanto, $r_n(mx) = 1$, isto é, $m \underset{n}{\odot} x = 1$. Contudo, não podemos afirmar que x é o simétrico procurado, pois não podemos garantir que $x \in \mathbb{Z}_n^*$.

Pelo algoritmo da divisão, existem $q, r \in \mathbb{Z}$ tais que $x = qn + r$, com $0 \leq r < n$. Logo, $r \in \mathbb{Z}_n$. Daí, substituindo x em $(*)$ e utilizando a recíproca do Teorema de Bezout, obtemos $\mathrm{mdc}(r, a) = 1$. *Logo $r \in \mathbb{Z}_n^*$. Por outro lado,substituindo x em $(**)$, obtemos:*

$$m(qn + r) = n(-y) + 1 \Rightarrow mr = n(-y - mq) + 1 \Rightarrow r_n(mr) = 1$$

Logo, $r \in \mathbb{Z}_n^*$ e $m \underset{n}{\odot} r = 1$. Como a operação é comutativa, obtemos $r \underset{n}{\odot} m = 1$ e, portanto, $m^{-1} = r$, o que conclui a demonstração de que $(\mathbb{Z}_n, \underset{n}{\odot})$ é um grupo abeliano.

Definição 4. *Seja E um conjunto não-vazio. Uma permutação de E é uma bijeção $f : E \longrightarrow E$.*

Exemplo 6. *O conjunto $S(E)$ das permutações de E munido da composição de funções $\circ$ é um grupo.*

Sejam $f, g, h \in S(E)$ e $x \in E$, então

$$\begin{aligned}((f \circ g) \circ h)(x) &= (f \circ g)(h(x)) \\ &= f(g(h(x)) \\ &= f((g \circ h)(x)) \\ &= (f \circ (g \circ h))(x)\end{aligned}$$

Logo, $(f \circ g) \circ h = f \circ (g \circ h)$. Assim, conclui-se que a operação $\circ$ é associativa em $S(E)$.

Seja $Id_E : E \longrightarrow E$ a função identidade, definida por $Id_E(x) = x$, para todo $x \in E$. Sendo uma bijeção, é claro que $Id_E \in S(E)$. Além disso, temos que

$$(Id_E \circ f)(x) = Id_E(f(x)) = f(x) = f(Id_E(x)) = (f \circ Id_E)(x),$$

ou seja, $Id_E \circ f = f = f \circ Id_E$. Isso prova que Id_E é o elemento neutro de $S(E)$ relativamente à composição de funções.

Por fim, seja $f \in S(E)$. Como $f : E \longrightarrow E$ é uma bijeção, existe $f^{-1} : E \longrightarrow E$ que também é uma bijeção, e portanto, $f^{-1} \in S(E)$. Evidentemente, $f \circ f^{-1} = Id_E = f^{-1} \circ f$, donde podemos concluir que todo elemento $f \in S(E)$ é inversível. Logo, $(S(E), \circ)$ é um grupo.

Observação 3. *Se E é finito e possui $n \in \mathbb{N}$ elementos, então $S(E)$ é finito e possui $n!$ elementos.*

Proposição 3. *Se E possuí mais do que dois elementos, $S(E)$ não é abeliano.*

Demonstração. Seja E um conjunto com mais de dois elementos. Então existem $a, b, c \in E$ distintos dois a dois. Considere agora $f, g \in S(E)$,tais que

$$f(x) = \begin{cases} b, & \text{se } x = a \\ c, & \text{se } x = b \\ a, & \text{se } x = c \\ x, & \text{se } x \in E - \{a, b, c\} \end{cases} \quad , \quad g(x) = \begin{cases} a, & \text{se } x = a \\ c, & \text{se } x = b \\ b, & \text{se } x = c \\ x, & \text{se } x \in E - \{a, b, c\} \end{cases}$$

Note que $(f \circ g)(a) = f(g(a)) = f(a) = b$ e $(g \circ f)(a) = g(f(a)) = g(b) = c$. Logo, $f \circ g \neq g \circ f$ e, portanto, $(S(E), \circ)$ não é abeliano, sempre que E possui mais de dois elementos. □

Observação 4. *Quando $E = \{1, 2, ..., n\}$, denotaremos $S(E)$ por S_n e o grupo $(S_n, \circ)$ é chamado de grupo simétrico de grau n. Cada elemento $f \in S_n$é denotado por*

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

Deste modo, sendo $E = \{1, 2, 3\}$, os elementos do grupo S_3 são

$$S_3 = \left\{ \begin{array}{lll} Id_E = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, & f_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, & f_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \\ f_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, & f_4 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, & f_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \end{array} \right\}$$

Exemplo 7. *Seja $\mathcal{F}$ uma figura geométrica. Então, $(S_{\mathcal{F}}, \circ)$ é um grupo, chamado de grupo das simetrias de $\mathcal{F}$.*

Sejam $f, g, h \in S_{\mathcal{F}}$. Já mostramos que $\circ$ está bem definida em $S_{\mathcal{F}}$. Deste modo, $(f \circ g) \circ h, f \circ (g \circ h) \in S_{\mathcal{F}}$. Além disso, como a composição de funções é associativa, ocorre $(f \circ g) \circ h = f \circ (g \circ h)$. Portanto, a operação de composição é associativa no conjunto de simetrias da figura $\mathcal{F}$.

A função $Id_{\mathcal{F}} : \mathcal{F} \longrightarrow \mathcal{F}$ é o elemento neutro de $S_{\mathcal{F}}$ relativamente a operação $\circ$, pois, para todo $f \in S_{\mathcal{F}}$, tem-se $Id_{\mathcal{F}} \circ f = f \circ Id_{\mathcal{F}} = f$.

Por fim, se $f \in S_{\mathcal{F}}$. Então, $f : \mathcal{F} \longrightarrow \mathcal{F}$ é uma bijeção e portanto, $f^{-1} : \mathcal{F} \longrightarrow \mathcal{F}$ está bem definida e é, também, uma bijeção. Além disso, se $P, Q \in \mathcal{F}$, então $f^{-1}(P), f^{-1}(Q) \in \mathcal{F}$. Daí, sendo f uma simetria de $\mathcal{F}$, então

$$\begin{aligned} d(f^{-1}(P), f^{-1}(Q)) &= d\left(f((f^{-1})(P)), f((f^{-1})(Q))\right) \\ &= d\left((f \circ f^{-1})(P), (f \circ f^{-1})(Q)\right) \\ &= d(Id_{\mathcal{F}}(P), Id_{\mathcal{F}}(Q)) \\ &= d(P, Q) \end{aligned}$$

Donde concluímos que $f^{-1} \in S_{\mathcal{F}}$*, e assim,* $(S_{\mathcal{F}}, \circ)$ *é um grupo.*

Exemplo 8. *Seja* $\{G_m\}_{m\in\{1,\cdots,n\}}$ *uma família de conjuntos não vazios. Para cada* $m \in \{1, \cdots, n\}$*, suponha que* $\underset{m}{\cdot}$ *seja uma operação sobre* G_m*. Nestas condições, defina a operação* $\cdot$ *sobre* $(G_1 \times \cdots \times G_n)$*, pondo*

$$(a_1, \cdots, a_n) \cdot (b_1, \cdots, b_n) := (a_1 \underset{1}{\cdot} b_1, \cdots, a_n \underset{n}{\cdot} b_n)$$

Temos: se para todo $m \in \{1, \cdots, n\}$*, o par* $(G_m, \underset{m}{\cdot})$ *for um grupo, então* $(G_1 \times \cdots \times G_n, \cdot)$ *é um grupo.*

Com efeito, sendo $\{G_m\}_{m\in\{1,\cdots,n\}}$ *uma família de grupos, então para cada* $m \in \{1, \cdots, n\}$*, seja* e_m *o elemento neutro em* G_m*. Afirmamos que* $(e_1, \cdots, e_n) \in G_1 \times G_2 \times \cdots \times G_n$ *é o elemento neutro, relativamente a operação definida anteriormente. De fato, se* $\alpha \in G_1 \times G_2 \times \cdots \times G_n$*, para cada* $m \in \{1, \cdots, n\}$*, existe* $a_m \in G_n$*, tal que* $\alpha = (a_1, \cdots, a_n)$*. Daí, temos*

$$(e_1, \cdots, e_n) \cdot \alpha = (e_1 \underset{1}{\cdot} a_1, \cdots, e_n \underset{n}{\cdot} a_n) = (a_1, \cdots, a_n),$$

$$\alpha \cdot (e_1, \cdots, e_n) = (a_1 \underset{1}{\cdot} e_1, \cdots, a_n \underset{n}{\cdot} e_n) = (a_1, \cdots, a_n),$$

$$\therefore (e_1, \cdots, e_n) \cdot \alpha = \alpha = \alpha \cdot (e_1, \cdots, e_n)$$

Além disso, como $\{G_m\}_{m\in\{1,\cdots,n\}}$ *é uma família de grupos, então para cada* $m \in \{1, \cdots, n\}$*, existe um único* $a_m^{-1} \in G_m$*. Logo,* $(a_1^{-1}, \cdots, a_n^{-1}) \in (G_1 \times \cdots \times G_n)$*. Segue-se então que*

$$\begin{aligned} (a_1, \cdots, a_n) \cdot (a_1^{-1}, \cdots, a_n^{-1}) &= (a_1 \underset{1}{\cdot} a_1^{-1}, \cdots, a_n \underset{n}{\cdot} a_n^{-1}) \\ &= (e_1, \cdots, e_n) \end{aligned}$$

De modo análogo, mostra-se que $(a_1^{-1}, \cdots, a_n^{-1}) \cdot (a_1, \cdots, a_n) = (e_1, \cdots, e_n)$*. Portanto,* $\alpha^{-1} = (a_1^{-1}, \cdots, a_n^{-1})$*.*

Agora, tomando $\beta, \gamma \in (G_1 \times \cdots \times G_n)$*, devem existir* $b_m, c_m \in G_m, \forall m \in \{1, \cdots, n\}$*,*

tais que $\beta = (b_1, \cdots, b_n)$ *e* $\gamma = (c_1, \cdots, c_n)$. *Daí*

$$\begin{aligned}
\alpha \cdot (\beta \cdot \gamma) &= (a_1, \cdots, a_2) \cdot (b_1 \underset{1}{\cdot} c_1, \cdots, b_n \underset{n}{\cdot} c_n) \\
&= (a_1 \underset{1}{\cdot} (b_1 \underset{1}{\cdot} c_1), \cdots, a_n \underset{n}{\cdot} (b_n \underset{n}{\cdot} c_n)) \\
&= ((a_1 \underset{1}{\cdot} b_1) \underset{1}{\cdot} c_1), \cdots, (a_n \underset{n}{\cdot} b_n) \underset{n}{\cdot} c_n)), \text{ pela associatividade em } (G_m, \underset{m}{\cdot}), \forall m \in \{1, \cdots, n\} \\
&= (a_1 \underset{1}{\cdot} b_1, \cdots, a_n \underset{n}{\cdot} b_n) \cdot (c_1, \cdots, c_n) \\
&= ((a_1, \cdots, a_n) \cdot (b_1, \cdots, b_n)) \cdot (c_1, \cdots, c_n) \\
&= (\alpha \cdot \beta) \cdot \gamma
\end{aligned}$$

Portanto, $(G_1 \times G_2 \times \cdots \times G_n, \cdot)$ *é um grupo.*

Observação 5. *O grupo do exemplo anterior é chamado de Produto Direto dos grupos* $G_1, G_2, \cdots, G_n$.

2.2 Subgrupos

Nem todo subconjunto de um grupo é, necessariamente, um grupo. No entanto, há subconjuntos que, quando considerados com a mesma operação do grupo ao qual estão contidos, satisfazem as propriedades necessárias para manter a estrutura de grupo, estes são os subgrupos. A noção de subgrupo é particularmente importante, pois facilita a verificação de que um determinado conjunto munido de uma operação é, de fato, um grupo, reduzindo a quantidade de propriedades que precisam ser verificadas, além de possibilitar a obtenção de novos exemplos de grupos a partir de estruturas já conhecidas.

Nesta seção, apresentamos critérios que permitem identificar quando certos subconjuntos de um grupo são, ainda, grupos; bem como exemplos e propriedades fundamentais dos subgrupos. Além disso, abordamos o processo de construção de novos grupos a partir de subconjuntos quaisquer de um grupo, por meio da noção de grupo gerado por um subconjunto. Esse conceito é central neste trabalho, uma vez que nosso Teorema principal, envolve a existência de um grupo desse tipo.

Definição 5. *Sejam* $(G, \cdot)$ *um grupo e* $\emptyset \neq H \subseteq G$. *Dizemos que* H *é um um subgrupo de* G *(e denotamos por* $H \leq G$*), quando, com a operação de* G*, o conjunto* H *é um grupo, isto é, quando as condições seguintes são satisfeitas:*

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

(ii) $(h_1 \cdot h_2) \cdot h_3 = h_1 \cdot (h_2 \cdot h_3)$, *para todo* $h_1, h_2, h_3 \in H$.

(iii) $\exists e_H \in H$ *tal que* $e_H \cdot h = h = e_H \cdot h, \forall h \in H$ *(*e_H *é o elemento neutro de* H*).*

(iv) $\forall h \in H$, *existe* $k \in H$ *tal que* $h \cdot k = e_H = k \cdot h$ *(*k *é o simétrico de* h *em* H*).*

Proposição 4. *(1) Sejam* G *um grupo e* $H \leq G$. *O elemento neutro de* H *é o mesmo de* G.

(2) Dado $h \in H$, o inverso de h em H é igual ao inverso de h em G.

Demonstração. (1) Sejam $e_H \in H, e_G \in G$ respectivamente os elementos neutro de H e de G. Daí, tomando $h \in H$, temos $e_H \cdot h = h$ e $e_G \cdot h = h$

$$\begin{aligned} e_H \cdot h &= e_G \cdot h \\ e_H \cdot h \cdot h^{-1} &= e_G \cdot h \cdot h^{-1} \\ e_H \cdot e_G &= e_G \cdot e_G \\ e_H &= e_G. \end{aligned}$$

(2) Sejam $h_H \in H$ e $h_G \in G$, respectivamente os inversos do elemento $h \in H$ em H e em G. Então,

$$h_H = h_H e_H = h_H e_G = h_H(hh_G) = (h_H h)h_G = e_H h_G = e_G h_G = h_G$$

$$\therefore h_H = h_G.$$

□

Proposição 5. *Sejam $(G, \cdot)$ um grupo e $\emptyset \neq H \subseteq G$. H é um subgrupo de G se, e somente se, valem:*

(1) $e \in H$; onde e é o elemento neutro de G.

(2) Se $a, b \in H$, então $ab \in H$.

(3) Se $a \in H$, então $a^{-1} \in H$.

Demonstração. ($\Rightarrow$) Se $H \leq G$, pela proposição anterior, valem (1) e (3). Além disso, pela condição (i) da definição de subgrupo, vale (2).

($\Leftarrow$) Agora suponha que valem (1), (2) e (3). Evidentemente, (i), (iii) e (iv) são válidas. Agora, se $a, b, c \in H \subseteq G$, então $a, b, c \in G$. Segue-se pelo fato de G ser um grupo que $(ab)c = a(bc)$. Logo, $H \leq G$. □

Proposição 6. *Sejam $(G, \cdot)$ um grupo com elemento neutro e e $\emptyset \neq H \subseteq G$. Então, $H \leq G$ se, e somente se, valem:*

(1) $e \in H$.

(2) Se $a, b \in H$, então $ab^{-1} \in H$.

Demonstração. ($\Rightarrow$) Suponha que $H \leq G$. Pela proposição anterior, (1) é válido. Agora considere $a, b \in H$. A condição (3) da proposição anterior nos assegura que $b^{-1} \in H$, enquanto que a condição (2) nos garante que $ab^{-1} \in H$.

($\Leftarrow$) Seja $\emptyset \neq H \subseteq G$, tal que as condições (1) e (2) sejam satisfeitas. Dado $c \in H$,como $e \in H$, temos que $c^{-1} = ec^{-1} \in H$. Deste modo, se $a, b \in H$, então $a, b^{-1} \in H$; donde conclui-se que $ab = a(b^{-1})^{-1} \in H$. □

Exemplo 9. *Seja $(G,\cdot)$ um grupo, com elemento neutro e. Então, $\{e\}$ e G são subgrupos de G; tais subgrupos são denominados triviais de G.*

De fato, se $a,b \in \{e\} \subseteq G$,então $a = b = e$. Daí, $ab^{-1} = ee^{-1} = ee = e \in \{e\}$.

Agora, sendo G é um grupo com elemento neutro e; dados $a,b \in G$, sabemos que $ab^{-1} \in G$.

Exemplo 10. *Sejam $n \in \mathbb{Z}$ e $n\mathbb{Z} := \{nz : z \in \mathbb{Z}\}$. Temos que $(n\mathbb{Z},+)$ é subgrupo de $(\mathbb{Z},+)$.*

Por definição, $n\mathbb{Z} \subseteq \mathbb{Z}$ e, como $0 = n \cdot 0$, conclui-se que $0 \in n\mathbb{Z}$. Logo, $n\mathbb{Z} \neq \emptyset$.

Agora se $x,y \in n\mathbb{Z}$, então existem $z_1, z_2 \in \mathbb{Z}$, tais que $x = nz_1$ e $y = nz_2$. Segue-se que $x - y = n(z_1 - z_2) \in n\mathbb{Z}$. Donde concluimos que $n\mathbb{Z} \leq \mathbb{Z}$.

Proposição 7. *Sejam $(G,\cdot)$ um grupo e H um subconjunto de G, não-vazio, finito e fechado relativamente à operação de G . Então, $H \leq G$.*

Demonstração. Sendo $H \neq \emptyset$, existe $h \in H$. Como H é finito, existem $n \in \mathbb{N} - \{0\}$ e $h_1, \cdots, h_n \in H$ distintos, tais que $H = \{h_1, \cdots, h_n\}$.

Como H é fechado relativamente à operação definida em G, temos que $hh_1, \cdots, hh_n \in H$ e, portanto, $\{hh_1, \cdots, hh_n\} \subseteq H$. Além disso, se para alguns $i,j \in \{1,2,\cdots,n\}$ tivermos $hh_i = hh_j$, então $h_i = h_j$. Como $h_1, \cdots, h_n$ são distintos, concluímos que $i = j$. Logo, $\{hh_1, \cdots, hh_n\}$ é um subconjunto de H com n elementos e, portanto, $H = \{hh_1, \cdots, hh_n\}$.

Como $h \in H$, existe $k \in \{1,2,\cdots,n\}$, tal que $h = hh_k$; donde conclui-se que $e = h_k \in H$.

Seja agora $a \in H$. Então, de modo análogo ao exposto anteriormente, podemos concluir que $H = \{ah_1, \cdots, ah_n\}$. Como $e \in H$, então existe $l \in \{1,2,\cdots,n\}$ tal que $e = ah_l$. Pela proposição 2, item (2), $a^{-1} = h_l \in H$.

Portanto, $H \leq G$. □

Exemplo 11. *Sejam $n \in \mathbb{N} - \{0\}$, e o número de Euller (base do logarítmo neperiano) e $\theta \in \mathbb{R}$. Definimos $e^{i\theta} = \cos(\theta) + i\sin(\theta)$. Então,*

(1) $U_n = \left\{ e^{\frac{2k\pi i}{n}} : k \in \{0,1,2,\cdots,n-1\} \right\}$,

(2) $\bigcup_{n\in\mathbb{N}} U_n$;

(3) $S^1 = \{z : z \in \mathbb{C} \wedge |z| = 1\}$

São subgrupos de $(\mathbb{C} - \{0\},\cdot)$, os quais formam, para cada $n \in \mathbb{N} - \{0\}$, a cadeia $U_n \leq \bigcup_{n\in\mathbb{N}} U_n \leq S^1 \leq \mathbb{C} - \{0\}$.

(1) Note que, sendo U_n finito e não-vazio, basta mostrarmos que U_n é fechado, isto é, $x,y \in U_n \Rightarrow xy \in U_n$.

Sejam $x,y \in U_n$. Então, existem $k_1, k_2 \in \{0,1,2,\cdots,n-1\}$, tais que $x = e^{\frac{2k_1\pi i}{n}}$ e

$y = e^{\frac{2k_2\pi i}{n}}$. *Logo,*

$$\begin{aligned} x \cdot y &= e^{\frac{2k_1\pi i}{n}} \cdot e^{\frac{2k_2\pi i}{n}} \\ &= e^{\frac{2(k_1+k_2)\pi i}{n}} \end{aligned}$$

Pelo algoritmo da divisão, existem $q, k \in \mathbb{Z}$, *com* $0 \leq k < n$, *tal que* $k_1 + k_2 = qn + k$. *Assim,*

$$\begin{aligned} x \cdot y &= e^{\frac{2(qn+k)\pi i}{n}} \\ &= e^{2\pi qi} \cdot e^{\frac{2k\pi i}{n}} \end{aligned}$$

Note que $e^{2\pi qi} = \cos(2\pi q) + i\sin(2\pi q) = 1 + 0i = 1$. *Segue-se que* $x \cdot y = e^{\frac{2k\pi i}{n}}$,*com* $k \in \{0, 1, 2, \cdots, n-1\}$ *e, portanto* $x \cdot y \in U_n$. *Logo,* $U_n \leq (\mathbb{C} - \{0\})$.

(2) Seja $U = \bigcup_{n\in\mathbb{N}} U_n$. *Por definição,* $U \subseteq (\mathbb{C} - \{0\})$ *e, sendo* $1 \in \{1\} = U_1 \subseteq U$, *então* $U \neq \emptyset$.

Dado $z \in U$, *existe* $m \in \mathbb{N} - \{0\}$,*tal que* $z \in U_m$. *Como* $U_m \leq (\mathbb{C} - \{0\})$, *então* $z^{-1} \in U_m \subseteq U$. *Logo,* $z^{-1} \in U$.

Agora, sendo $z, w \in U$, *então existem* $m, p \in \mathbb{N} - \{0\}$, *tais que* $z \in U_m$ *e* $w \in U_p$. *Novamente, existem* $k_1 \in \{0, 1, 2, \cdots, m-1\}$ *e* $k_2 \in \{0, 1, 2, \cdots, p-1\}$, *tais que* $z = e^{\frac{2\pi k_1 i}{m}}$ *e* $e^{\frac{2\pi k_2 i}{p}}$. *Daí,*

$$\begin{aligned} z \cdot w &= e^{\frac{2\pi k_1 i}{m}} \cdot e^{\frac{2\pi k_1 i}{p}} \\ &= e^{\frac{2\pi p k_1 i + 2\pi m k_2 i}{mp}} \\ &= e^{\frac{2\pi(pk_1 + mk_2)i}{mp}} \end{aligned}$$

Pelo algoritmo da divisão euclidiana, existem $q, r \in \mathbb{Z}$,*com* $0 \leq r < mp$; *tais que* $pk_1 + mk_2 = q(mk) + r$. *Logo,*

$$\begin{aligned} z \cdot w &= e^{\frac{2\pi(qmp+r)i}{mp}} \\ &= e^{\frac{2\pi qmpi}{mp}} \cdot e^{\frac{2\pi ri}{mp}} \\ &= e^{2\pi qi} \cdot e^{\frac{2\pi ri}{mp}} \\ &= 1 \cdot e^{\frac{2\pi ri}{mp}} \\ &= e^{\frac{2\pi ri}{mp}} \end{aligned}$$

Logo, $z \cdot w \in U_{mp} \subseteq U$, *ou seja,* $z \cdot w \in U$; *o que conclui a prova de que* U *é um subgrupo do grupo multiplicativo dos complexos.*

(3) Por definição, $S^1 \subseteq \mathbb{C} - \{0\}$, *uma vez que* $0 \notin S^1$, *pois* $|0 + 0i| = |0| = 0 \neq 1$. *Além disso,* $|1 + 0i| = |1| = 1$ *e assim,* $1 \in S^1$. *Logo,* $S^1 \neq \emptyset$.

Sejam $z, w \in S^1$, então $|z| = 1$ e $|w| = 1$. Daí, $zw \in \mathbb{C}$ e $|zw| = |z||w| = 1$, logo $zw \in S^1$. Além disso, Temos que

$$1 = z \cdot z^{-1} \Rightarrow 1 = |z \cdot z^{-1}| = |z| \cdot |z^{-1}| = 1 \cdot |z^{-1}| = |z^{-1}|$$

Portanto $S^1 \leq \mathbb{C} - \{0\}$.

Por fim, sabendo que, dado $n \in \mathbb{N} - \{0\}$ e se $z \in U_n$, então existe $k \in \{0, 1, 2, \cdots, n-1\}$, tal que $z = e^{\frac{2\pi ki}{n}} = \cos(\frac{2\pi k}{n}) + \sin(\frac{2\pi k}{n})$. Segue-se que

$$|z| = \sqrt{\cos^2\left(\frac{2\pi k}{n}\right) + \sin^2\left(\frac{2\pi k}{n}\right)} = 1$$

Logo, $z \in S^1$ e, portanto, $U_n \subseteq S^1$. De modo análogo, mostra-se que $\underset{n\in\mathbb{N}}{\cup} U_n \subseteq S^1$. Portanto, temos a seguinte cadeia de subgrupos

$$U_n \leq \underset{n\in\mathbb{N}}{\cup} U_n \leq S^1 \leq \mathbb{C} - \{0\}.$$

Exemplo 12. *Seja $(G, \cdot)$ um grupo. O subconjunto $Z(G) := \{g : g \in G \wedge gx = xg, \forall x \in G\}$ é um subgrupo de G, o qual chamamos de centro de G.*

Seja e o elemento neutro de G. Então, $eg = g = ge, \forall g \in G$. Logo $e \in Z(G)$. Se $h, k \in Z(G)$, então $hx = xh$ e $kx = xk$, para todo x em G. Daí, dado $x \in G$, temos

$$(hk)x = hxk = x(hk)$$

Logo, $hk \in Z(G)$. Também, dado $x \in G$, temos

$$h^{-1}x = h^{-1}(x^{-1})^{-1} = (x^{-1}h)^{-1} \overset{(*)}{=} (hx^{-1})^{-1} = (x^{-1})^{-1}h^{-1} = xh^{-1}$$

Onde a igualdade em $(*)$, decorre de h ser um elemento do centro de G. Deste modo, $h^{-1} \in Z(G)$ e, portanto, $Z(G) \leq G$.

Proposição 8. *Sejam $(G, \cdot)$ um grupo e $\{H_\lambda\}_{\lambda\in L}$ uma família de subgrupos de G. Então, $\underset{\lambda\in L}{\cap} H_\lambda \leq G$.*

Demonstração. Seja e o elemento neutro de G. Então, $e \in H_\lambda, \forall \lambda \in L$, e assim, $e \in \underset{\lambda\in L}{\cap} H_\lambda$. Logo, $\emptyset \neq \underset{\lambda\in L}{\cap} H_\lambda \subseteq G$.

Agora, sejam $x, y \in \underset{\lambda\in L}{\cap} H_\lambda$. Então, $x, y \in H_\lambda, \forall \lambda \in L$. Como $H_\lambda \leq G$, para todo $\lambda \in L$, então $xy^{-1} \in H_\lambda, \forall \lambda \in L$. Logo, $xy^{-1} \in \underset{\lambda\in L}{\cap} H_\lambda$ e, portanto, $\underset{\lambda\in L}{\cap} H_\lambda \leq G$. □

Definição 6. *Sejam $(G, \cdot)$ um grupo, $S \subseteq G$ e $\{H_\lambda\}_{\lambda\in L}$ a família dos subgrupos de G que contêm S. O subgrupo $\underset{\lambda\in L}{\cap} H_\lambda$ é chamado de o subgrupo de G gerado por S, o qual é denotado por $\langle S\rangle$. Isto é, $\langle S\rangle = \underset{\lambda\in L}{\cap} H_\lambda$*

Observação 6. *Quando o conjunto S é finito, digamos, $S = \{a_1, a_2, \cdots, a_n\}$, denotamos o subgrupo $\langle S\rangle$, por $\langle a_1, a_2, \cdots, a_n\rangle$ e dizemos que $\langle a_1, a_2, \cdots, a_n\rangle$ é o subgrupo gerado por $a_1, a_2, \cdots, a_n$.*

Proposição 9. *Seja $S \subseteq G$. Então, o subgrupo gerado por S é o menor subgrupo de G que contém S. Noutras palavras,*

(1) $S \subseteq \langle S\rangle$

(2) Se $H \leq G$ e $S \subseteq H$, então $\langle S\rangle \subseteq H$.

Demonstração. (1) Por definição, $\langle S\rangle = \bigcap_{\lambda\in L} H_\lambda$; onde $S \subseteq H_\lambda, \forall\lambda \in L$. Logo, $S \subseteq \langle S\rangle$.

(2) Suponha que $H \leq G$ e $S \subseteq H$. Como H contém S, temos que $H \in \{H_\lambda\}_{\lambda\in L}$. Logo, existe $\mu \in L$, tal que $H = H_\mu$. Segue-se que $\bigcap_{\lambda\in L} H_\lambda \subseteq H_\mu$, i.e., $\langle S\rangle \subseteq H$. □

Definição 7. *Sejam $(G, \cdot)$ (respectivamente $(G, +)$) um grupo com elemento neutro e e $a \in G$. Definimos, para $n \in \mathbb{N}$:*

$$\begin{cases} a^0 = e \\ a^{n+1} = a^n \cdot a \\ a^{-n} = (a^{-1})^n \end{cases} \qquad \textit{resp.} \qquad \begin{cases} 0 \cdot a = e \\ (n+1)\cdot a = na + a \\ (-n)\cdot a = n \cdot (-a) \end{cases}$$

a^n é chamado de potência de a de expoente n e $n \cdot a$ é chamado de múltiplo de a, segundo o inteiro n.

Observação 7. *As potências e os múltiplos definidos possuem propriedades análogas às potências e os múltiplos de números reais. Por exemplo, se $(G, \cdot)$ (respectivamente, $(G, +)$) é um grupo, $a \in G$ e $m, n \in \mathbb{Z}$,então $a^n \cdot a^m = a^{n+m}$ (resp. $n\cdot a + m\cdot a = (n+m)\cdot a$), etc.*

Teorema 1. *Sejam $(G, \cdot)$ um grupo, $\emptyset \neq S \subseteq G$. Então, temos:*

(1) $\langle\emptyset\rangle = \{e\}$; onde e é o elemento neutro de G.

(2) $\langle S\rangle = \left\{a_1^{k_1} \cdot a_2^{k_2} \cdot \cdots \cdot a_n^{k_n} : n \in \mathbb{N} - \{0\} \wedge a_{i's} \in S \wedge k_{i's} \in \mathbb{Z}\right\}$.

Demonstração. (1) $\{e\}$ é o menor (isto é, está incluído) membro da família de subgrupos de G que contém $\emptyset$. Logo, $\{e\}$é a interseção desta família, ou seja, $\langle\emptyset\rangle = \{e\}$.

(2) Seja $H = \left\{a_1^{k_1} \cdot a_2^{k_2} \cdot \cdots \cdot a_n^{k_n} : n \in \mathbb{N} - \{0\} \wedge a_i \in S \wedge k_i \in \mathbb{Z} \wedge i \in \{1, 2, \cdots, n\}\right\}$. Seja $a \in S$, então $a = a^1$, logo $a \in H$ e, portanto, $S \subseteq H$. Agora vamos mostrar que $H \leq G$ e assim, por meio da proposição 9, concluiremos que $\langle S\rangle \subseteq H$. Com efeito, se $a, b \in H$, então existem $n, m \in \mathbb{N} - \{0\}, a_1, \cdots, a_n, b_1, \cdots, b_m \in S$ e $k_1, \cdots, k_n, r_1, \cdots, r_m \in \mathbb{Z}$, tais que

$$a = a_1^{k_1} a_2^{k_2} \cdots a_n^{k_n} \quad \text{e} \quad b = b_1^{r_1} b_2^{r_2} \cdots b_m^{r_m}$$

Note que, como $-k_1, \cdots, -k_n \in \mathbb{Z}$ e $a_1, \cdots, a_n \in S$, então $a^{-1} = a_n^{-k_n} \cdots a_1^{-k_1} \in H$.

Além disso, H é fechado, pois, fazendo $k_{n+1} := r_1, \cdots, k_{n+m} := r_m$ e também $a_{n+1} := b_1, \cdots, a_{n+m} := b_m$, temos que

$$\begin{aligned} a \cdot b &= a_1^{k_1} a_2^{k_2} \cdots a_n^{k_n} b_1^{r_1} b_2^{r_2} \cdots b_m^{r_m} \\ &= a_1^{k_1} a_2^{k_2} \cdots a_n^{k_n} a_{n+1}^{k_{n+1}} \cdots a_{n+m}^{k_{n+m}} \in H \end{aligned}$$

Logo, H é um subgrupo de G e, portanto, $\langle S \rangle \subseteq H$.

Agora, seja $x \in H$. Então, existem $n \in \mathbb{N} - \{0\}$, $k_1, \cdots, k_n \in \mathbb{Z}$ e $a_1, \cdots, a_n \in S$, tais que $x = a_1^{k1} a_2^{k_2} \cdots a_n^{k_n}$. Note que $a_1 \in S \subseteq \langle S \rangle$. Logo, $a_1 \in \langle S \rangle$. Agora, supondo que $a_1^k \in \langle S \rangle$, para algum $k \in \mathbb{N} - \{0\}$, como $\langle S \rangle$ é fechado relativamente a operação de G, então, $a_1^{k+1} = a_1^k a_1 \in \langle S \rangle$. Logo, $a^k \in \langle S \rangle, \forall k \in \mathbb{N} - \{0\}$. Do fato de $\langle S \rangle$ ser um grupo, concluímos que $a_1^0 = e \in \langle S \rangle$ e $a_1^{-k} \in \langle S \rangle$. Logo, $a_1^k \in S, \forall k \in \mathbb{Z}$. Em particular, $a_1^{k_1} \in \langle S \rangle$. De modo análogo, mostra-se que $a_i^{k_i} \in \langle S \rangle, \forall i \in \{1, 2, \cdots, n\}$. Novamente, como $\langle S \rangle$ é fechado, tem-se que $x = a_1^{k_1} a_2^{k_2} \cdots a_n^{k_n} \in \langle S \rangle$. Logo, $H \subseteq \langle S \rangle$ e, portanto, $H = \langle S \rangle$. □

Observação 8. *Caso G seja um grupo aditivo, tem-se*

$$\langle S \rangle = \{k_1 a_1 + k_2 a_2 + \cdots + k_n a_n : n \in \mathbb{N} - \{0\} \wedge a_i \in S \wedge k_i \in \mathbb{Z} \wedge i \in \{1, 2, \cdots, n\}\}.$$

Definição 8. *Seja G um grupo. Dizemos que G é cíclico, se existe $g \in G$ tal que $G = \langle g \rangle$.*

Observação 9. *No caso de grupos multiplicativos, tem-se $\langle g \rangle = \{g^k : k \in \mathbb{Z}\}$, enquanto que para grupos aditivos, tem-se $\langle g \rangle = \{kg : k \in \mathbb{Z}\}$.*

Exemplo 13. *$\mathbb{Z}$, $\mathbb{Z}_n$ e U_n são grupos cíclicos.*

De fato, Seja $1 \in \mathbb{Z}$. Então

$$\langle 1 \rangle = \{1 \cdot z : z \in \mathbb{Z}\} = \{z : z \in \mathbb{Z}\} = \mathbb{Z}$$

Agora, tomando $1 \in \mathbb{Z}_n$, temos $\langle 1 \rangle = \{1 \cdot z : z \in \mathbb{Z}\}$. Precisamos mostrar que $1 \cdot z = r_n(z), \forall z \in \mathbb{Z}$, para assim, concluirmos que

$$\langle 1 \rangle = \{1 \cdot z : z \in \mathbb{Z}\} = \{r_n(z) : z \in \mathbb{Z}\} = \{0, 1, 2, \cdots, n-1\} = \mathbb{Z}_n$$

Inicialmente, mostraremos que, se $a \in \mathbb{Z}_n$, então $k \cdot a = r_n(k \cdot a), \forall k \in \mathbb{N}$. Note que, por definição de múltiplo, temos que $0 \cdot a = 0 = r_n(0 \cdot a)$. Além disso, se supormos que $k \cdot a = r_n(k \cdot a)$, para algum $k \in \mathbb{N}$, então

$$(k+1) \cdot a = k \cdot a \underset{n}{\oplus} a = r_n(k \cdot a) \underset{n}{\oplus} a = r_n(r_n(k \cdot a) + a) = r_n(k \cdot a + a) = r_n((k+1) \cdot a)$$

Pelo princípio de indução, concluímos que $k \cdot a = r_n(k \cdot a), \forall k \in \mathbb{N}$.

Deste modo, dado $1 \in \mathbb{Z}_n$, *então* $0 \cdot 1 = 0 = r_n(0)$. *Supondo que* $k \cdot 1 = r_n(k)$, *para algum* $k \in \mathbb{N}$, *então*

$$(k+1) \cdot 1 = k \cdot 1 \underset{n}{\oplus} 1 = r_n(k) \underset{n}{\oplus} 1 = r_n(r_n(k)+1) = r_n(r_n(k)+r_n(1)) = r_n(k+1)$$

Novamente, pelo princípio de indução, concluímos que $1 \cdot z = r_n(z), \forall z \in \mathbb{N}$. *Daí, tomando* $z \in \mathbb{N} - \{0\}$, *então*

$$(-k)\cdot 1 = k\cdot(-1) \overset{(1)}{=} k\cdot(n-1) \overset{(2)}{=} r_n(k\cdot(n-1)) = r_n(kn-k) = r_n(r_n(kn)+r_n(-k)) = r_n(-k)$$

onde a igualdade (1) *vem do fato de* $n-1$ *ser o inverso de* 1 *em* $\mathbb{Z}_n$, *enquanto que a igualdade* (2), *decorre do que mostramos inicialmente nesse exemplo. Logo, obtemos que* $k \cdot 1 = r_n(k), \forall k \in \mathbb{Z}$ *e, portanto,* $\langle 1 \rangle = \mathbb{Z}_n$.

Por fim, sendo $e^{\frac{2\pi i}{n}} \in U_n$, *então*

$$\begin{aligned}
\langle e^{\frac{2\pi i}{n}} \rangle &= \left\{ \left(e^{\frac{2\pi i}{n}}\right)^z : z \in \mathbb{Z} \right\} \\
&= \left\{ \left(e^{\frac{2\pi i}{n}}\right)^0, \left(e^{\frac{2\pi i}{n}}\right)^1, \left(e^{\frac{2\pi i}{n}}\right)^2, \left(e^{\frac{2\pi i}{n}}\right)^3, \cdots, \left(e^{\frac{2\pi i}{n}}\right)^{n-1} \right\} \\
&= \left\{ 1, e^{\frac{2\pi i}{n}}, e^{\frac{4\pi i}{n}}, e^{\frac{6\pi i}{n}}, \cdots, e^{\frac{2(n-1)\pi i}{n}} \right\} \\
&= U_n
\end{aligned}$$

Proposição 10. *Se* G *é cíclico, então* G *é abeliano.*

Demonstração. Seja G um grupo cíclico gerado por $g \in G$. Se $x, y \in G$, então existem $k_1, k_2 \in \mathbb{Z}$, tais que $x = g^{k_1}$ e $y = g^{k_2}$. Daí,

$$xy = g^{k_1}g^{k_2} = g^{k_1+k_2} = g^{k_2+k_1} = g^{k_2}g^{k_1} = yx$$

Portanto, G é abeliano. □

Proposição 11. *Se* G *é cíclico e* $H \leq G$, *então* H *é cíclico.*

Demonstração. Sejam G um grupo, H um subgrupo de G e $a \in G$, tal que $G = \langle a \rangle$.

1º Caso: $H = \{e\}$. Neste caso, $\langle e \rangle = \{e^q : q \in \mathbb{Z}\} = \{e\} = H$. Logo, H é cíclico.

2º Caso: $H \neq \{e\}$. Então, existe $h \in H$ tal que $h \neq e$. Como $H \subseteq G = \langle a \rangle$, existe $k \in \mathbb{Z}$ de modo que $h = a^k$. Daí, sendo $H \leq G$, temos que $h^{-1} = a^{-k} \in H$. Logo, $k > 0$ ou $-k > 0$.

Seja $A = \{m : m \in \mathbb{N} - \{0\} \ \wedge a^m \in H\}$. Por definição, $A \subseteq \mathbb{N}$. Além disso, $A \neq \emptyset$, uma vez que $k \in A \vee -k \in A$. Segue-se pelo Princípio da Boa Ordenação que A possui um menor elemento, seja $m = \min A$. Vamos mostrar que $H = \langle a^m \rangle$.

Com efeito, como $a^m \in H$, concluímos que $\langle a^m \rangle \subseteq H$.

Agora, se $x \in H$, então $x = a^t$ para algum $t \in \mathbb{Z}$. Pelo algoritmo da divisão, existem $q, r \in \mathbb{Z}$ tais que $t = mq + r$, com $0 \leq r < m$. Daí, $x = a^{mq+r} = a^{mq}a^r$, isto é, $a^r = (a^m)^{-q}x$, donde concluímos que $a^r \in H$, pois $(a^m)^{-q} \in \langle a^m \rangle \subseteq H$ e $x \in H$. Segue-se pelo fato de m ser mínimo, que $r = 0$. Deste modo, $x = (a^m)^q \in \langle a^m \rangle$ e, portanto $H = \langle a^m \rangle$. □

Definição 9. *Sejam $(G, \cdot)$ um grupo e $g \in G$.*

(1) A ordem de G é o número de elementos de G, o qual denotamos por $|G|$.

(2) A ordem de g é a ordem do subgrupo $\langle g \rangle$. Denotamos a ordem de g por $o(g)$.

Quando G é infinito , dizemos que a ordem é infinita e escrevemos $|G| = \infty$.

Exemplo 14. *Temos que $|\mathbb{Z}| = \infty$, $|\mathbb{Z}_n| = n$, e $|S_n| = n!$.*

Teorema 2. *Seja $G = \langle g \rangle$ um grupo cíclico, então são equivalentes*

(1) $o(g) < \infty$ (i.e., $o(g)$ é finita).

(2) Existe $t \in \mathbb{N} - \{0\}$ tal que $g^t = e$.

Demonstração. (1) ($\Rightarrow$) (2) Seja $G = \langle g \rangle$; com $o(g) < \infty$. Note que $e = g^0, g^1, g^2, \cdots, g^n, \cdots \in G$. Sendo um grupo finito, as potências anteriores não podem ser todas distintas. Logo, existem $r, s \in \mathbb{N}$ com $r \neq s$, tais que $g^r = g^s$. Sem perda de generalidade, suponha que $r < s$. Então, de $g^r = g^s$, temos $g^{s-r} = e$. Pondo $t = s - r$, temos $g^t = e$; com $t \geq 1$.

(2) ($\Leftarrow$) (1) Suponhamos que existe $t \in \mathbb{N} - \{0\}$ tal que $g^t = e$. Dado $x \in \langle g \rangle$, existe $k \in \mathbb{Z}$ tal que $x = g^k$. Pelo algoritmo da divisão, existem $q, r \in \mathbb{Z}$ tais que $k = qt + r$, com $0 \leq r < t$. Daí,

$$x = g^k = \left(g^t\right)^q g^r = eg^r = g^r$$

Mas $0 \leq r < t$, logo $g^r \in \{e, g, \cdots, g^{t-1}\}$. Segue-se que $G \subseteq \{e, g, \cdots, g^{t-1}\}$ e, portanto, $G = \langle g \rangle$ é finito. Logo, $o(g) < \infty$. □

Observação 10. *Note que a contrapositiva do Teorema anterior nos diz que, quando $G = \langle a \rangle$ tem ordem infinita, $g^t = 0$ se, e somente se, $t = 0$.*

Teorema 3. *Sejam $(G, \cdot)$ um grupo, $g \in G$. Se $G = \langle g \rangle$ e $o(g) = n$,então*

(i) $G = \{e, g, g^2, \cdots, g^{n-1}\}$ e $g^n = e$.

(ii) Se $m \in \mathbb{Z}$, então $g^m = e$ se, e somente se $n|m$.

Demonstração. (i) Suponhamos que $g \in G$ é tal que $o(g) = n \in \mathbb{N} - \{0\}$. Então, pelo teorema anterior, existe $t \in \mathbb{N} - \{0\}$,tal que $g^t = e$. Considere o conjunto $S = \{m : m \in \mathbb{N} - \{0\} \wedge g^m = e\} \subseteq \mathbb{N}$. Evidentemente, $S \neq \emptyset$, uma vez que $t \in S$. Logo, pelo princípio da boa ordenação, existe $k \in S$ tal que $k = \min S$. Como consequência, temos que $g^k = e$ e, se $m \in \mathbb{N} - \{0\}$ e $m < k$, então $g^m \neq e$.

Segue-se que, se $g^i = g^j$, para certos $i, j \in \{0, 1, 2, \cdots, k-1\}$, então $g^{|i-j|} = e$. Donde concluímos que $|i - j| = 0$,isto é, $i = j$. Portanto, $e = g^0, g, g^2, \cdots, g^{k-1}$ são distintos, ou

seja, $\left\{e = g^0, g, g^2, \cdots, g^{k-1}\right\}$ é finito com k elementos. Como $\left\{e = g^0, g, g^2, \cdots, g^{k-1}\right\} \subseteq G$, então $k \leq n$.

Agora se $x \in G$, então $x = g^m$, para algum $m \in \mathbb{Z}$. Pelo algoritmo da divisão euclidiana, existem $p, l \in \mathbb{Z}$ tais que $m = pk + l$, com $0 \leq l < k$. Daí,

$$x = g^m = \left(g^k\right)^p g^l = eg^l = g^l$$

Como $0 \leq l < k$, temos que $g^l \in \left\{e, g, g^2, \cdots, g^{k-1}\right\}$, ou seja, $G \subseteq \left\{e, g, g^2, \cdots, g^{k-1}\right\}$. Logo, $n \leq k$ e, portanto, $n = k$. Segue-se que $g^n = g^k$,, isto é, $g^n = e$. Também $G = \left\{e = g^0, g, g^2, \cdots, g^{k-1}\right\} = \{e = g^0, g, g^2, \cdots, g^{n-1}\}$,o que concluí a demonstração.

(ii) $(\Rightarrow)$ Suponha que $m \in \mathbb{Z}$ e $g^m = e$. Pelo algoritmo da divisão, existem $q, r \in \mathbb{Z}$ tais que $m = nq + r$, com $0 \leq r < n$. Daí, temos que $g^r \in \{e = g^0, g, g^2, \cdots, g^{n-1}\}$ e além disso,

$$e = g^m = (g^n)^q g^r = eg^r = g^r$$

Como $0 \leq r < m$, devemos ter $r = 0$ e portanto, $m = nq$, isto é, $m|n$.

$(\Leftarrow)$ Suponha que $m \in \mathbb{Z}$ e $n|m$. Então, existe $q \in \mathbb{Z}$ tal que $m = nq$. Segue-se que $g^m = (g^n)^q = e$. □

Observação 11. *Da prova do teorema 3, segue-se que, se g é um elemento de ordem finita de um grupo G, então $o(g) = min\left\{k : k \in \mathbb{N} - \{0\} \wedge g^k = e\right\}$.*

Definição 10. *Se G é um grupo. O subgrupo $\langle\{xyx^{-1}y^{-1} : x, y \in G\}\rangle$ é chamado de o subgrupo dos comutadores do grupo G; ele será denotado por G'.*

Proposição 12. *G é abeliano se, e somente se, $G' = \{e\}$.*

Demonstração. $(\Rightarrow)$ Suponha que G é abeliano. Então $G' = \langle\{xyx^{-1}y^{-1} : x, y \in G\}\rangle = \langle\{xx^{-1}yy^{-1} : x, y \in G\}\rangle = \langle\{e : x, y \in G\}\rangle = \{e\}$.

$(\Leftarrow)$ Reciprocamente, suponha que $G' = \{e\}$. Daí, se $x, y \in G$, então $xyx^{-1}y^{-1} = e$, e daí, $xy = yx$. Logo, G é abeliano. □

Proposição 13. *Seja G um grupo e seja $\alpha \in G - \{e\}$. Então*

(1) $o(\alpha) = 2 \iff \alpha = \alpha^{-1}$.

(2) $o(\alpha) = mn \Rightarrow o(\alpha^m) = n$.

(3) $o(\alpha^{-1}) = o(\alpha)$,

(4) Se $o(\beta) = 2, \forall \beta \in G - \{e\}$, então G é abeliano.

Demonstração. (1) $(\Rightarrow)$ Suponha que $o(\alpha) = 2$. Então, $\alpha^2 = e \Rightarrow \alpha^2\alpha^{-1} = e\alpha^{-1} \Rightarrow \alpha = \alpha^{-1}$.

$(\Leftarrow)$ Se $\alpha \in G - \{e\}$, então $o(\alpha) \neq 1$. Suponha que $\alpha = \alpha^{-1}$. Então, $\alpha^2 = \alpha\alpha^{-1}$,i.e., $\alpha^2 = e$. Logo, $o(\alpha) = 2$.

(2) Suponha agora que $o(\alpha) = mn$. Note que $(\alpha^m)^n = \alpha^{mn} = e$. Portanto, basta mostrar que mn é o menor natural não nulo com essa propriedade. Note que, se $t \in \mathbb{N} - \{0\}$ e $t < n$, então $mt < mn = o(\alpha)$. Logo, $(\alpha^m)^t = \alpha^{mt} \neq e$. Portanto, $o(\alpha^m) = n$.

(3) Seja $\alpha \in G - \{e\}$ um elemento de ordem $n \in \mathbb{N} - \{0\}$, então $\alpha^n = e$. Daí, $(\alpha^{-1})^n = (\alpha^n)^{-1} = e^{-1} = e$. Deste modo, se $k \in \mathbb{N} - \{0\}$, é tal que $k < n$ $(\alpha^{-1})^k = e$, então teríamos $\alpha^k = \left((\alpha^{-1})^k\right)^{-1} = e^{-1} = e$, uma contradição, uma vez que $o(\alpha) = n$. Portanto, $o(\alpha^{-1}) = n$, i.e., $o(\alpha^{-1}) = o(\alpha)$.

(4) Suponha que G é um grupo tal que $o(\beta) = 2, \forall \beta \in G - \{e\}$. Se $x, y \in G - \{e\}$, então $x^2 = y^2 = e$. Como $xy \in G$, também $(xy)^2 = e$. Daí,

$$xy = (xy)e = (xy)\,(yxyx) = (xyyx)(yx) = (xex)(yx) = (xx)(yx) = e(yx) = yx$$

$$\therefore xy = yx$$

Logo, G é abeliano. □

2.3 Classes Laterais e o Teorema de Lagrange

O estudo das classes laterais e do Teorema de Lagrange é fundamental para a compreensão da estrutura de grupos finitos, pois permite estabelecer uma relação entre a ordem de um grupo e a ordem de seus subgrupos. As classes laterais podem ser interpretadas como classes de equivalência, o que conduz naturalmente a uma partição do grupo, fornecendo o suporte necessário para a enunciação e demonstração do Teorema de Lagrange. Nesta seção, definimos as classes laterais, apresentamos algumas de suas propriedades básicas e discutimos algumas consequências do Teorema de Lagrange.

Definição 11. *Sejam $(G, \cdot)$ um grupo e H um subgrupo de G. Para cada elemento $g \in G$, chama-se classe lateral à esquerda (respectivamente à direita) de H determinada por g o conjunto*

$$g \cdot H = \{gh : h \in H\} \qquad (\text{resp. } H \cdot g = \{hg : h \in H\})$$

Observação 12. *Desde que não haja confusão, representaremos $g \cdot H$ e $H \cdot g$ respectivamente por gH e Hg.*

Definição 12. *Sejam $(G, \cdot)$ um grupo, H um subgrupo de G e $a, b \in G$. Dizemos que a é côngruo à esquerda a b módulo H (e escrevemos $a \underset{E}{\equiv} b \pmod{H}$) se $a^{-1}b \in H$.*

Observação 13. *De modo análogo, diz-se que a é côngruo à direita a b módulo H, quando $ab^{-1} \in H$.*

Proposição 14. *Sejam G um grupo e H um subgrupo de G. Então $\underset{E}{\equiv} \pmod{H}$ é uma relação de equivalência sobre G.*

Demonstração. Seja e o elemento neutro de G.

(1) Dado $a \in G$, temos que $a^{-1}a = e \in H$. Logo, por definição, $a \underset{E}{\equiv} a \pmod{H}$.

(2) Dados $a, b \in G$, suponhamos que $a \underset{E}{\equiv} b \pmod{H}$. Então, $a^{-1}b \in H$. Como $H \leq G$,$(a^{-1}b)^{-1} \in H$, isto é, $b^{-1}a \in H$. Logo, $b \underset{E}{\equiv} a \pmod{H}$.

(3) Suponhamos que $a, b, c \in G$, são tais que $a \underset{E}{\equiv} b \pmod{H}$ e $b \underset{E}{\equiv} c \pmod{H}$. Então, $a^{-1}b, b^{-1}c \in H$. Segue-se pelo de fato de H ser subgrupo de G que $(a^{-1}b)(b^{-1}c) \in H$, isto é, $a^{-1}c \in H$. Logo, $a \underset{E}{\equiv} c \pmod{H}$.

Portanto, de (1), (2) e (3), concluímos que $\underset{E}{\equiv} \pmod{H}$ é uma relação de equivalência sobre G. □

Exemplo 15. *Sejam G um grupo com elemento neutro e e $H = \{e\}$. Então, dados $a, b \in G$, temos*

(1) $a \underset{E}{\equiv} b \pmod{H} \iff a^{-1}b \in H = \{e\} \iff a = b$

Ou seja, a relação $\underset{E}{\equiv} \pmod{H}$ *coincide com a relação de igualdade sobre G.*

Exemplo 16. *Sejam $\mathbb{Z}$ o grupo dos números inteiros, $n \in \mathbb{N} - \{0\}$ e $H = n\mathbb{Z}$. Dados $a, b \in \mathbb{Z}$ temos*

$$\begin{aligned} a \underset{E}{\equiv} b \pmod{n\mathbb{Z}} &\iff -a + b \in H = n\mathbb{Z} \\ &\iff \exists q \in n\mathbb{Z}, b - a = nq \\ &\iff n | b - a \\ &\iff a \equiv b \ (mod\ n) \end{aligned}$$

Neste caso, a relação $\underset{E}{\equiv} \pmod{n\mathbb{Z}}$ *coincide com a relação de congruência módulo n sobre $\mathbb{Z}$.*

Definição 13. *Sejam $(G, \cdot)$ um grupo, $H \leq G$ e $a \in G$. O conjunto*

$$\bar{a} = \left\{ x : x \in G \wedge x \underset{E}{\equiv} a \pmod{H} \right\}$$

é chamado de classe de equivalência à esquerda determinada por a.

Enquanto que o conjunto

$$G/H = \{\bar{a} : a \in G\}$$

é chamado de conjunto quociente de G por H segundo a relação $\underset{E}{\equiv} \pmod{H}$.

Proposição 15. *Sejam $(G, \cdot)$ um grupo, H um subgrupo de G. A classe de equivalência determinada por um elemento $a \in G$ coincide com a classe lateral à esquerda determinada por esse mesmo elemento, isto é, $\bar{a} = aH, \forall a \in G$.*

Demonstração. Seja $a \in G$. Observe que

$$x \in \bar{a} \iff x \underset{E}{\equiv} a \pmod{H} \iff a^{-1}x \in H \iff \exists h \in H, a^{-1}x = h \iff x = ah \iff x \in aH$$

Portanto, $\bar{a} = aH, \forall a \in G$. □

Teorema 4. *Sejam G um grupo, $H \leq G$ e $a, b \in G$. Então:*

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

(2) H, aH e Ha possuem a mesma quantidade de elementos.

(3) G/H é uma partição de G.

Demonstração. (1) ($\Rightarrow$) Suponhamos que $aH = bH$. Observe que $b = b \cdot e$, logo, $b \in bH = aH$. Daí, $b \in aH$ e então, existe $h \in H$ tal que $b = ah$, o que implica $a^{-1}b = h \in H$, isto é, $a^{-1}b \in H$.

($\Leftarrow$) Suponhamos agora que $a^{-1}b \in H$, então $a^{-1}b = h_1$, para algum $h_1 \in H$. Assim, podemos escrever $a = bh_1^{-1}$. Agora, se $x \in aH$, então $x = ah_2$, para algum $h_2 \in H$.

Note que $x = ah_2 = (bh_1^{-1})h_2 = b(h_1^{-1}h_2)$. Como H é subgrupo de G, temos que $h_1^{-1}h_2 \in H$ e, portanto, $b(h_1^{-1}h_2) \in bH$, isto é, $x \in bH$. Logo, $aH \subseteq bH$. Analogamente, mostra-se que $bH \subseteq aH$. Assim, podemos concluir que $aH = bH$.

(2) Recordemos que, dois conjuntos possuem a mesma quantidade de elementos quando é possível estabelecer uma bijeção entre eles. Deste modo, para provar o desejado, vamos mostrar que as funções abaixo são bijetivas.

$$\begin{array}{rcl} f : H & \longrightarrow & aH \\ h & \longmapsto & f(h) = ah \end{array} \qquad \begin{array}{rcl} g : H & \longrightarrow & Ha \\ h & \longmapsto & f(h) = ha \end{array}$$

Sejam $h_1, h_2 \in H$ tais que $f(h_1) = f(h_2)$, isto é, $ah_1 = ah_2$. Então,

$$ah_1 = ah_2 \Rightarrow a^{-1}ah_1 = a^{-1}ah_2 \Rightarrow h_1 = h_2$$

Logo, f é injetiva. Além disso,

$$Im(f) = \{f(h) : h \in H\} = \{ah : h \in H\} = aH$$

O que mostra a sobrejetividade de f. Portanto, f é uma bijeção. De modo análogo, pode-se mostrar que g é bijetiva.

Portanto, H, aH e Ha tem a mesma quantidade de elementos.

(3) Mostraremos que G/H é uma partição de G. Dado $\alpha \in G/H$, então existe $x \in G$ tal que $\alpha = xH$. Na prova do item (1), vimos que $x \in xH = \alpha$. Logo, $\alpha \neq \emptyset$.

Precisamos mostrar que, se $\alpha, \beta \in G/H$ são tais que $\alpha \neq \beta$, então $\alpha \cap \beta = \emptyset$, ou seja, se $\alpha \cap \beta \neq \emptyset$, então $\alpha = \beta$.

Sejam $\alpha, \beta \in G/H$ tais que $\alpha \cap \beta \neq \emptyset$. Logo, existe $c \in \alpha \cap \beta$, isto é, $c \in \alpha \wedge c \in \beta$. Também existem $a, b \in G$ tais que $\alpha = aH, \beta = bH$. Como $c \in aH$ e $c \in bH$, existem $h_1, h_2 \in H$ tais que $c = ah_1$ e $c = bh_2$. Daí, $e = cc^{-1} = (ah_1)(bh_2)^{-1} = ah_1h_2^{-1}b^{-1}$. Logo, $a^{-1}b = h_1h_2^{-1} \in H$, isto é, $a^{-1}b \in H$. Pelo item (1), $aH = bH$, ou seja, $\alpha = \beta$.

Além disso, para cada $x \in G$, temos $x \in xH \subseteq G \Rightarrow \{x\} \subseteq xH \subseteq G$. Daí,

$$G = \bigcup_{x \in G} \{x\} \subseteq \bigcup_{x \in G} xH \subseteq G \Rightarrow \bigcup_{x \in G} xH = G$$

Portanto, G/H é uma partição de G.

□

Definição 14. *Sejam G um grupo, H um subgrupo de G. Então, chama-se índice de H em G ao cardinal do conjunto G/H. Denotamos este cardinal por $(G : H)$.*

Teorema 5 (Teorema de Lagrange)**.** *Sejam G um grupo finito e H um subgrupo de G, então, a ordem de H divide a ordem de G. Também, o índice de H em G divide a ordem de G.*

Demonstração. Sendo G finito, então o conjunto das partes de G, o qual denotamos por $P(G)$ é finito. Como $G/H \subseteq P(G)$, então G/H é finito. Logo, existem $r \in \mathbb{N}$ e $a_1, a_2, \cdots, a_r \in G$ distintos, com $a_i H \cap a_j H = \emptyset$, para todos $i, j \in \{1, 2, \cdots, r\}$ e $i \neq j$; tais que $G/H = \{a_1 H, a_2 H, \cdots, a_r H\}$. Segue-se que

$$\dot{\bigcup_{i=1}^{r}} a_i H = G \Rightarrow \Big|\dot{\bigcup_{i=1}^{r}} a_i H\Big| = \big|G\big|$$

Como a união é disjunta, segue-se

$$\sum_{i=0}^{r} \big|a_i H\big| = \big|G\big| \Rightarrow r\big|H\big| = \big|G\big|$$

Como $r = (G : H)$, concluímos que $|H|\big||G|$ e $(G : H)\big||G|$. □

Corolário 1. *Sejam G um grupo finito e $g \in G$. Então, $o(g)\big||G|$.*

Demonstração. Seja $g \in G$, então $\langle g \rangle$ é um subgrupo de G. Pelo teorema de Lagrange, $|\langle g \rangle|\big||G|$,isto é, $o(g)\big||G|$. □

Corolário 2. *Seja $p \in \mathbb{N}$ um número primo e $a \in \mathbb{Z}$ tal que $mdc(a, p) = 1$. Então, $a^{p-1} \equiv 1 \pmod{p}$.*

Demonstração. Sabemos que $\mathbb{Z}_p^* = \{m : m \in \mathbb{Z}_p \wedge \text{mdc}(m, p) = 1\} = \{1, 2, \cdots, p-1\}$, logo, $|\mathbb{Z}_p^*| = p - 1$.

Dado $a \in \mathbb{Z}$, existem $q, r \in \mathbb{Z}$ tais que $a = qp + r$, com $0 \leq r < p$. Logo, $a \equiv r \pmod{p}$. Note que, se $r = 0$, teríamos que $p|a$ e assim, $\text{mdc}(a, p) \neq 1$, um absurdo. Logo, $r \neq 0$ e, portanto, $r \in \mathbb{Z}_p^*$. Segue-se que $r^{|\mathbb{Z}_p^*|} = 1$, ou seja $r^{p-1} = 1$. Mais precisamente, $r_p(r^{p-1}) = 1$, donde concluímos que $r^{p-1} \equiv 1 \pmod{p}$.

Por fim, pela transitividade da congruência módulo p, concluímos que $a^{p-1} \equiv r^{p-1} \equiv 1 \pmod{p}$, ou seja, $a^{p-1} \equiv 1 \pmod{p}$. □

Corolário 3. *Todo grupo finito de ordem prima é cíclico.*

Demonstração. Seja G um grupo finito de ordem p prima. Então, $G \neq \{e\}$. Logo, existe $g \in G - \{e\}$. Pelo corolário 1 do Teorema de Lagrange, $o(g)\big||G|$, isto é, $o(g)\big|p$. Como p é primo, então $o(g) = 1$ ou $o(g) = p$, mas, sendo $g \neq e$, concluímos que $o(g) = p$. Segue-se que $G = \langle g \rangle$. Portanto, G é cíclico. □

Proposição 16. *Seja G um grupo abeliano. Se $a, b \in G$ são dois elementos de ordem finita, tais que $mdc(o(a), o(b)) = 1$,então $o(ab) = o(a)o(b)$.*

Demonstração. Sejam $n = o(a), m = o(b)$ e $t = o(ab)$. Como a e b comutam (pois G é abeliano), temos $(ab)^{nm} = (a^n)^m(b^m)^n = e$. Assim, $t\big|nm$. Novamente, pelo fato de a e b comutarem, temos que $e = (ab)^t = a^t b^t$, isto é, $a^t = b^{-t} \in \langle a \rangle \cap \langle b \rangle$.

Note que, se $x \in \langle a \rangle \cap \langle b \rangle$, pelo corolário 1 do teorema de Lagrange, $o(x)\big||\langle a \rangle|$ e $o(x)\big|\langle b \rangle$, i.e., $o(x)\big|n$ e $o(x)\big|m$, logo, $o(x)\big|\text{mdc}(n, m) = 1$. Portanto, $o(x) = 1$.

Assim, podemos concluir que $\langle a \rangle \cap \langle b \rangle = \{e\}$; ou seja, $a^t = e$ e $b^t = e$. Logo, $n\big|t \wedge m\big|t$. Como $\text{mdc}(m, n) = 1$, então $nm\big|t$. Portanto, $t = nm$, ou seja, $o(ab) = o(a)o(b)$. □

2.4 Subgrupos Normais e Grupos Quocientes

Seja $(G, \cdot)$ um grupo e $H \leq G$. Nosso intuito é descobrir qual (ou quais) propriedades um subgrupo H de G devem possuir, para que a operação de G induza de forma natural uma operação sobre o conjunto das classes laterais à esquerda de H em G, isto é, quais condições H deve possuir para que o seguinte conjunto $\varphi = \{((aH, bH), (ab)H) : a, b \in G\}$ defina uma função de $\left(G/H \times G/H\right)$ em G/H.

Definição 15. *Sejam G um grupo e H um subgrupo de G. Dizemos que H é um subgrupo normal de G (e denotamos por $H \trianglelefteq G$) se, para todo $g \in G$, tem-se $gH = Hg$.*

Proposição 17. *Seja $(G, \cdot)$ um grupo e H um subgrupo de G. Então, são equivalentes:*
(i) φ é um operação sobre G/H.
(ii) $gHg^{-1} := \{ghg^{-1} : h \in H\} \subseteq H, \forall g \in G$.
(iii)$gHg^{-1} = H, \forall g \in G$.
(iv) $gH = Hg, \forall g \in G$.

Demonstração. $(i) \Rightarrow (ii)$ Suponhamos que $\varphi : \left(G/H \times G/H\right) \longrightarrow G/H$ esteja bem definida. Seja $\alpha \in gHg^{-1}$. Então existe $h \in H$ tal que $\alpha = ghg^{-1}$. Note que $\varphi\left((gh)H, g^{-1}H\right) = (ghg^{-1})H$ e $\varphi(gH, g^{-1}H) = eH$, onde e é o elemento neutro de G. Além disso, $gH = (gh)H$, uma vez que $g^{-1}gh = h \in H$. Portanto, sendo φ uma função, $(ghg^{-1})H = eH$. Segue-se então que $e^{-1}(ghg^{-1}) \in H$, isto é, $\alpha \in H$. Logo, $gHg^{-1} \subseteq H, \forall g \in G$.

$(ii) \Rightarrow (iii)$ Suponha que $gHg^{-1} \subseteq H, \forall g \in G$. Isso implica que $g^{-1}Hg \subseteq H, \forall g \in G$. Daí, para todo $g \in G$, temos

$$H = g\left(g^{-1}Hg\right)g^{-1} \subseteq gHg^{-1}.$$

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

$(iii) \Rightarrow (iv)$ Sejam $g \in G$ e $\alpha \in gH$, então existe $h \in H$, tal que $\alpha = gh$. Note que $\alpha g^{-1} = ghg^{-1} \in gHg^{-1} = H$, logo, existe $h \in H$ tal que $h = \alpha g^{-1}$, o que implica $\alpha = hg \in Hg$. Logo, $gH \subseteq Hg$. Procedendo de modo análogo, mostra-se que $Hg \subseteq gH$; o que concluí a prova de que $gH = Hg, \forall g \in G$.

$(iv) \Rightarrow (i)$ Agora, suponha que $gH = Hg, \forall g \in G$. Sejam $\alpha, \beta \in \left(G/H \times G/H\right)$ e $\gamma, \delta \in G/H$, tais que $(\alpha, \gamma), (\beta, \delta) \in \varphi$ e $\alpha = \beta$. Então, existem $a, b, c, d \in G$, tais que $\alpha = (aH, bH)$ e $\beta = (cH, dH)$. Por definição de φ, temos que $\gamma = (ab)H$ e $\delta = (cd)H$. Além disso, da igualdade $\alpha = \beta$, decorre que $cH = aH$ e $dH = bH$, ou seja, $c^{-1}a, d^{-1}b \in H$.

Note que $(cd)^{-1}(ab) = d^{-1}(c^{-1}a)b$, com $(c^{-1}a)b \in Hb = bH$. Logo, existe $h \in H$, tal que $bh = c^{-1}ab$. Daí, como $d^{-1}b, h \in H$, temos que

$$(cd)^{-1}(ab) = (d^{-1}b)h \in H$$

Portanto, $(ab)H = (cd)H$, ou seja, $\gamma = \delta$, donde concluímos que φ é um função de $G/H \times G/H$ em G/H e, portanto, uma operação sobre G/H. □

Observação 14. *Observe que a condição (iv) corresponde precisamente ao critério de normalidade de um subgrupo. Assim, a proposição anterior nos oferece outras três maneiras de verificar quando um subgrupo H é normal em um grupo G.*

Exemplo 17. *Sendo G um grupo com elemento neutro e, os subgrupos $\{e\}, G$ são normais em G.*

De fato, dados $e \in \{e\}, g, h \in G$, tem-se $geg^{-1} = e \in \{e\}$ e $ghg^{-1} \in G$.

Exemplo 18. *Seja G um grupo. Se $H \leq Z(G)$, então $H \trianglelefteq G$. Em particular, $Z(G) \trianglelefteq G$.*

Suponha que $H \leq Z(G)$. Seja $h \in H \subseteq Z(G)$, então $gh = hg, \forall g \in G$. Segue-se que $ghg^{-1} = gg^{-1}h = eh = h \in H$, logo $H \trianglelefteq G$. Como $Z(G) \leq Z(G)$, concluímos que $Z(G) \trianglelefteq G$.

Exemplo 19. *Se G é abeliano e $H \leq G$, então $H \trianglelefteq G$.*

De fato, $gH = \{gh : h \in G\} = \{hg : h \in G\} = Hg$, logo $H \trianglelefteq G$.

Proposição 18. *Sejam $(G, \cdot)$ um grupo e $\emptyset \neq S \subseteq G$. Então, $\langle S\rangle \trianglelefteq G$ se, e somente se, $gsg^{-1} \in \langle S\rangle, \forall g \in G$ e $\forall s \in S$.*

Demonstração. $(\Rightarrow)$ Suponha que $\langle S\rangle \trianglelefteq G$. Por definição, sabemos que $S \subseteq \langle S\rangle$. Daí, se $s \in S$, então $s \in \langle S\rangle$. Portanto, pela hipótese inicial, concluímos que $gsg^{-1} \in \langle S\rangle$.

$(\Leftarrow)$ Sejam $g \in G$ e $x \in \langle S\rangle$, então existem $n \in \mathbb{N} - \{0\}; s_1, s_2, \cdots, s_n \in S$ e $k_1, k_2, \cdots, k_n \in \mathbb{Z}$ tais que $x = s_1^{k_1} s_2^{k_2} \cdots s_n^{k_n}$

Inicialmente, mostraremos que $gs^n g^{-1} = (gsg^{-1})^n, \forall n \in \mathbb{Z}$.

De fato, $gs^0g^{-1} = e = (gsg^{-1})^0$ e, supondo que para algum $n \in \mathbb{N} - \{0\}$, tenha-se $(gsg^{-1})^n = gs^ng^{-1}$, então

$$(gs^ng^{-1})^{n+1} = (gsg^{-1})^n(gsg^{-1}) \overset{H.I.}{=} (gs^ng^{-1})(gsg^{-1}) = gs^nesg^{-1} = gs^{n+1}g^{-1}$$

Pelo princípio de indução, concluímos que $gs^ng^{-1} = (gsg^{-1})^n, \forall n \in \mathbb{N}$. Além disso, temos

$$(gs^{-1}g^{-1}) = (gs^{-1}g^{-1})e = (gs^{-1}g^{-1})\left((gsg^{-1})(gsg^{-1})^{-1}\right) = (gsgg^{-1}sg^{-1})(gsg^{-1})^{-1} = (gsg^{-1})^{-1}$$

Deste modo, se $t \in \mathbb{Z}$ e $t < 0$, então $t = -k$, para algum $k \in \mathbb{N}$. Logo,

$$(gsg^{-1})^t = (gsg^{-1})^{-k} = \left((gsg^{-1})^{-1}\right)^k = (gs^kg^{-1})^{-1} = gs^{-k}g^{-1} = (gs^tg^{-1})$$

Donde concluímos que $gs^ng^{-1} = (gsg^{-1})^n, \forall n \in \mathbb{Z}$. Daí, segue-se que

$$\begin{aligned} gxg^{-1} &= gs_1^{k_1}s_2^{k_2}\cdots s_n^{k_n}g^{-1} \\ &= gs_1^{k_1}es_2^{k_2}e\cdots es_n^{k_n}g^{-1} \\ &= (gs_1^{k_1}g^{-1})(gs_2^{k_2}g^{-1})\cdots(gs_n^{k_n}g^{-1}) \end{aligned}$$

Mas por hipótese, temos que $gsg^{-1} \in \langle S\rangle, \forall g \in G$ e $\forall s \in S$. Logo,

$$\begin{aligned} gxg^{-1} &= (gs_1^{k_1}g^{-1})(gs_2^{k_2}g^{-1})\cdots(gs_n^{k_n}g^{-1}) \\ &= (gs_1g^{-1})^{k_1}(gs_2g^{-1})^{k_2}\cdots(gs_ng^{-1})^{k_n} \end{aligned}$$

Como $(gs_ig^{-1})^{k_i} \in \langle S\rangle, \forall i \in \{1, 2, \cdots, n\}$. Concluí-se que, $gxg^{-1} \in \langle S\rangle$ e, portanto, $\langle S\rangle \trianglelefteq G$. □

Observação 15. *Na demonstração da proposição anterior, precisamos mostrar que, dados $g \in G$ e $s \in S \subseteq G$, ocorre $gs^ng^{-1} = (gsg^{-1})^n, \forall n \in \mathbb{Z}$. Utilizaremos esse fato futuramente.*

Exemplo 20. *Seja G um grupo. Então, $G' \trianglelefteq G$.*

Por definição, $G' = \langle S\rangle$, onde $S := \{xyx^{-1}y^{-1} : x, y \in G\}$. Além disso, já sabemos que $G' \leq G$.

Sejam $g \in G$ e $s \in S$, então existem $x, y \in S$ tais que $s = xyx^{-1}y^{-1}$. Daí,

$$\begin{aligned} gsg^{-1} &= gxyx^{-1}y^{-1}g^{-1} \\ &= gxeyex^{-1}ey^{-1}eg^{-1} \\ &= (gxg^{-1})(gyg^{-1})(gx^{-1}g^{-1})(gy^{-1}g^{-1}) \\ &= (gxg^{-1})(gyg^{-1})(gxg^{-1})^{-1}(gyg^{-1})^{-1} \in S \subseteq \langle S\rangle \end{aligned}$$

Logo, $gsg^{-1} \in \langle S \rangle = G'$. Pela proposição 18, concluímos que $G' \trianglelefteq G$

Exemplo 21. *Sejam $(G, \cdot)$ um grupo e $H \leq G$. Se $(G : H) = 2$, então $H \trianglelefteq G$.*

De fato, sendo $(G : H) = 2$, então $G/H = \{H, G - H\}$. Daí, dado $g \in G$, como G/H é uma partição de G, temos que $g \in H$ ou $g \in G - H$.

1^{o} Caso: $g \in H$. Neste caso, como $H \leq G$, então $g^{-1} \in H$. Consequentemente, $ghg^{-1} \in H, \forall h \in H$. Logo, $gHg^{-1} \subseteq H$.

2^{o} Caso: $g \notin H$. Neste caso, $g \in G - H = gH$. Vamos mostrar que $gHg^{-1} \subseteq H$. Suponha por absurdo que exista $h \in H$, tal que $ghg^{-1} \notin H$. Então, $ghg^{-1} \in gH$. Segue que $ghg^{-1} = gh_0$, para algum $h_0 \in H$. Logo,

$$ghg^{-1} = gh_0 \Rightarrow hg^{-1} = h_0 \in H$$

Como H é um subgrupo de G, então $(hg^{-1})^{-1} \in H$, isto é, $gh^{-1} \in H$. Logo,

$$(gh^{-1})h \in H \Rightarrow g \in H$$

O que contraria nossa suposição inicial de que $g \notin H$. Logo, $gHg^{-1} \subseteq H$.

Em ambos os casos, concluímos que $gHg^{-1} \subseteq H$. Em virtude da proposição 17, concluímos que $H \trianglelefteq G$.

Exemplo 22. *Sejam G um grupo e $n \in \mathbb{N} - \{0\}$. Se G possui um único subgrupo H de ordem n, então $H \trianglelefteq G$.*

De fato, como $H \leq G$, temos que $e \in H$. Daí, $e = geg^{-1} \in gHg^{-1}$ e, portanto, $gHg^{-1} \neq \emptyset$. Sejam $x, y \in gHg^{-1}$. Então, existem $h_1, h_2 \in H$, tais que $x = gh_1g^{-1}$ e $y = gh_2g^{-1}$. Daí,

$$xy^{-1} = (gh_1g^{-1})(gh_2^{-1}g^{-1}) = g(h_1h_2^{-1})g^{-1} \in gHg^{-1}$$

Portanto, $gHg^{-1} \leq G$.

Agora, Considere a função

$$\begin{array}{rcl} f : H & \longrightarrow & gHg^{-1} \\ h & \longmapsto & f(h) = ghg^{-1} \end{array}$$

Se $h_1, h_2 \in H$ são tais que $f(h_1) = f(h_2)$, então

$$gh_1g^{-1} = gh_2g^{-1} \Rightarrow g^{-1}gh_1g^{-1}g = g^{-1}gh_2g^{-1}g \Rightarrow h_1 = h_2$$

Logo, f injetiva. Por outro lado,

$$f(H) = \{f(h) : h \in H\} = \{ghg^{-1} : h \in H\} = gHg^{-}1$$

O que nos permite concluir que f é sobrejetiva e, portanto, uma bijeção entre H e gHg^{-1}. Logo, $|gHg^{-}1| = |H| = n$, mas por hipótese, H é o único subgrupo de G de ordem n. Logo, $gHg^{-1} = H$. Assim, pela proposição 17, concluímos que $H \trianglelefteq G$.

Teorema 6. *Seja $(G, \cdot)$ um grupo e $H \trianglelefteq G$. Então G/H com a operação induzida de G é um grupo.*

Demonstração. Por hipótese, $H \trianglelefteq G$. Segue-se da proposição 17, que a operação de G induz uma operação sobre o conjunto das classes laterais de H em G, isto é,

$$\begin{array}{rcl} \cdot : G/H \times G/H & \longrightarrow & G/H \\ (aH, bH) & \longmapsto & (aH) \cdot (bH) = (ab)H \end{array}$$

Queremos mostrar que $(G/H, \cdot)$ é um grupo. Para isso, tomemos $\alpha, \beta, \gamma \in G/H$. Então existem $a, b, c \in G$, tais que $\alpha = aH, \beta = bH, \gamma = cH$.

(i) Note que

$$\begin{aligned} (\alpha \cdot \beta) \cdot \gamma &= ((aH) \cdot (bH)) \cdot (cH) \\ &= (ab)H \cdot (cH) \\ &= ((ab)c)\, H \\ &= (a(bc))\, H \\ &= (aH) \cdot (bc)H \\ &= (aH) \cdot ((bH) \cdot (cH)) \\ &= \alpha \cdot (\beta \cdot \gamma) \end{aligned}$$

O que garante a associatividade da operação induzida sobre G/H,

(ii) Sendo e o elemento neutro do grupo G, afirmamos que eH é o elemento neutro de G/H relativamente a operação nele induzida por G. Com efeito,

$$(eH) \cdot \alpha = (eH) \cdot (aH) = (ea)H = aH = \alpha$$

De modo análogo, mostra-se que $\alpha \cdot (eH) = \alpha$.

(iii) Afirmamos que $\alpha^{-1} = a^{-1}H$. De fato,

$$(aH) \cdot (a^{-1})H = (aa^{-1})H = eH \qquad (a^{-1}H) \cdot (aH) = (a^{-1}a)H = eH$$

Portanto, de $(i), (ii)$ e (iii), concluímos que $(G/H, \cdot)$ é um grupo. □

Definição 16. *Sejam G um grupo e $H \trianglelefteq G$. O grupo de suas classes laterais com a operação induzida pela operação de G, é chamado de grupo quociente de G por H; ele será denotado por G/H ou $\frac{G}{H}$.*

Exemplo 23. *Sejam $(G,\cdot)$ e e seu elemento neutro. Sendo $H=\{e\}$, temos*

$$\frac{G}{H}=\{gH : g\in G\}=\{g\{e\} : g\in G\}=\{\{g\} : g\in G\}$$

Exemplo 24. *Sejam $n\in\mathbb{N}-\{0\}$. Note que $\frac{\mathbb{Z}}{n\mathbb{Z}}=\{m+n\mathbb{Z} : m\in\mathbb{Z}\}$. Daí, se $x\in\frac{\mathbb{Z}}{n\mathbb{Z}}$, então $x=m+n\mathbb{Z}$, para algum $m\in\mathbb{Z}$. Pelo algoritmo da divisão euclidiana, existem $q,r\in\mathbb{Z}$, com $0\leq r<n$, tal que $m=nq+r$. Desse fato, segue-se que*

$$x=(nq+r)+n\mathbb{Z}=(nq+n\mathbb{Z})+(r+n\mathbb{Z})$$

Como $nq-0=nq\in n\mathbb{Z}$, temos que $nq+n\mathbb{Z}=0+n\mathbb{Z}$. Logo, $x=r+n\mathbb{Z}$, com $0\leq r<n$, isto é,

$$\frac{\mathbb{Z}}{n\mathbb{Z}}=\{r+n\mathbb{Z} : r\in\{0,1,2,\cdots,n-1\}\}=\{0+n\mathbb{Z},1+n\mathbb{Z},\cdots,(n-1)+n\mathbb{Z}\}$$

Observação 16. *Já estabelecemos que a classe de equivalência de um elemento em um grupo, segundo a relação de congruência módulo um subgrupo H, coincide com a classe lateral à esquerda determinada pelo mesmo elemento e em relação à H. Dessa forma, podemos escrever $\overline{k}=k+n\mathbb{Z}$. Com essa notação, temos*

$$\frac{\mathbb{Z}}{n\mathbb{Z}}=\left\{\overline{0},\overline{1},\cdots,\overline{n-1}\right\}.$$

Proposição 19. *Sejam $(G,\cdot)$ um grupo e G' seu subgrupo dos comutadores. Então*

(i) $\frac{G}{G'}$ é abeliano.

(ii) G' é o menor subgrupo normal de G com esta propriedade, isto é, se $H\trianglelefteq G$ e $\frac{G}{H}$ é abeliano, então $G'\subseteq H$.

Demonstração. (i) Sejam $\alpha,\beta\in\frac{G}{G'}$, então existem $a,b\in G$ tais que $\alpha=aG'$ e $\beta=bG'$. Queremos mostrar que $\alpha\beta=\beta\alpha$, ou seja, $(ab)G'=(ba)G'$; mas isso corre se, e somente se, $(ba)^{-1}(ab)\in G'$.

Note que $(ba)^{-1}(ab)=a^{-1}b^{-1}ab\in\{xyx^{-1}y : x,y\in S\}\subseteq\langle xyx^{-1}y : x,y\in S\rangle=G'$ e, portanto, $(ab)G'=(ba)G'$.

(ii) Suponha que $H\trianglelefteq G$ e $\frac{G}{H}$ é abeliano. Então, dados $x,y\in G$, temos que $(yx)H=(xy)H$, isto é, $(yx)^{-1}(xy)\in H$, ou ainda $x^{-1}y^{-1}xy=x^{-1}y^{-1}(x^{-1})^{-1}(y^{-1})^{-1}\in H$. Segue-se que $\{xyx^{-1}y^{-1} : x,y\in G\}\subseteq H$. Daí, $G'=\langle xyx^{-1}y^{-1} : x,y\in G\rangle\subseteq H$. □

Proposição 20. *Seja $(G,\cdot)$ um grupo e $Z(G)$ seu centro. Se $\frac{G}{Z(G)}$ é cíclico, então G é abeliano. Em particular, o índice do centro nunca é primo.*

Demonstração. Suponhamos que $\frac{G}{Z(G)}$ seja cíclico. Então, existe $g\in G$, tal que $\langle gZ(G)\rangle=\frac{G}{Z(G)}=\frac{G}{Z}$; onde $Z=Z(G)$.

Dados $a, b \in G$, temos que $aZ, bZ \in \frac{G}{Z}$. Então, existem $m, n \in \mathbb{Z}$ tais que $aZ = (gZ)^m$ e $bZ = (gZ)^n$. Como $a \in aZ = g^m Z$ e $b \in bZ = g^n Z$, existem $z_1, z_2 \in Z$, tais que $a = g^m z_1$ e $b = g^n z_2$. Segue-se que

$$ab = (g^m z_1)(g^n z_2) = (z_1 g^m)(g^n z_2) = z_1 g^{m+n} z_2 = z_2 g^{n+m} z_1 = (z_2 g^n)(g^m z_1) = ba$$

Portanto, G é abeliano sempre que $\frac{G}{Z}$ é cíclico.

Agora, supondo que $(G : Z)$ é primo, então $\frac{G}{Z}$ é cíclico e, pelo que acabamos de mostrar, teríamos G abeliano; o que ocorre se, e somente se, $Z = G$. Segue-se que

$$(G : Z) = (G : G) = \frac{|G|}{|G|} = 1$$

Uma contradição. □

Definição 17. *Sejam H, K subgrupos de um grupo $(G, \cdot)$. O produto de H por K é o conjunto $HK = \{hk : h \in H \wedge k \in K\}$.*

Observação 17. *O conjunto HK nem sempre é um subgrupo de G. A seguir, mostraremos condições para que $HK \leq G$.*

Proposição 21. *Sejam $(G, \cdot)$ um grupo e H, K subgrupos de G. Nestas condições:*

$$\langle H \cup K \rangle = HK \iff HK \leq G$$

Demonstração. ($\Rightarrow$) Suponha que $\langle H \cup K \rangle = HK$. Como $\langle H \cup K \rangle$ é, por definição, um subgrupo de G, segue imediatamente que $HK \leq G$.

($\Leftarrow$) Seja e o elemento neutro de G (e, portanto, elemento neutro de H e de K). Para quaisquer $h \in H$ e $k \in K$, temos:

$$h = he \in HK \qquad k = ek \in HK$$

O que mostra que $H \subseteq HK$ e $K \subseteq HK$. Consequentemente, $H \cup K \subseteq HK$. Como $\langle H \cup K \rangle$ é o menor subgrupo de G que contém $H \cup K$, então $\langle H \cup K \rangle \subseteq HK$.

Por outro lado, como os elementos de HK são produtos de elementos de H por elementos de K (isto é, são da forma hk, com $h \in H \subseteq HK$ e $k \subseteq K \subseteq HK$), segue que $h, k \in H \cup K \subseteq \langle H \cup K \rangle$. Logo, $hk \in \langle H \cup K \rangle$ e então, $HK \subseteq \langle H \cup K \rangle$ e, portanto, $HK = \langle H \cup K \rangle$. □

Proposição 22. *Sejam $(G, \cdot)$ um grupo e H, K subgrupos de G. Então,*

$$HK \leq G \iff HK = KH$$

Demonstração. ($\Rightarrow$) Se $x \in KH$, então existem $k \in K$ e $h \in H$, tais que $x = kh$. Segue-se que $x^{-1} = h^{-1}k^{-1} \in HK \leq G$; logo, $hk = (x^{-1})^{-1} = x \in HK$ e, portanto, $KH \subseteq HK$. Agora, seja $y \in HK \leq G$. Então, $y^{-1} \in HK$; o que implica que $y^{-1} = hk$, para certos $h \in H$ e $k \in K$. Logo, $y = k^{-1}h^{-1} \in KH$, donde concluímos que $HK = KH$.

($\Leftarrow$) Suponha que $HK = KH$. Por definição, $HK \subseteq G$. Sendo e o elemento neutro de G (e consequentemente, de H e de K) temos $e = ee \in HK$ e, portanto, $HK \neq \emptyset$.

Agora, sejam $x, y \in HK$. Então, $x = h_1k_1$ e $y = h_2k_2$, para certos $h_1, h_2 \in H$ e $k_1, k_2 \in K$. Daí,

$$xy = (h_1k_1)(h_2k_2) = h_1(k_1h_2)k_2$$

Como $k_1h_2 \in KH = HK$, existem $h_3 \in H$ e $k_3 \in K$, tais que $k_1h_2 = h_3k_3$, deste modo

$$xy = h_1(k_1h_2)k_2 = h_1(h_3k_3)k_2 = (h_1h_3)(k_3k_2) \in HK$$

Além disso, temos:

$$x^{-1} = (h_1k_1)^{-1} = k_1^{-1}h_1^{-1} \in KH = HK$$

Portanto, $HK \leq G$. □

Corolário 4. *Sejam H e K dois subgrupos de $(G, \cdot)$. Se H ou K for normal em G, então HK é um subgrupo de G.*

Demonstração. Suponha que $H \trianglelefteq G$. Sejam $x \in HK$, então existem $h \in H$ e $k \in K$, tais que $x = hk$. Daí,

$$x = hk = e(hk) = kk^{-1}(hk) = k(k^{-1}hk) = k(k^{-1}h(k^{-1})^{-1})$$

Pela normalidade de H em G, temos $(k^{-1}h(k^{-1})^{-1}) \in H$; então, $x \in KH$ e assim, $HK \subseteq KH$.

Agora, se $y \in KH$, então $y = kh$, para certos $k \in K$ e $h \in H$. De modo análogo ao caso anterior, temos:

$$y = kh = (kh)e = (khk^{-1})k \in HK$$

O que conclui a prova de que $HK = KH$. Portanto, pela proposição anterior, $HK \leq G$. □

Proposição 23. *Sejam H e K dois subgrupos de um grupo finito G. Então:*

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

Demonstração. Considere a função

$$\begin{array}{rcl} \varphi : H \times K & \longrightarrow & HK \\ (h, k) & \longmapsto & \varphi(h, k) = hk \end{array}$$

Note que φ é sobrejetiva, pois

$$\varphi(H \times K) = \{\varphi(h,k) : h \in H \wedge k \in K\} = \{hk : h \in H \wedge k \in K\} = HK$$

Deste modo, temos que $\dot{\bigcup}_{x \in HK} \varphi^{-1}(x) = H \times K$.

Vamos mostrar que, para cada $x \in HK$, a sua imagem inversa via φ possui $|H \cap K|$ elementos. Isso nos permitirá obter

$$|H \times K| = \left| \dot{\bigcup}_{x \in HK} \varphi^{-1}(x) \right| = \sum_{x \in HK} |\varphi^{-1}(x)| = \sum_{x \in HK} |H \cap K| = |HK| \cdot |H \cap K|$$

Dado $x \in HK$, então $x = hk$, para certos $h \in H$ e $k \in K$.

Sejam $A = \{(h\alpha^{-1}, \alpha k) : \alpha \in H \cap K\}$ e $a \in A$. Então, existe $\alpha \in H \cap K$, tal que $a = (h\alpha, \alpha^{-1}k)$. Note que

$$\varphi(a) = \varphi(h\alpha, \alpha^{-1}k) = h\alpha\alpha^{-1}k = hk = x$$

Logo $a \in \varphi^{-1}(x)$ e, portanto $A \subseteq \varphi^{-1}(x)$. Agora suponha que $a \in \varphi^{-1}(x)$. Então, $\varphi(a) = hk$. Como $\varphi^{-1}(x) \subseteq H \times K$, existem $h_1 \in H$ e $k_1 \in K$, tais que $a = (h_1, k_1)$. Assim, $h_1k_1 = hk$, isto é $k_1k^{-1} = h_1^{-1}h \in H \cap K$. Tomando $\alpha = k_1k^{-1} = h_1^{-1}h$, segue-se que $a = (h_1\alpha, \alpha^{-1}k_1) \in A$. Logo, $\varphi^{-1}(x) \subseteq A$ e, portanto, $\varphi^{-1}(x) = A$, o que prova que $|\varphi^{-1}(x)| = |H \cap K|, \forall x \in HK$. Portanto, temos que $|H \times K| = |HK| \cdot |H \cap K|$, o que implica

$$|HK| = \frac{|H \times K|}{|H \cap K|} = \frac{|H| \cdot |K|}{|H \cap K|}$$

□

2.5 Homomorfismos e Isomorfismos de Grupos

Definição 18. *Sejam $(G_1, \cdot)$ e $(G_2, \times)$ dois grupos. Uma função $f : G_1 \longrightarrow G_2$ é dita um homomorfismo de G_1 em G_2, se, para todos $x, y \in G_1$*

$$f(x \cdot y) = f(x) \times f(y)$$

Além disso, dizemos que:

(1) f é um monomorfismo, quando f é injetiva.

(2) f é um epimorfismo, se f é sobrejetiva.

(3) f é um isomorfismo, quando fé bijetiva. Neste caso, dizemos que G_1 é isomorfo a G_2 e utilizamos a seguinte notação para indicar esse fato: $G_1 \simeq G_2$.

Exemplo 25. *Seja G um grupo. A função*

$$\begin{aligned} Id_G : G &\longrightarrow G \\ g &\longmapsto Id_G(g) = g \end{aligned}$$

é um homomorfismo chamado identidade.

De fato, dados $x, y \in G$, temos:

$$Id_G(x \cdot y) = x \cdot y = Id_G(x) \cdot Id_G(y).$$

Como a função identidade é sempre bijetiva, concluímos que Id_G é um isomorfismo.

Exemplo 26. *Sejam G_1, G_2 dois grupos, e_2 o elemento neutro de G_2. A função*

$$\begin{aligned} e : G_1 &\longrightarrow G_2 \\ g &\longmapsto e(g) = e_2 \end{aligned}$$

é um homomorfismo chamado trivial.

Com efeito, se $x, y \in G_1$, então

$$e(xy) = e_2 = e_2 e_2 = e(x)e(y).$$

Exemplo 27. *Se G é um grupo e $g \in G$, então a função*

$$\begin{aligned} \mathfrak{I}_g : G &\longrightarrow G \\ x &\longmapsto \mathfrak{I}_g(x) = gxg^{-1} \end{aligned}$$

é um isomorfismo chamado de automorfismo interno determinado pelo elemento g.

Sejam $x, y \in G$, então

$$\mathfrak{I}_g(x)\mathfrak{I}_g(y) = (gxg^{-1})(gyg^{-1}) = gxyg^{-1}\mathfrak{I}_g(xy)$$

Logo, $\mathfrak{I}_g$ é um homomorfismo. Note que, $\mathfrak{I}_g^{-1} = \mathfrak{I}_{g^{-1}}$, pois

$$(\mathfrak{I}_g \circ \mathfrak{I}_{g^{-1}})(x) = \mathfrak{I}_g(\mathfrak{I}_{g^{-1}}(x)) = \mathfrak{I}_g(g^{-1}xg) = gg^{-1}xgg^{-1} = x = Id_G(x)$$

De modo análogo, mostra-se que $(\mathfrak{I}_{g^{-1}} \circ \mathfrak{I}_g)(x) = Id_G$ e, com isso, concluímos que $\mathfrak{I}_g$ é bijetiva, uma vez que possui inversa a direita e à esquerda. Portanto, $\mathfrak{I}_g$ é um isomorfismo de G em G.

Proposição 24. *Sejam G um grupo e $H \leq G$. Então, $H \trianglelefteq G$ se, e somente se, $\mathfrak{I}_g(H) = H, \forall g \in G$.*

Demonstração. Para todo $g \in G$, temos que

$$\mathfrak{I}_g(H) = \{\mathfrak{I}_g(h) : h \in H\} = \left\{ghg^{-1} : h \in H\right\} = gHg^{-1}$$

Então,

$$H \trianglelefteq G \iff gHg = H, \forall g \in G \iff \mathfrak{I}_g(H) = H, \forall g \in G$$

□

Exemplo 28. *Sejam G um grupo e $H \trianglelefteq G$. Então,*

$$\begin{aligned} \eta_{_H} : G &\longrightarrow \tfrac{G}{H} \\ g &\longmapsto \eta_{_H}(g) = gH \end{aligned}$$

é um epimorfismo chamado de projeção canônica G sobre $\frac{G}{H}$.

De fato, sejam $x, y \in G$, então

$$\eta_{_H}(x) \cdot \eta_{_H}(y) = xH \cdot yH = (xy)H = \eta_{_H}(xy)$$

Além disso, note que $\eta_{_H}(G) = \{\eta_{_H}(x) : x \in G\} = \{xH : x \in G\} = \frac{G}{H}$ e, portanto, $\eta_{_H}$ é um epimorfismo.

Definição 19. *Sejam $f : G_1 \longrightarrow G_2$ um homomorfismo de grupos e e_2 o elemento neutro do grupo G_2. O conjunto*

$$\ker f = \{x : x \in G_1 \wedge f(x) = e_2\}$$

é chamado de núcleo de f.

Exemplo 29. *Sejam G um grupo, $H \trianglelefteq G$ e $\eta_{_H}$ a projeção canônica de G sobre $\frac{G}{H}$. Note que*

$$\begin{aligned} \ker \eta_{_H} &= \{x : x \in G \wedge \eta_{_H}(x) = eH\} \\ &= \{x : x \in G \wedge xH = eH\} \\ &= \left\{x : x \in G \wedge e^{-1}x \in H\right\} \\ &= \{x : x \in G \wedge x \in H\} \\ &= G \cap H = H, \text{ pois } H \subseteq G. \end{aligned}$$

Teorema 7 (Propriedades elementares dos Homomorfismos)**.** *Sejam $(G_1, \cdot)$, $(G_2, \times)$ grupos; $f : G_1 \longrightarrow G_2$ um homomorfismo; e_1, e_2 elementos neutros de G_1, G_2 respectivamente e $x \in G_1$, então:*

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

(2) $f(x^{-1}) = [f(x)]^{-1}$.

(3) Se $H \leq G_1$, então $f(H) \leq G_2$. Como consequência, $f(G_1) \leq G_2$.
(4) Se $H \trianglelefteq G_1$, então $f(H) \trianglelefteq f(G_1)$.
(5) Se $H \leq G_1$, então $f^{-1}(f(H)) = H \cdot \ker f$.
(6) Se $K \leq G_2$, então $f^{-1}(K)$ é um subgrupo de G_1 que contém $\ker f$.
(7) Se $K \trianglelefteq G_2$, então $f^{-1}(K) \trianglelefteq G_1$. Como consequência, $\ker f \trianglelefteq G_1$.
(8) Se $K \leq G_2$, então $f(f^{-1}(K)) = K \cap f(G_1)$.
(9) f é injetiva se, e somente se, $\ker f = \{e_1\}$
(10) Se $a \in G$ é um elemento de ordem n, então $o(f(a)) \,|\, n$.
(11) Se f é um monomorfismo, então $o(f(a)) = o(a), \forall a \in G_1$.
(12) Se $(G_3, *)$ é um grupo e $h : G_2 \longrightarrow G_3$ um homomorfismo, então $h \circ f$ é um homomorfismo de G_1 em G_3.

Demonstração. (1) Como f é um homomorfismo, temos que $f(e_1) \times f(e_1) = f(e_1 \cdot e_1)$, isto é, $f(e_1) \times f(e_1) = f(e_1)$. Como $f(e_1)$ está no grupo G_2, segue que

$$\begin{aligned} f(e_1) &= f(e_1) \times e_2 \\ &= f(e_1) \times (f(e_1) \times [f(e_1)]^{-1}) \\ &= (f(e_1) \times f(e_1)) \times [f(e_1)]^{-1} \\ &= f(e_1 \cdot e_1) \times [f(e_1)]^{-1} \\ &= f(e_1) \times [f(e_1)]^{-1} \\ &= e_2 \end{aligned}$$

(2) Note que $e_2 = f(e_1) = f(x \cdot x^{-1}) = f(x) \times f(x^{-1})$, ou seja, $e_2 = f(x) \times f(x^{-1})$. Como $f(x) \in G_2$, segue-se que

$$\begin{aligned} [f(x)]^{-1} &= [f(x)]^{-1} \times e_2 \\ &= [f(x)]^{-1} \times f(e_1) \\ &= [f(x)]^{-1} \times f(x \cdot x^{-1}) \\ &= [f(x)]^{-1} \times \big(f(x) \times f(x^{-1})\big) \\ &= \big([f(x)]^{-1} \times f(x)\big) \times f(x^{-1}) \\ &= e_2 \times f(x^{-1}) \\ &= f(x^{-1}) \end{aligned}$$

(3) Por definição, temos $f(H) \subseteq G_2$ e, como $f(e_1) = e_2$, então $f(H) \neq \emptyset$. Se $y_1, y_2 \in f(H)$, então existem $h_1, h_2 \in H$, tais que $f(h_1) = y_1$ e $f(h_2) = y_2$. Segue que

$$y_1 y_2^{-1} = f(h_1)\,[f(h_2)]^{-1} = f(h_1 h_2^{-1}) \in f(H)$$

Portanto, $f(H) \leq G_2$. Como $G_1 \leq G_1$, pelo que foi demonstrado, concluímos que

$f(G_1) \leq G_2$, isto é, $I_m f \leq G_1$.

(4) Sendo $H \trianglelefteq G_1$, em virtude do item (3), concluímos que $f(H) \leq G_2$. Além disso, se $g_2 \in f(G_1)$ e $y \in f(H)$, então existem $h \in H$ e $g_1 \in G_1$, tais que $y = f(h)$ e $g_2 = f(g_1)$. Deste modo,

$$g_2 \times y \times g_2^{-1} = f(g_1) \times f(h) \times f(g_1^{-1}) = f(g_1 h g_1^{-1})$$

Assim, pela hipótese de que $H \trianglelefteq G_1$, segue que $g_1 h g_1^{-1} \in H$ e, portanto, $f(H) \trianglelefteq f(G)$.

(5) Por definição $f^{-1}(f(H)) = \{x : x \in G_1 \wedge f(x) \in f(H)\}$. Seja $x \in f^{-1}(f(H))$, então $f(x) \in f(H)$. Assim, existe $h \in H$ tal que $f(h) = f(x)$. Daí,

$$e = f(h^{-1}) \times f(x) = f(h^{-1}x)$$

Donde concluímos que $h^{-1}x \in \ker f$. Note que $h \in H$ e $h^{-1}x \in \ker f$, então $x = h(h^{-1}x) \in H\ker f$. Logo, $f^{-1}(f(H)) \subseteq H\ker f$.

Agora, dado $x \in H\ker f$, existem $h \in H$ e $k \in \ker f$, tais que $x = hk$, daí

$$f(x) = f(hk) = f(h) \times f(k) = f(h) \times e_2 = f(h)$$

Deste modo, $f(x) = f(h)$. Mas como $h \in H$, temos que $f(h) \in f(H)$, ou seja, $f(x) \in f(H)$. Logo, $x \in f^{-1}(f(H))$,donde concluímos que $H\ker f \subseteq f^{-1}(f(H))$ e, portanto, $f^{-1}(f(H)) = H\ker f$.

(6) Por definição $f^{-1}(K) = \{g : g \in G_1 \wedge f(g) \in K\}$. Daí, $f^{-1}(K) \subseteq G_1$. Por (1), temos que $f(e_1) = e_2 \in K$, logo $e_1 \in f^{-1}(K)$, assim, $f^{-1}(K) \neq \emptyset$.

Sejam $x_1, x_2 \in f^{-1}(K)$, então $f(x_1), f(x_2) \in K$. Como $K \leq G_2$, temos que $f(x_2^{-1}) = [f(x_2)]^{-1} \in K$, e assim, $f(x_1) \times f(x_2^{-1}) \in K$, isto é, $f(x_1 x_2^{-1}) \in K$, o que implica que $x_1 x_2^{-1} \in f^{-1}(K)$ e, portanto, $f^{-1}(K) \leq G_1$.

Além disso, se $x \in \ker f$, então $f(x) = e_2 \in K$. Logo, $f(x) \in K$, isto é, $x \in f^{-1}(K)$; donde concluímos que $\ker f \subseteq f^{-1}(K)$.

(7) Sendo $K \trianglelefteq G_2$, em particular, $K \leq G_2$. Daí, por (6), temos que $f^{-1}(K) \leq G_1$. Sejam $x \in f^{-1}(K)$ e $g \in G_1$. Como $f(x) \in K$, pela normalidade de K em G_2, ocorre $f(g) \times f(x) \times f(g^{-1}) \in K$, ou seja, $f(gxg^{-1}) \in K$. Portanto, $gxg^{-1} \in f^{-1}(K)$. Isso mostra que $f^{-1}(K) \trianglelefteq G_1$. Tomando $K = \{e_2\}$, então $f^{-1}(K) \trianglelefteq G_1$. Mas,

$$f^{-1}(K) = f^{-1}(\{e_2\}) = \{x : x \in G_1 \wedge f(x) \in \{e_2\}\} = \{x : x \in G_1 \wedge f(x) = e_2\} = \ker f$$

Portanto, $\ker f \trianglelefteq G_1$.

(8) Suponha que $y \in f(f^{-1}(K))$. Então, existe $x \in f^{-1}(K)$, tal que $y = f(x)$. Como $x \in f^{-1}(K)$, então $f(x) \in K$. Deste modo, $y \in f(G_1)$ e $y \in K$,isto é, $y \in K \cap f(G_1)$ e, portanto, $f(f^{-1}(K)) \subseteq K \cap f(G_1)$.

Sendo $y \in K \cap f(G_1)$, então $y \in K$ e $y \in f(G_1)$. Assim, existe $g_1 \in G_1$, tal que

$y = f(g_1)$. Sendo $f(g_1) = y \in K$, temos que $g_1 \in f^{-1}(K)$. Evidentemente, temos $f(g_1) \in f(f^{-1}(K))$, isto é, $y \in f(f^{-1}(K))$. Logo, $f(f^{-1}(K)) \subseteq K \cap f(G_1)$ e, portanto, $f(f^{-1}(K)) = K \cap f(G_1)$.

(9) ($\Rightarrow$) Suponha que f é injetiva. Seja $x \in \ker f$. Então, $f(x) = e_2$. Mas sendo f um homomorfismo, por (1), $f(e_1) = e_2$. Pela injetividade de f, segue que $x = e_1$, i.e., $\ker f = \{e_1\}$.

($\Leftarrow$) Reciprocamente, suponha que $\ker f = \{e_1\}$. Sejam $a, b \in G_1$, tais que $f(a) = f(b)$. Então $f(ab^{-1}) = e_2$. Logo, $ab^{-1} \in \ker f$ e, portanto, $ab^{-1} = e_2$, isto é, $a = b$. Segue-se que f é injetiva.

(10) Seja $a \in G_1$, com $o(a) = n \in \mathbb{N} - \{0\}$. Então, $[f(a)]^n = f(a^n) = f(e_1) = e_2$, isto é, $[f(a)]^n = e_2$. Daí, $o(f(a))$ é finito e, além disso, $o(f(a))\big|n$.

(11) Seja $a \in G_1$. Iremos analisar dois casos:

1º Caso: $o(a) < \infty$. Neste caso, por (10) temos que $o(f(a))\big|o(a)$. Note que $[f(a)]^{o(f(a))} = e_2$, isto é, $f(a^{o(f(a))}) = e_2$. Logo, $a^{o(f(a))} \in \ker f$. Como f é um monomorfismo, de (9), segue-se que $a^{o(f(a))} = e_1$. Daí, $o(a)\big|o(f(a))$; donde concluímos que $o(f(a)) = o(a)$.

2º Caso: $o(a) = \infty$. Neste caso, suponha por absurdo que $o(f(a)) < \infty$. Seja $n = o(f(a))$. Daí, $[f(a)]^n = e_2$. De modo análogo ao caso anterior, concluímos que $a^n = e_1$, o que contradiz nossa suposição inicial de que $o(a) = \infty$. Portanto, $o(f(a)) = \infty = o(a)$.

(12) Sejam $(G_3, *)$ é um grupo e $h : G_2 \longrightarrow G_3$ um homomorfismo. Se $x, y \in G_1$, note que

$$\begin{aligned}(h \circ f)(x) * (h \circ f)(y) &= h(f(x)) * h(f(y)) \\ &= h(f(x) \times f(y)) \\ &= h(f(x \cdot y)) \\ &= (h \circ f)(x \cdot y)\end{aligned}$$

Portanto, $h \circ f : G_1 \longrightarrow G_3$ é um homomorfismo de grupos. □

Proposição 25. *Se G é um grupo cíclico, então G é finito ou G é infinito enumerável.*

Demonstração. Seja G cíclico. Então, existe $a \in G$, tal que $G = \langle a \rangle$.

1º Caso: G é infinito. Neste caso, considere a função

$$\begin{aligned} f : \mathbb{Z} &\longrightarrow G \\ z &\longmapsto f(z) = a^z \end{aligned}$$

dados $x, y \in \mathbb{Z}$, então

$$f(x+y) = a^{x+y} = a^x a^y = f(x)f(y)$$

Logo, f é um homomorfismo. Além disso, temos:

$$f(\mathbb{Z}) = \{f(z) : z \in \mathbb{Z}\} = \{a^z : z \in \mathbb{Z}\} = \langle a \rangle = G$$

Isso nos permite concluir que f é um epimorfismo.

Por outro lado, se $x, y \in \mathbb{Z}$ são tais que $f(x) = f(y)$, então $a^x = a^y$, ou seja, $a^{x-y} = e$. Como $|G| = \infty$, pelo que mencionamos na observação 10, concluímos que $x - y = 0$, i.e., $x = y$. Portanto, f é um isomorfismo.

$2^{\underline{o}}$ Caso: G é finito. Neste caso, seja $n = |G|$. Iremos considerar a aplicação

$$\begin{array}{rcl} f : \mathbb{Z}_n & \longrightarrow & G \\ z & \longmapsto & f(z) = a^z \end{array}$$

De modo análogo ao caso anterior, mostra-se que f é um epimorfismo.

Agora, se $x, y \in \mathbb{Z}_n$ são tais que $f(x) = f(y)$, então $a^{x-y} = e$. Logo $n \big| x - y$, o que implica $n \big| |x - y|$. Mas, sendo $x, y \in \mathbb{Z}_n$, temos que $0 \leq x, y < n$; isso acarreta $0 \leq |x - y| < n$, ou seja, $|x - y|$ é múltiplo de n não negativo e menor que n, logo, só pode ser $|x - y| = 0$ e, assim, $x = y$. Portanto, f é um isomorfismo.

Deste modo, podemos concluir que os únicos grupos cíclicos (a menos de isomorfismos) são $(\mathbb{Z}, +)$ e $(\mathbb{Z}, \underset{n}{\oplus})$. □

Teorema 8 (Teorema Fundamental dos Isomorfismos para Grupos)**.** *Sejam $(G_1, \cdot), (G_2, *)$ dois grupos, $f : G_1 \longrightarrow G_2$ um homomorfismo, $H = kerf$ e $\eta_H : G_1 \longrightarrow \frac{G_1}{H}$ a projeção canônica de G sobre $\frac{G}{H}$. Então, valem:*

(1) Existe um único monomorfismo $g : \frac{G_1}{H} \longrightarrow G_2$, tal que $f = g \circ \eta_H$

(2) $I_m g = I_m f$. Como consequência, $\frac{G_1}{H} \simeq I_m f$.

Demonstração. (1) Sejam $g := \{(xH, f(x)) : x \in G_1\}$ uma relação de $\frac{G_1}{H}$ em G_2 e $(\alpha, \beta), (\gamma, \delta) \in g$, tais que $\alpha = \gamma$. Então, existem $a, b \in G$, tais que $(\alpha, \beta) = (aH, f(a))$ e $(\gamma, \delta) = (bH, f(b))$. Como $\gamma = \alpha$, temos que $b^{-1}a \in H = \ker f$. Logo, $e_2 = f(b^{-1}a) = f(b^{-1}) * f(a)$, o que acarreta $f(a) = f(b)$, isto é, $\beta = \delta$. Portanto $g : \frac{G_1}{H} \longrightarrow G_2$ está bem definida.

Sejam $\alpha, \beta \in \frac{G_1}{H}$. Então, existem $a, b \in G_1$, tais que $\alpha = aH$ e $\beta = bH$. Segue-se que

$$\begin{aligned} g(\alpha \cdot \beta) &= g\left((aH) \cdot (bH)\right) = g(aH) * g(bH) = g(\alpha) * g(\beta) \\ &= g((ab)H) \\ &= f(ab) \\ &= f(a) * f(b) \\ &= g(aH) * g(bH) \\ &= g(\alpha) * g(\beta) \end{aligned}$$

Logo, g é um homomorfismo. Seja $\alpha = aH \in \ker g$, então $g(aH) = e_2$, isto é, $f(a) = e_2$, daí $a \in \ker f$, logo $aH = e_1H$, ou seja $\alpha = e_1H$ e, portanto, $\ker g = \{e_1H\}$. Segue-se que g é um monomorfismo.

Note que, dado $x \in G_1$,temos

$$(g \circ \eta_{_H})(x) = g(\eta_{_H}(x)) = g(xH) = f(x)$$

Logo, $f = g \circ \eta_{_H}$.

Por fim, para mostrar a unicidade de g, suponha que existe um outro monomorfismo $h : \frac{G_1}{H} \longrightarrow G_2$ tal que $f = h \circ \eta_{_H}$. Como $\eta_{_H}$ é sobrejetiva, existe $\eta : \frac{G_1}{H} \longrightarrow G_1$, tal que $\eta_{_H} \circ \eta = Id_{\frac{G_1}{H}}$. Como por hipótese, temos $f = g \circ \eta_H$, então

$$g \circ \eta_{_H} = h \circ \eta_{_H} \Rightarrow g \circ (\eta_{_H} \circ \eta) = h \circ (\eta_{_H} \circ \eta) \Rightarrow g \circ Id_{\frac{G_1}{H}} = h \circ Id_{\frac{G_1}{H}} \Rightarrow g = h$$

Isso nos permite concluir que $g : \frac{G_1}{H} \longrightarrow G_2$ é o único monomorfismo, tal que $f = g \circ \eta_{_H}$.

(2) Observe que $I_m g = \{g(xH) : x \in G_1\} = \{f(x) : x \in G_1\} = I_m f$. Daí, segue-se que $g : \frac{G_1}{H} \longrightarrow I_m f$ é um homomorfismo bijetivo, ou seja, g é um isomorfismo de $\frac{G_1}{H}$ em $I_m f$. Logo, $\frac{G_1}{H} \simeq I_m f$. □

Corolário 5. *Sejam $H \trianglelefteq G$ e $K \leq G$. Então*

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

Demonstração. Inicialmente, vamos mostrar que $\frac{KH}{H}$ é de fato um grupo. Observe que, sendo $H \trianglelefteq G$ e $K \leq G$, temos que $HK \leq G$ e, portanto, $HK = KH$. Como $H \trianglelefteq G$, vale $ghg^{-1} \in H$, para todo $h \in H$ e para todo $g \in G$; em particular, ghg^{-1}, para todo $h \in H$ e para todo $g \in HK \subseteq G$. Logo, $H \trianglelefteq KH$. Segue-se que $(\frac{KH}{H}, \cdot)$ é um grupo.

Agora, considere a projeção canônica $\eta_{_{KH}} : KH \longrightarrow \frac{KH}{H}$. Recordemos que $K \subseteq KH$, uma vez que $\langle H \cup K \rangle = KH$. Considere a restrição $\eta_{_{KH}}\big|_{_K} : K \longrightarrow \frac{KH}{H}$, então

$$\frac{KH}{H} = \{(kh)H : k \in K \wedge h \in H\} = \{(kH)(hH) : k \in K \wedge h \in H\} = \{kH : k \in K\} = \eta_{_{KH}}\big|_{_K}(K)$$

Além disso, temos

$$\begin{aligned}\ker \eta_{KH}\big|_K &= \Big\{x : x \in K \wedge \eta_{KH}\big|_K(x) = eH\Big\}\\ &= \{x : x \in K \wedge xH = eH\}\\ &= \{x : x \in K \wedge x \in H\}\\ &= H \cap K\end{aligned}$$

Portanto, pelo teorema fundamental do isomorfismo, concluímos que $K\big/(\ker \eta_{KH}\big|_K) \simeq \eta_{KH}\big|_K(K)$, isto é, $\frac{K}{H\cap K} \simeq \frac{KH}{H}$. □

Exemplo 30. *Sejam G_1, G_2 dois grupos,$H_1 \trianglelefteq G_1$ e $H_2 \trianglelefteq G_2$. Então,*

(1) $H_1 \times H_2 \trianglelefteq G_1 \times G_2$.

(2) $\frac{G_1\times G_2}{H_1\times H_2} \trianglelefteq \left(\frac{G_1}{H_1}\right) \times \left(\frac{G_2}{H_2}\right)$

Como $H_1 \trianglelefteq G_1$ e $H_2 \trianglelefteq G_2$, podemos considerar tomar os epimorfismos η_{H_1} e η_{H_2}, que são, respectivamente, as projeções canônicas de G_1 sobre $\frac{G_1}{H_1}$ e de G_2 sobre $\frac{G_2}{H_2}$. Considere a função

$$\begin{aligned}\eta : G_1 \times G_2 &\longrightarrow \left(\tfrac{G_1}{H_1}\right) \times \left(\tfrac{G_2}{H_2}\right)\\ (x, y) &\longmapsto \eta(x, y) = \big(\eta_{H_1}(x), \eta_{H_2}(y)\big)\end{aligned}$$

É evidente que η é um homomorfismo, pois, se $\alpha, \beta \in G_1 \times G_2$, então $\alpha = (x, y)$ e $\beta = (z, w)$, para certos $x, z \in G_1$ e $y, w \in G_2$. Daí,

$$\begin{aligned}\eta(\alpha \cdot \beta) &= \eta((x, y) \cdot (z, w))\\ &= \eta(x \cdot z, y \cdot w)\\ &= \big(\eta_{H_1}(x \cdot z), \eta_{H_2}(y \cdot w)\big)\\ &= \big(\eta_{H_1}(x) \cdot \eta_{H_1}(z), \eta_{H_2}(y) \cdot \eta_{H_2}(w)\big)\\ &= \big(\eta_{H_1}(x), \eta_{H_2}(y)\big) \cdot \big(\eta_{H_1}(z), \eta_{H_2}(w)\big)\\ &= \eta(x, y) \cdot \eta(z, w)\\ &= \eta(\alpha) \cdot \eta(\beta)\end{aligned}$$

Mais precisamente, η é um epimorfismo, poi

$$\begin{aligned}\eta(G_1 \times G_2) &= \{\eta(x, y) : (x, y) \in G_1 \times G_2\}\\ &= \big\{(\eta_{H_1}(x), \eta_{H_2}(y)) : x \in G_1 \wedge y \in G_2\big\}\\ &= \big\{\eta_{H_1}(x) : x \in G_1\big\} \times \big\{\eta_{H_2}(y) : y \in G_2\big\}\\ &= \eta_{H_1}(G_1) \times \eta_{H_2}(G_2)\\ &= \left(\frac{G_1}{H_1}\right) \times \left(\frac{G_2}{H_2}\right)\end{aligned}$$

Além disso, temos que

$$\begin{aligned}\ker\eta &= \{(x,y) : (x,y) \in G_1 \times G_2 \wedge \eta(x,y) = (eH_1, eH_2)\}\\ &= \big\{(x,y) : (x \in G_1 \wedge y \in G_2) \wedge \big(\eta_{H_1}(x), \eta_{H_2}(y)\big) = (eH_1, eH_2)\big\}\\ &= \big\{(x,y) : \big(x \in G_1 \wedge \eta_{H_1}(x) = eH_1\big) \wedge \big(y \in G_2 \wedge \eta_{H_2}(y) = eH_2\big)\big\}\\ &= \big\{x : x \in G_1 \wedge \eta_{H_1}(x) = eH_1\big\} \times \big\{y : y \in G_2 \wedge \eta_{H_2}(y) = eH_2\big\}\\ &= \ker\eta_{H_1} \times \ker\eta_{H_2}\\ &= H_1 \times H_2\end{aligned}$$

Pelo teorema 7 item (7), segue que $\ker\eta \trianglelefteq G_1 \times G_2$*, ou seja,* $H_1 \times H_2 \trianglelefteq G_1 \times G_2$*. Por outro lado, do teorema fundamental dos isomorfismos de grupos, decorre que* $\frac{G_1\times G_2}{\ker\eta} \simeq \eta(G_1 \times G_2)$*, isto é,* $\frac{G_1\times G_2}{H_1\times H_2} \simeq \left(\frac{G_1}{H_1}\right) \times \left(\frac{G_2}{H_2}\right)$*.*

Teorema 9 (Teorema da correspondência)**.** *Sejam* $f : (G_1, \cdot) \longrightarrow (G_2, \times)$ *um homomorfismo de grupos,* $K = \ker f$*,* $\mathcal{S}_K(G_1)$ *o conjunto dos subgrupos de* G_1 *que contém* K *,* $\mathcal{S}(f(G_1))$ *o conjunto dos subgrupos de* $f(G_1)$ *e as funções*

$$\begin{array}{rcl}\varphi : \mathcal{S}_K(G_1) & \longrightarrow & \mathcal{S}(f(G_1))\\ H & \longmapsto & \varphi(H) = f(H)\end{array} \qquad \begin{array}{rcl}\psi : \mathcal{S}(f(G_1)) & \longrightarrow & \mathcal{S}_K(G_1)\\ L & \longmapsto & \psi(L) = f^{-1}(L)\end{array}$$

Então,

(1) φ *e* ψ *são bijeções, inversas uma da outra.*

(2) $H \trianglelefteq G_1 \Rightarrow \varphi(H) \trianglelefteq \varphi(G_1) = f(G_1)$*.*

(3) $L \trianglelefteq I_m f \Rightarrow \psi(L) \trianglelefteq \psi(f(G_1)) = G_1$*.*

Demonstração. (1) Vamos mostrar que φ e ψ são inversas uma da outra e, portanto, bijeções. Seja $H \in \mathcal{S}_K(G_1)$, então $H \leq G_1$ e $K \subseteq H$. Note que $\varphi(H) = f(H) \in \mathcal{S}(f(G_1))$, daí

$$(\psi \circ \varphi)(H) = \psi(\varphi(H)) = \psi(f(H)) = f^{-1}(f(H))$$

Pelo teorema 7, item (5), segue-se que $f^{-1}(f(H)) = HK$ e, então, sendo $K \subseteq H$, concluímos que $HK = H$. Logo, $(\psi \circ \varphi)(H) = H = Id_{\mathcal{S}_K(G_1)}(H)$, ou seja, $\varphi \circ \psi = Id_{\mathcal{S}_K(G_1)}$ e, portanto, ψ é sobrejetiva e φ é injetiva.

Seja agora $L \in \mathcal{S}_K(G_1)$, então $L \leq f(G_1)$. Observe que $f^{-1}(L) = \psi(L) \in \mathcal{S}(f(G_1))$, deste modo

$$(\varphi \circ \psi)(L) = \varphi(\psi(L)) = \varphi(f^{-1}(L)) = f(f^{-1}(L))$$

Novamente, decorre do teorema 7, mas agora, do item (8), que $f(f^{-1}(L)) = L \cap f(G_1)$. Como $L \leq f(G_1)$, obtemos $L \cap f(G_1) = L$. Logo, $(\varphi \circ \psi)(L) = L$, donde concluímos que φ é sobrejetiva e ψ é injetiva. Portanto, φ e ψ são bijeções e, além disso, $\varphi^{-1} = \psi$.

(2) Como $H \trianglelefteq G_1$, do teorema 7, segue $f(H) \trianglelefteq f(G_1) = I_m f$, ou seja, $\varphi(H) \trianglelefteq \varphi(G_1) = f(G_1)$.

(3) Sendo $L \trianglelefteq I_m f$, mais uma vez, pelo teorema 7, temos $\psi(L) = f^{-1}(L) \trianglelefteq f^{-1}(f(G_1)) = \psi(f(G_1)) = G_1$, isto é, $\psi(L) \trianglelefteq G_1$. □

Corolário 6. *Seja $H \trianglelefteq G$. Sejam $\mathcal{N}_H(G)$ o conjunto dos subgrupos normais de G que contêm H e $\mathcal{N}(G)$ o conjunto dos subgrupos normais em $\frac{G}{H}$. Então a função*

$$\begin{array}{rcl} \eta : \mathcal{N}_H(G) & \longrightarrow & \mathcal{N}\left(\frac{G}{H}\right) \\ K & \longmapsto & \eta(K) = \frac{K}{H} \end{array}$$

é uma bijeção.

Demonstração. No teorema anterior, tome $G_1 = G$, $G_2 = \frac{G}{H}$ e $f = \eta_{_H}$. Do exemplo 29, temos que $\ker \eta_{_H} = H$. Portanto,

$$\begin{array}{rcl} \varphi : \mathcal{S}_H(G) & \longrightarrow & \mathcal{S}\left(\frac{G}{H}\right) \\ K & \longmapsto & \varphi(K) = \eta_{_H}(K) \end{array}$$

é uma bijeção que leva subgrupos normais de $\mathcal{S}_H(G)$ em subgrupos normais de $\mathcal{S}\left(\frac{G}{H}\right)$, isto é, leva elementos de $\mathcal{N}_H(G)$, em elementos de $\mathcal{N}\left(\frac{G}{H}\right)$.

Note que, se $x \in \varphi(\mathcal{N}_H(G))$, então existe $K \in \mathcal{N}_H(G) \subseteq \mathcal{S}_H(G)$, tal que $x = \varphi(K)$. Como $K \trianglelefteq G$, então, pelo teorema anterior, item (2), tem-se $x = \varphi(K) \trianglelefteq \varphi(G) = \frac{G}{H}$. Logo, $x \in \mathcal{N}(\frac{G}{H})$ e, portanto, $\varphi(\mathcal{N}_H(G)) \subseteq \mathcal{N}(\frac{G}{H})$.

Agora, se $L \in \mathcal{N}(\frac{G}{H}) \subseteq \mathcal{S}(\frac{G}{H})$, então $L \trianglelefteq \frac{G}{H}$. Além disso, pelo item (3) do teorema anterior, temos que $\varphi^{-1}(L) \trianglelefteq \varphi^{-1}(\frac{G}{H}) = G$. Logo, $\varphi^{-1}(L) \in \mathcal{N}_H(G)$, isto é, $L = \varphi(\varphi^{-1}(L)) \in \varphi(\mathcal{N}_H(G))$ e, portanto, $\mathcal{N}(\frac{G}{H}) \subseteq \varphi(\mathcal{N}_H(G))$. Logo, $\varphi(\mathcal{N}_H(G)) = \mathcal{N}(\frac{G}{H})$.

Daí, é fácil ver que a função η coincide com a restrição (que também é uma bijeção) de φ ao domínio $\mathcal{N}_H(G)$ e contradomínio $\varphi(\mathcal{N}_H(G)) = \mathcal{N}(\frac{G}{H})$ e, portanto, η é uma bijeção.

□

3 Grupos finitos gerados por dois elementos

Na seção sobre subgrupos, definimos o *subgrupo gerado por um subconjunto* S de um grupo G como a interseção da família de subgrupos de G que contêm S. Provamos também que $\langle S\rangle$ é o menor subgrupo de G que contém S e que, na notação multiplicativa, seus elementos são produtos, com quantidade finita de fatores, onde cada fator é uma potência de elementos de S com expoentes inteiros. Assim, se $a, b \in G$ e $x \in \langle a, b\rangle$, então existem $n \in \mathbb{N} - \{0\}$, elementos $a_1, a_2, \ldots, a_n \in \{a, b\}$ e $k_1, k_2, \ldots, k_n \in \mathbb{Z}$, tais que $x = a_1^{k_1} a_2^{k_2} \cdots a_n^{k_n}$. Nesta seção, mostramos que, quando os geradores a e b satisfazem certas relações, a descrição dos elementos do subgrupo gerado por eles torna-se consideravelmente mais simples. Além disso, demonstramos que as condições de congruência apresentadas na introdução são necessárias para a existência de grupos com dois elementos a, b sujeitos a tais relações e, quando essas condições são satisfeitas, que tal grupo é único a menos de isomorfismo.

Teorema 10. *Sejam $s \in \mathbb{N} - \{0\}$, G_1 um grupo finito com elemento neutro e e $a, b \in G_1$ satisfazendo $ba = a^s b$ (ou equivalentemente $\mathfrak{I}_g(a) = a^s$). Sejam $m, n \in \mathbb{N} - \{0\}$ inteiros tais que $a^n = e$ e $b^m \in \langle a\rangle$, então*

(1) $b^t \cdot a^r = a^{rs^t} \cdot b^t, \forall t \in \mathbb{N}$ e $\forall r \in \mathbb{Z}$.

(2)$\langle a, b\rangle = \{a^i b^j : i, j \in \mathbb{N} \wedge 0 \leq i \leq n-1 \wedge 0 \leq j \leq m-1\}$.

(3) $o(a) = n$ e $m = \min\{l : l \in \mathbb{N} - \{0\} \wedge b^l \in \langle a\rangle\} \iff |\langle a, b\rangle| = nm$.

(4) Se $n = o(a)$, $m = \min\{l : l \in \mathbb{N} - \{0\} \wedge b^l \in \langle a\rangle\}$, u um inteiro tal que $b^m = a^u$, G_2 um grupo com elemento neutro e_2 e $\alpha, \beta \in G_2$, então existe um homomorfismo $f : \langle a, b\rangle \longrightarrow G_2$ tal que $f(a) = \alpha$ e $f(b) = \beta$ se, e somente se, $\beta\alpha = \alpha^s\beta$, $\alpha^n = e_2$ e $\beta^m = \alpha^u$.

Demonstração. (1) Na demonstração da proposição 18, vimos que $(bab^{-1})^k = ba^k b^{-1}, \forall k \in \mathbb{Z}$. Utilizaremos esse fato para mostrar que $b^t \cdot a^r = a^{rs^t} \cdot b^t, \forall r \in \mathbb{Z}$. Para isso, realizaremos indução sobre t.

Para todo $r \in \mathbb{Z}$, temos $b^0 a^r = a^r = a^{rs^0} b^0$. Se $t \in \mathbb{N} - \{0\}$ é tal que $b^t a^r = a^{rs^t} b^t$, para todo $r \in \mathbb{Z}$, então

$$b^{t+1}a^r = b(b^t a^r) = ba^{rs^t}b^t = (ba^{rs^t}b^{-1})b^{t+1} \overset{(i)}{=} (bab^{-1})^{rs^t}b^{t+1} = (a^s bb^{-1})^{rs^t}b^{t+1} = a^{rs^{t+1}}b^{t+1}$$

Onde a igualdade (i) decorre da proposição mencionada inicialmente. Assim, pelo Princípio de Indução, temos que $b^t a^r = a^{rs^t} b^t, \forall t \in \mathbb{N}, \forall r \in \mathbb{Z}$.

(2) Seja $H = \{a^i b^j : i, j \in \mathbb{N} \wedge 0 \leq i \leq n-1 \wedge 0 \leq j \leq m-1\}$. Evidentemente, $H \subseteq \langle a, b\rangle$. Agora, se $x \in \langle a, b\rangle$, então, usando o fato de que $a^n = e$ e $b^m \in \langle a\rangle$, existem $k \in \mathbb{N} - \{0\}$ e $r_1, r_2, \cdots, r_k, t_1, t_2, \cdots, t_k \in \mathbb{N}$, tais que $x = a^{r_1} b^{t_1} a^{r_2} b^{t_2} \cdots a^{r_k} b^{t_k}$. Novamente, utilizaremos indução; agora, sobre k. Os caso $k = 0$ e $k = 1$ são evidentes, pois $ab = a^1 b^1, e = a^0 b^0 \in H$.

Supondo que $a^{r_1}b^{t_1}a^{r_2}b^{t_2}\cdots a^{r_{k-1}}b^{t_{k-1}} = a^ib^j$, para $k-1 \in \mathbb{N}-\{0\}$, $0 \leq r_1, r_2, \cdots, r_{k-1}, i < n$ e $0 \leq t_1, t_2, \cdots, t_{k-1}, i < m$. Daí,

$$x = (a^ib^j)(a^{r_k}b^{t_k}) = a^i(b^ja^{r_k})b^{t_k} \overset{(*)}{=} a^i(a^{r_k s^j}b^j)b^{t_k} = a^{i+r_k s^j}b^{j+t_k}$$

Onde a igualdade $(*)$ decorre do item (1) deste teorema. Deste modo, pelo algoritmo da divisão euclidiana, existem $q_1, q_2, p_1, p_2 \in \mathbb{Z}$, com $0 \leq p_1 < n$ e $0 \leq p_2 < m$, tais que $i + r_k s^j = q_1 n + p_1$ e $j + t_k = q_2 m + p_2$. Segue-se que

$$x = (a^n)^{q_1}a^{p_1}(b^m)^{q_2}b^{p_2} = a^{p_1}a^{uq_2}b^{p_2}$$

Mais uma vez, aplicando o algoritmo da divisão euclidiana, existem $q_3, p_3 \in \mathbb{Z}$, com $0 \leq p_3 < n$, tais que $p_1 + uq_2 = q_3 n + p_3$, donde concluímos que $x = a^{p_3}b^{p_2}$ e, portanto, $x \in H$, isto é, $\langle a, b\rangle \subseteq H$. Logo, $\langle a, b\rangle = \{a^ib^j : 0 \leq i \leq n-1 \wedge 0 \leq j \leq m-1\}$.

(3) $(\Rightarrow)$ Suponha que $o(a) = n$ e $m = \min\left\{l : l \in \mathbb{N} \wedge b^l \in \langle a\rangle\right\}$,vamos mostrar que os elementos de $\{a^ib^j : 0 \leq i \leq n-1 \wedge 0 \leq j \leq m-1\}$ são dois a dois distintos; isso nos permitirá concluir que $\left|\langle a, b\rangle\right| = \left|\,\{0, 1, 2, \cdots, n-1\} \times \{0, 1, 2, \cdots, m-1\}\,\right| = nm$.

Sejam $i, k \in \{0, 1, 2, \cdots, n-1\}$ e $j, l \in \{0, 1, 2, \cdots, m-1\}$, tais que $a^ib^j = a^kb^l$, então $b^{j-l} = a^{k-i} \in \langle a\rangle$. Como $m := \min\left\{p : p \in \mathbb{N} \wedge b^l \in \langle a\rangle\right\}$, segue que $m\big|j-l$, mais geralmente, $m\big||j-l|$. Entretanto, sendo $j, l \in \{0, 1, 2, \cdots, m-1\}$, concluímos que $0 \leq |j-l| < m$, com $m\big||j-l|$. Logo, $|j-l| = 0$ e, portanto, $j = l$. Daí, $a^{k-i} = b^{j-j} = b^0 = e$, como $o(a) = n$, temos $n\big||k-i|$, e de modo análogo ao que foi feito anteriormente, obtemos $k = i$. Portanto, os elementos de $\langle a, b\rangle$ são dois a dois distintos e, daí, $\left|\langle a, b\rangle\right| = nm$.

$(\Leftarrow)$ Suponha que $\left|\langle a, b\rangle\right| = nm$. Por hipótese, temos $a^n = e$ e $b^m \in \langle a\rangle$. Então, $o(a)\big|n$, e assim, $o(a) \leq n$. A fim de obter uma contradição, suponha que existam $n' \in \mathbb{N} - \{0\}$ tais que $n' < n$, com $a^{n'} = e$. Então, em virtude do item (2) deste teorema, teríamos

$$\langle a, b\rangle = \{a^ib^j : i, j \in \mathbb{N} \wedge 0 \leq i \leq n'-1 \wedge 0 \leq j \leq m-1\}$$

Ou seja $\langle a, b\rangle$ teria no máximo $n'm < nm$ elementos, uma contradição. De modo análogo, tomando $m' < m$ com $b^m \in \langle a\rangle$, obtemos que $\langle a, b\rangle$ teria no máximo $nm' < nm$ elementos. Portanto, $o(a) = n$ e $m = \min\left\{l : l \in \mathbb{N} \wedge b^l \in \langle a\rangle\right\}$.

(4) $(\Rightarrow)$ Suponha que exista um homomorfismo $f : \langle a, b\rangle \longrightarrow G_2$ com $f(a) = \alpha$ e $f(b) = \beta$. Então,

$$\beta\alpha = f(b)f(a) = f(ba) = f(a^sb) = [f(a)]^s f(b) = \alpha^s\beta$$

Além disso, como $\alpha^n = [f(a)]^n = f(a^n) = f(e) = e_2$ e

$$\beta^m = [f(b)]^m = f(b^m) = f(a^u) = [f(a)]^u = \alpha^u.$$

($\Leftarrow$) Suponha agora que $\beta\alpha = \alpha^s\beta, \alpha^n = e_2$e $\beta^m = \alpha^u$. Em virtude do item (2) deste teorema, a função abaixo está bem definida

$$\begin{array}{rcl} f : \langle a, b\rangle & \longrightarrow & G_2 \\ a^i b^j & \longmapsto & f(a^i b^j) = \alpha^i \beta^j \end{array}$$

Sejam $x, y \in \langle a, b\rangle$, então existem $i, k \in \{0, 1, 2, \cdots, n-1\}$ e $j, l \in \{0, 1, 2, \cdots, m-1\}$, tais que $x = a^i b^j$ e $y = a^k b^l$. Note que,

$$xy = a^i(b^j a^k)b^l = a^i(a^{ks^j} b^j)b^l = a^{i+ks^j} \cdot b^{j+l}$$

Assim, para que possamos aplicar f ao composto xy, devemos assegurar que $0 \leq i + ks^j < n$ e $0 \leq j + l < m$. Assim, pelo algoritmo da divisão euclidiana, existem $q_1, q_2, r_1, r_2 \in \mathbb{Z}$, com $0 \leq r_1 < n$ e $0 \leq r_2 < m$, tais que $i+ks^j = q_1 n+r_1$ e $j+l = q_2 m+r_2$. Logo,

$$xy = (a^n)^{q_1} a^{r_1} (b^m)^{q_2} b^{r_2} = e a^{r_1} a^{uq_2} b^{r_2} = a^{r_1+u} b^{r_2}$$

Aplicando novamente o algoritmo da divisão, temos que $r_1 + uq_2 = q_3 n + r_3$, para certos $q_3, r_3 \in \mathbb{Z}$ e $0 \leq r_3 < n$. Daí,

$$xy = (a^n)^{q_3} a^{r_3} b^{r_2} = a^{r_3} b^{r_2}$$

Logo, $f(xy) = f(a^{r_3} b^{r_2}) = \alpha^{r_3}\beta^{r_2}$. Contudo, como $r_2 = j + l - q_2 m$ e $r_3 = r_1 + uq_2 - q_3 n = i + ks^j - q_1 n + u - q_3 n$, ou seja, $r_2 = -mq_2 + j + l$ e $r_3 = i + ks^j + uq_2 - n(q_1 + q_3)$. Segue-se que

$$\begin{aligned} f(xy) &= \alpha^{r_3}\beta^{r_2} \\ &= \alpha^i \alpha^{ks^j} (\alpha^u)^{q_2} (\alpha^n)^{-(q_1+q_3)} \beta^{-mq_2} \beta^j \beta^l \\ &= \alpha^i \alpha^{ks^j} (\beta^{mq_2} e \beta^{-mq_2}) \beta^j \beta^l \\ &= \alpha^i \alpha^{ks^j} (\beta^{mq_2 - mq_2}) \beta^j \beta^l \\ &= \alpha^i (\alpha^{ks^j} \beta^j) \beta^l \end{aligned}$$

Do item (1) deste teorema, também segue que $\beta^t \alpha^r = \alpha^{rs^t}\beta; \forall r, t \in \mathbb{N}$. Logo,

$$f(xy) = \alpha^i(\beta^j \alpha^k)\beta^l = (\alpha^i \beta^j)(\alpha^k \beta^l) = f(x)f(y)$$

Portanto, f é um homomorfismo entre os grupos $\langle a, b\rangle$ e G_2. □

Teorema 11. *Sejam $n, m, s \in \mathbb{N} - \{0\}$ e $u \in \mathbb{N}$.*

(1) Se G é um grupo de ordem nm e $a, b \in G$ são tais que

$$(*)\begin{cases} G &= \langle a, b\rangle \\ a^n &= e \\ b^m &= a^u \\ ba &= a^s b \end{cases}$$

Então, $s^m \equiv 1 \pmod{n}$ e $u(s-1) \equiv 0 \pmod{n}$.

(2) Quando existe um grupo de ordem nm satisfazendo $(*)$, ele é único a menos de isomorfismos.

Demonstração. (1) Pelo primeiro item do teorema 10, temos que $b^m a^1 = a^{1\cdot s^m} b^m$ e $b^1 a^u = a^{us^1} b^1$. Como $b^m = a^u \in \langle a\rangle$, e $\langle a\rangle$ é cíclico (portanto abeliano), temos que

$$ab^m = a^{s^m} b^m \Rightarrow a = a^{s^m} \Rightarrow a^{s^m - 1} = e \Rightarrow o(a) \big| s^m - 1$$

Por outro lado, como $a^u = b^m \in \langle b\rangle$, que também é abeliano, segue que

$$a^u b = a^{us} b \Rightarrow a^u = a^{us} \Rightarrow a^{u(s-1)} = e \Rightarrow o(a) \big| u(s-1)$$

Mas como $|\langle a, b\rangle| = nm$ e valem $(*)$, em virtude do terceiro item do teorema 10, segue que $o(a) = n$. Portanto, $n \big| s^m - 1$ e $n \big| u(s-1)$, ou seja, $s^m \equiv 1 \pmod{n}$ e $u(s-1) \equiv 0 \pmod{n}$.

(2) Suponha que G_1, G_2 sejam dois grupos de ordem nm e que admitam elementos $a, b \in G_1$ e $\alpha, \beta \in G_2$, que estes satisfaçam $(*)$, isto é,

$$\begin{cases} G_1 &= \langle a, b\rangle \\ a^n &= e \\ b^m &= a^u \in \langle a\rangle \\ ba &= a^s b \end{cases} \qquad \begin{cases} G_2 &= \langle \alpha, \beta\rangle \\ \alpha^n &= e_2 \\ \beta^m &= \alpha^u \in \langle \alpha\rangle \\ \beta\alpha &= \alpha^s \beta \end{cases}$$

Onde e e e_2 são, respectivamente os elementos neutros dos grupos G_1 e G_2. Como $|\langle a, b\rangle| = nm = |\langle \alpha, \beta\rangle|$, segue do terceiro item do teorema 10 que n e m são mínimos com essas propriedades. Decorre do item (4) do teorema mencionado que existe um homomorfismo $f : G_1 \longrightarrow G_2$, tal que $f(a) = \alpha$ e $f(b) = \beta$.

Dado $y \in \langle \alpha, \beta\rangle$, existe $i, j \in \mathbb{N}$, com $0 \leq i < n$ e $0 \leq j < m$, tais que $y = \alpha^i \beta^j$. Daí,

sendo $a^ib^j \in \langle a, b\rangle$, temos que

$$f(a^ib^j) = [f(a)]^i\,[f(b)]^j = \alpha^i\beta^j = y$$

Portanto f é sobrejetiva.

Sejam $x, y \in \langle a, b\rangle$, tais que $f(x) = f(y)$. Então, existem $i, j, k, l \in \mathbb{N}$, com $0 \leq i, k < n$ e $0 \leq j, l < m$, tais que $x = a^ib^j$ e $y = a^kb^l$. Daí,

$$f(a^ib^j) = f(a^kb^l) \Rightarrow \alpha^i\beta^j = \alpha^k\beta^l \Rightarrow \beta^{j-l} = \alpha^{k-i} \in \langle a\rangle$$

Como $m := \min\{t : t \in \mathbb{N} \wedge \beta^t \in \langle a\rangle\}$, segue que $m\big|j-l$, logo, $m\big||j-l|$. Entretanto, sendo $0 \leq j, l < n$, conclui-se que $|j-l| = 0$, ou seja, $j = l$. Deste modo, $\alpha^{k-i} = e_2$ e, portanto, $n = o(a)\big|k-i \Rightarrow n\big||k-i| \overset{(**)}{\Rightarrow} k = i$, onde a implicação $(**)$, decorre de termos $0 \leq i, k < n$. Logo, f é injetiva e, portanto, um isomorfismo de G_1 em G_2, ou seja, $G_1 \simeq G_2$. □

3.1 Uma condição de existência

No teorema a seguir, mostraremos que se n, m, s são inteiros positivos e $u \in \mathbb{N}$, então as condições $s^m \equiv 1 \pmod{n}$ e $u(s-1) \equiv 0 \pmod{n}$ são suficientes para a existência de um grupo finito G de ordem nm e de $a, b \in G$ satisfazendo as condições:

$$(*)\begin{cases} G &= \langle a, b\rangle \\ a^n &= e \\ b^m &= a^u \\ ba &= a^sb. \end{cases}$$

Um teorema de existência, afirma a existência de um objeto satisfazendo certas propriedades. A prova de um teorema desta natureza consiste em exibir um objeto e provar que o mesmo tem as propriedades exigidas. É comum, na literatura matemática, apresentar-se o objeto em questão sem fornecer a ideia do que motivou a escolha do mesmo. Por exemplo, no Teorema 4 de Lima (2020, p. 17); Monteiro (1969, p. 39) no Teorema 10; Vieira (2021, p. 397) no Teorema 6.1 e Gonçalves (2017, p. 39), ao comentar sobre o anel dos Quatérnions.

O teorema a seguir (nosso principal resultado) é um teorema de existência. Antes de sua prova, apresentaremos uma motivação para escolha do objeto em questão.

Teorema 12 (Condições suficientes para a existência de um grupo finito G satisfazendo as condições em $(*)$)**.** *Sejam $n, m, s \in \mathbb{N}-\{0\}$ e $u \in \mathbb{N}$. Se $s^m \equiv 1 \pmod{n}$ e $u(s-1) \equiv 0$*

$(\mathrm{mod}\ n)$, *então existe um grupo finito* G *de ordem* nm *e elementos* $a, b \in G$, *tais que*

$$(*)\begin{cases} G &= \langle a, b\rangle \\ a^n &= e \quad , \text{ (e - elemento neutro de } G) \\ b^m &= a^u \\ ba &= a^s b \end{cases}$$

Motivação 1. *Vimos que, se* G_1 *é um grupo finito de ordem* nm *gerado por dois elementos* $\alpha, \beta \in G_1$ *satisfazendo as relações em* $(*)$, *então* $s^m \equiv 1\ (\mathrm{mod}\ n)$, $u(s-1) \equiv 0\ (\mathrm{mod}\ n)$ *e* $G_1 = \{\alpha^i\beta^j : (i,j) \in \mathbb{Z}_n \times \mathbb{Z}_m\}$. *Além disso, dados* $(x,y), (x_1,y_1) \in \mathbb{Z}_n \times \mathbb{Z}_m$, *temos:*

$$\begin{aligned}
(\alpha^x\beta^y)(\alpha^{x_1}\beta^{y_1}) &= \alpha^x(\beta^y\alpha^{x_1})\beta^{y_1} \\
&= \alpha^x(\alpha^{x_1 s^y}\beta^y)\beta^{y_1} \\
&= \alpha^{x+x_1s^y}\beta^{m\cdot q_m(y+y_1)+r_m(y+y_1)} \\
&= \alpha^{x+x_1s^y}\,(\beta^m)^{q_m(y+y_1)}\,\beta^{r_m(y+y_1)} \\
&= \alpha^{x+x_1s^y}\,(\alpha^u)^{q_m(y+y_1)}\,\beta^{r_m(y+y_1)} \\
&= \alpha^{x+x_1s^y+u\cdot q_m(y+y_1)}\beta^{r_m(y+y_1)} \\
&= \alpha^{qn+r_n(x+x_1s^y+u\cdot q_m(y+y_1))}\beta^{r_m(y+y_1)} \\
&= (\alpha^n)^q(\alpha^{r_n(x+x_1s^y+u\cdot q_m(y+y_1))})\beta^{r_m(y+y_1)} \\
&= e^q(\alpha^{r_n(x+x_1s^y+u\cdot q_m(y+y_1))})\beta^{r_m(y+y_1)} \\
&= \alpha^{r_n(x+x_1s^y+uq_m(y+y_1))}\beta^{r_m(y+y_1)}
\end{aligned}$$

Onde $q_m(k)$, *indica o quociente da divisão do inteiro* k *por* m *e* $q = q_n(x + x_1s^y + uq_m(y+y_1))$, *ou seja:*

$$(\alpha^x\beta^y)(\alpha^{x_1}\beta^{y_1}) = \alpha^{r_n(x+x_1s^y+uq_m(y+y_1))}\beta^{r_m(y+y_1)} \tag{1}$$

.

A igualdade em (1) *induz uma operação* $\odot$ *sobre* $\mathbb{Z}_n \times \mathbb{Z}_m$, *dada por:*

$$(x,y) \odot (x_1,y_1) = (r_n(x + x_1s^y + uq_m(y+y_1)), r_m(y+y_1))$$

Esperamos que $(\mathbb{Z}_n \times \mathbb{Z}_m, \odot)$ *seja um grupo (de ordem* nm*) satisfazendo as relações em* $(*)$. *Além disso, se isto for verdade, a função*

$$\begin{aligned}
\varphi : \mathbb{Z}_n \times \mathbb{Z}_m &\longrightarrow G_1 \\
(x,y) &\longmapsto \varphi(x,y) = \alpha^i\beta^j
\end{aligned}$$

deve ser um isomorfismo.

Isto nos dá ideia, de como escolher $a, b \in \mathbb{Z}_n \times \mathbb{Z}_m$*, os quais devem ser tais que* $\varphi(a) = \alpha$ *e* $\varphi(b) = \beta$ *e, então,* $a = (1, 0)$ *e* $b = (0, 1)$*. Também, o elemento neutro de* $G = \mathbb{Z}_n \times \mathbb{Z}_m$ *deve ser* $e = (0, 0)$*.*

Além disso, para que todo elemento $(x, y) \in \mathbb{Z}_n \times \mathbb{Z}_m$ *seja simetrizável, devem existir* $x_1 \in \mathbb{Z}_n$ *e* $y_1 \in \mathbb{Z}_m$*, tais que*

$$(x, y) \odot (x_1, y_1) = e = (x_1, y_1) \odot (x, y)$$

Mas isso ocorre se, e somente se,

$$\begin{cases} r_n(x + x_1 s^y + u \cdot q_m(y + y_1)) & = 0 \\ r_n(x_1 + x s^{y_1} + u \cdot q_m(y_1 + y)) & = 0 \\ r_m(y + y_1) & = 0 \end{cases}$$

Da terceira equação, obtemos que $m \big| y + y_1$*. como* $y, y_1 \in \mathbb{Z}_m$*, temos que* $0 \leq y + y_1 < 2m$*. Daí, devemos ter* $y = y_1 = 0$ *ou* $y + y_1 = m$*, ou seja, temos* $y = y_1 = 0$ *ou* $y_1 = m - y$*; se* $y \neq 0$*. No primeiro caso, temos:*

$$\begin{cases} r_n(x + x_1 s^0 + u \cdot q_m(0 + 0)) & = 0 \\ r_n(x_1 + x s^0 + u \cdot q_m(0 + 0)) & = 0 \end{cases}$$

Como $q_m(0) = 0$*, então* $r_n(x + x_1) = 0$*, isto é,* $n \big| x + x_1$*. De modo análogo, devemos ter* $x = x_1 = 0$ *ou* $x_1 = n - x$*. Dessa forma, obtemos:*

$$(x_1, y_1) = \begin{cases} (0, 0), & \text{se } x = y = 0 \\ (n - x, 0) & \text{se } x \neq 0 \wedge y = 0 \end{cases}$$

No segundo caso, como $q_m(m) = 1$*, temos:*

$$\begin{cases} r_n(x + x_1 s^y + u \cdot q_m(m)) & = 0 \\ r_n(x_1 + x s^{m-y} + u \cdot q_m(m)) & = 0 \\ r_m(m) & = 0 \end{cases} \implies \begin{cases} r_n(x + x_1 s^y + u) & = 0 \\ r_n(x_1 + x s^{m-y} + u) & = 0 \\ 0 & = 0 \end{cases}$$

Da segunda equação, obtemos $x_1 \equiv (-x s^{m-y} - u) \pmod{n}$ *e, sendo* $x_1 \in \mathbb{Z}_n$*, então* $x_1 = r_n(x_1) = r_n(-x s^{m-y} - u)$*.*

Por outro lado, da primeira equação, obtemos $x_1 s^y \equiv (-x - u) \pmod{n}$*. Como assumimos que* $1 \equiv s^m \pmod{n}$*, então* $x_1 \equiv x_1 s^m \pmod{n}$*. Daí,*

$$x_1 \equiv x_1 s^m \equiv (x_1 s^y)(s^{m-y}) \equiv (-x - u)(s^{m-y}) \equiv (-x s^{m-y} - u s^{m-y}) \pmod{n}$$

Além disso, de $u(s-1) \equiv 0 \pmod{n}$*, obtemos* $us \equiv u \pmod{n}$*. Por indução, podemos concluir que* $us^k \equiv u \pmod{n}, \forall k \in \mathbb{N}$*. Em particular, temos que* $us^{m-y} \equiv u \pmod{n}$*. Isso nos permite obter* $x_1 \equiv (-xs^{m-y} - u) \pmod{n}$*. Daí,*

$$x_1 = r_n(x_1) = r_n(-xs^{m-y} - u)$$

Logo, a solução do sistema para $y \neq 0$ *é o par* $(r_n(-xs^{m-y} - u), m - y)$*.*

Em síntese, nosso candidato a inverso do elemento $(x, y) \in G$ *é o elemento* $(x_1, y_1) \in G$*, dado por:*

$$(x,y)^{-1} = (x_1, y_1) = \begin{cases} (0,0), & \text{se } x = y = 0 \\ (n-x, 0), & \text{se } y = 0 \\ (r_n(-xs^{m-y} - u), m - y), & \text{se } y \neq 0 \end{cases}$$

Com essas considerações, inciemos a prova do teorema em questão.

Demonstração. Inciaremos mostrando que $e := (0,0)$ é o elemento neutro de G relativamente à operação $\odot$. Para isso, tomemos $(x, y) \in G$, então:

$$\begin{aligned} (x,y) \odot (0,0) &= (r_n(x + 0s^y + uq_m(y + 0), r_m(y + 0)) \\ &= (r_n(x + uq_m(y), r_m(y)) \\ &= (r_n(x + u \cdot 0), r_m(y)) \\ &= (r_n(x), r_m(y)) \\ &= (x, y) \end{aligned}$$

$$\begin{aligned} (0,0) \odot (x,y) &= \big(r_n(0 + xs^0 + uq_m(0 + y), r_m(0 + y)\big) \\ &= (r_n(x + u \cdot 0), r_m(y)) \\ &= (r_n(x), y) \\ &= (x, y) \end{aligned}$$

Segue-se que e é o elemento neutro de G relativamente à operação $\odot$.

Agora, dado $(x, y) \in G$, seja $(x_1, y_1) \in G$, definido por:

$$(x_1, y_1) = \begin{cases} (0,0), & \text{se } x = y = 0 \\ (n-x, 0), & \text{se } y = 0 \\ (r_n(-xs^{m-y} - u), m - y), & \text{se } y \neq 0 \end{cases}$$

Mostraremos que $(x, y)^{-1} = (x_1, y_1)$.

$1^{\underline{o}}$ Caso: $(x, y) = (0, 0)$. Neste caso, temos

$$\begin{aligned}(x, y) \odot (x_1, y_1) &= (0, 0) \odot (0, 0) \\ &= \big(r_n(0 + 0s^0 + uq_m(0 + 0)), r_m(0 + 0)\big) \\ &= (r_n(0 + 0 + u \cdot 0), 0) \\ &= (0, 0)\end{aligned}$$

$$\therefore (x, y) \odot (x_1, y_1) = (0, 0) = (x_1, y_1) \odot (x, y)$$

$2^{\underline{o}}$ Caso: $y = 0$. Neste caso, $(x_1, y_1) = (n - u, 0)$. Temos, então:

$$\begin{aligned}(x, y) \odot (x_1, y_1) &= (x, 0) \odot (n - x, 0) \\ &= \big(r_n(x + (n - x)s^0 + uq_m(0 + 0)), r_m(0 + 0)\big) \\ &= (r_n(x + n - x + uq_m(0)), r_m(0)) \\ &= (r_n(n + u \cdot 0), 0) \\ &= (r_n(n), 0) \\ &= (0, 0)\end{aligned}$$

$$\therefore (x_1, y_1) \odot (x, y) = (0, 0)$$

$$\begin{aligned}(x_1, y_2) \odot (x, y) &= (n - x, 0) \odot (x, 0) \\ &= \big(r_n((n - x) + xs^0 + uq_m(0 + 0)), r_m(0 + 0)\big) \\ &= (r_n(n - x + x + u \cdot 0), 0) \\ &= (r_n(n), 0) \\ &= (0, 0)\end{aligned}$$

$$\therefore (x, y) \odot (x_1, y_1) = (0, 0)$$

$3^{\underline{o}}$ Casos: $y \neq 0$. Neste caso, $(x_1, y_1) = (r_n(-xs^{m-y} - u), m - y)$. Então:

$$\begin{aligned}(x, y) \odot (x_1, y_1) &= (x, y) \odot (r_n(-xs^{m-y} - u), m - y) \\ &= \big(r_n(x + r_n(-xs^{m-y} - u)s^y + uq_m(y + (m - y)), r_m(y + (m - r)\big) \\ &= \big(r_n(x + (-xs^{m-y} - u)s^y + uq_m(m)), r_m(m)\big) \\ &= (r_n(x - xs^m - us^y + u \cdot 1, 0) \\ &= (r_n(x(1 - s^m) - us^y + u, 0)\text{ , mas } 1 - s^m \equiv 0 \pmod{n} \text{ e } us^y \equiv u \pmod{n} \\ &= (r_n(x \cdot 0 - u + u), 0) \\ &= (0, 0)\end{aligned}$$

$$\therefore (x_1, y_1) \odot (x, y) = (0, 0)$$

$$\begin{aligned}
(x_1, y_1) \odot (x, y) &= (r_n(-xs^{m-y} - u), m - y) \odot (x, y) \\
&= \big(r_n(r_n(-xs^{m-y} - u) + xs^{m-y} + uq_m((m - y) + y)), r_m((m - y) + y)\big) \\
&= \big(r_n(-xs^{m-y} - u + xs^{m-y} + uq_m(m)), r_m(m)\big) \\
&= (r_n(-u + u \cdot 1), 0) \\
&= (0, 0)
\end{aligned}$$

$$\therefore (x, y) \odot (x_1, y_1) = (0, 0)$$

Em ambos os casos, mostramos que $(x, y) \odot (x_1, y_1) = e = (x_1, y_1) \odot (x, y)$. Isso nos possibilita concluir que

$$(x, y)^{-1} = (x_1, y_1) = \begin{cases} (0, 0) & \text{se } x = 0 \wedge y = 0 \\ (n - x, 0), & \text{se } y = 0 \\ (r_n(-xs^{m-y} - u), m - y), & \text{se } y \neq 0 \end{cases}$$

Deste modo, para concluir que $(G, \odot)$ é um grupo, resta verificar que a operação $\odot$ sobre G é associativa. Sejam $\alpha, \beta, \gamma \in G$, então existem $x, x_1, x_2 \in \mathbb{Z}_n$ e $y, y_1, y_2 \in \mathbb{Z}_m$, tais que $\alpha = (x, y), \beta = (x_1, y_1)$ e $\gamma = (x_2, y_2)$. Apenas aplicando a definição da operação, obtemos o seguinte resultado para $(\alpha \odot \beta) \odot \gamma$:

$$\big(r_n(r_n(x + x_1 s^y + uq_m(y + y_1)) + x_2 s^{r_m(y+y_1)} + uq_m(r_m(y + y_1) + y_2)), r_m(r_m(y + y_1) + y_2)\big)$$

Indiquemos por t_1 e t_2, respectivamente, a primeira e segunda componente do elemento $(\alpha \odot \beta) \odot \gamma$. Daí,

$$\begin{aligned}
t_2 &= r_m(r_m(y + y_1) + y_2) \\
&= r_m(r_m(y + y_1) + r_m(y_2)) \\
&= r_m(y + y_1 + y_2) \\
&= r_m(r_m(y) + r_m(y_1 + y_2)) \\
&= r_m(y + r_m(y_1 + y_2))
\end{aligned}$$

Por outro lado, para a primeira componente, temos:

$$\begin{aligned}
t_1 &= r_n(r_n(x + x_1 s^y + uq_m(y + y_1)) + x_2 s^{r_m(y+y_1)} + uq_m(r_m(y + y_1) + y_2)) \\
&\overset{\text{(i)}}{=} r_n(x + x_1 s^y + uq_m(y + y_1) + x_2 s^{y+y_1} + uq_m(r_m(y + y_1) + y_2)) \\
&\overset{\text{(iii)}}{=} r_n(x + (x_1 + x_2 s^{y_1})s^y + u(q_m(y + y_1) + q_m(r_m(y + y_1) + y_2)) \\
&\overset{\text{(iii)}}{=} r_n(x + (x_1 + x_2 s^{y_1})s^y + uq_m(y + y_1 + y_2) \\
&\overset{\text{(iii)}}{=} r_n(x + (x_1 + x_2 s^{y_1})s^y + u(q_m(y_1 + y_2) + q_m(y + r_m(y_1 + y_2)))) \\
&= r_n(x + (x_1 + x_2 s^{y_1})s^y + uq_m(y_1 + y_2) + uq_m(y + r_m(y_1 + y_2))) \\
&\overset{\text{(iv)}}{=} r_n(x + (x_1 + x_2 s^{y_1})s^y + us^y q_m(y_1 + y_2) + uq_m(y + r_m(y_1 + y_2))) \\
&= r_n(x + (x_1 + x_2 s^{y_1} + uq_m(y_1 + y_2))s^y + uq_m(y + r_m(y_1 + y_2))) \\
&= r_n(x + (r_n(x_1 + x_2 s^{y_1} + uq_m(y_1 + y_2)))\, s^y + uq_m(y + r_m(y_1 + y_2)))
\end{aligned}$$

Ou seja,

$$\begin{aligned}
(\alpha \odot \beta) \odot \gamma = (&r_n(x + (r_n(x_1 + x_2 s^{y_1} + uq_m(y_1 + y_2)))\, s^y \\
&+ uq_m(y + r_m(y_1 + y_2))), r_m(y + r_m(y_1 + y_2)))
\end{aligned}$$

Assim, obtemos:

$$\begin{aligned}
(\alpha \odot \beta) \odot \gamma &= (x, y) \odot ((r_n(x_1 + x_2 s^{y_1} + uq_m(y_1 + y_2)), r_m(y_1 + y_2)) \\
&= (x, y) \odot ((x_1, y_1) \odot (x_2, y_2)) \\
&= \alpha \odot (\beta \odot \gamma)
\end{aligned}$$

Logo, a operação $\odot$ sobre G é associativa e, portanto, $(G, \odot)$ é um grupo. Agora, precisamos mostrar que existem elementos $a, b \in G$ satisfazendo as relações em $(*)$. Pondo $a := (1, 0)$ e $b := (0, 1)$, observe que

$$a^2 = a \odot a = (1, 0) \odot (1, 0) = \big(r_n(1 + 1s^0 + uq_m(0 + 0)), r_m(0 + 0)\big) = (r_m(2), 0)$$

Isso nos indica que possivelmente teremos, para $k \in \mathbb{N}$, $a^k = (r_n(k), 0)$. De fato,

---

(i) $r_n(\sum_{i=1}^{k} x_i) = r_n(\sum_{i=1}^{k} r_n(x_i)), \forall k \in \mathbb{N} \wedge \forall x_i \in \mathbb{Z}$

(ii) $s^{y+y_1} \equiv s^{r_m(y+y_1)} \pmod{n}$

(iii) $q_m(y + y_1) + q_m(r_m(y + y_1) + y_2) = q_m(y + y_1 + y_2) = q_m(y_1 + y_2) + q_m(y + r_m(y_1 + y_2))$

(iv) $u(s - 1) \equiv 0 \mod n \Rightarrow us^y \equiv u \mod n$

$a^0 = (0,0) = (r_n(0),0)$. Supondo que $a^k = (r_n(k),0)$, para algum $k \in \mathbb{N} - \{0\}$, então

$$\begin{aligned} a^{k+1} &= a^k \odot a \\ &= (r_n(k),0) \odot (1,0) \\ &= \big(r_n(r_n(k) + 1s^0 + uq_m(0+0), r_m(0+0)\big) \\ &= (r_n(r_n(k) + r_n(1)) + u \cdot 0), 0) \\ &= (r_n(k+1),0) \end{aligned}$$

Pelo Princípio de Indução, temos que $a^k = (r_n(k),0)$, para todo $k \in \mathbb{N}$. Como consequência, $a^k = (k,0) \neq (0,0)$, para todo $k \in \mathbb{N}$; com $0 < k < n$ e $a^n = (r_n(n),0) = (0,0) = e$. Logo, $o(a) = n$.

Além disso, note que $b^2 = b \odot b = (0,1) \odot (0,1) = (r_n(0 + 0s^1 + uq_m(1+1)), r_m(1+1)) = (r_n(uq_m(2)), r_m(2))$; isso nos leva a conjecturar que $b^k = (r_n(uq_m(k)), r_m(k))$. Para $k = 0$, temos $b^0 = (0,0) = (r_n(uq_m(0)), r_m(0))$. Para algum $k \in \mathbb{N} - \{0\}$, suponha que $b^k = (r_n(uq_m(k)), r_m(k))$. Então,

$$\begin{aligned} b^{k+1} &= b^k \odot b \\ &= (r_n(uq_m(k)), r_m(k)) \odot (0,1) \\ &= \big(r_n(r_n(uq_m(k)) + 0s^{r_m(k)} + uq_m(r_m(k)+1), r_m(r_m(k)+1)\big) \\ &= (r_n(uq_m(k) + uq_m(r_m(k)+1), r_m(k+1)) \\ &= (r_n(u(q_m(k) + q_m(r_m(k)+1), r_m(k+1)) \\ &= (r_n(u(q_m(k) + 0 + q_m(r_m(k) + r_m(1)), r_m(k+1)) \\ &= (r_n(u(q_m(k) + q_m(1) + q_m(r_m(k) + r_m(1)), r_m(k+1)) \\ &\overset{(v)}{=} \big(r_n(uq_m(k+1)), r_m(k+1)\big) \end{aligned}$$

Novamente, pelo Princípio de Indução, temos $b^k = (r_n(uq_m(k)), r_m(k))\ \forall k \in \mathbb{N}$. Daí,

$$b^m = (r_n(uq_m(m)), r_m(m)) = (r_n(u \cdot 1)), 0) = (r_n(u), 0) = a^u$$

Além disso, se $k \in \mathbb{N}$ e $0 < k < m$, então

$$b^k = (r_n(uq_m(k)), r_m(k)) = (r_n(u \cdot 0), k) = (0,k) \neq a^u$$

Observe que $\langle a \rangle = \big\{a^k : k \in \mathbb{Z}\big\} = \{(r_n(k),0) : k \in \mathbb{Z}\}$. Como $b^k = (0,k) \notin \langle a \rangle$, sempre que k é um inteiro entre 0 e m, podemos concluir que $m = \min\{t : t \in \mathbb{N} - \{0\} \wedge b^t \in \langle a \rangle\}$.

(v) $q_m(a+b) = q_m(a) + q_m(b) + q_m(r_m(a) + r_m(b)), \forall a, b \in \mathbb{Z}$

Também, temos que

$$\begin{aligned} a^s \odot b &= (r_n(s), 0) \odot (0, 1) = \big(r_n(r_n(s) + 0s^0 + uq_m(0 + 1)), r_m(0 + 1)\big) \\ &= (r_m(s + uq_m(1)), r_m(1)) \\ &= b \odot a \end{aligned}$$

Como n e m são mínimos satisfazendo $a^n = e$ e $b^m \in \langle a \rangle$, pelo item (3) do teorema 10, segue-se que $|\langle a, b \rangle| = nm$. Mas $|G| = \big|\mathbb{Z}_n \times \mathbb{Z}_m\big| = \big|\mathbb{Z}_n\big| \cdot \big|\mathbb{Z}_m\big| = nm$ e, portanto, $G = \langle a, b \rangle$. □

3.2 Aplicações

A prova que apresentamos do Teorema Principal foi construtiva: além de garantir a existência de grupos finitos gerados por dois elementos satisfazendo certas relações, ela nos permite descrever explicitamente o conjunto subjacente e a operação que o torna um grupo. Deste modo, para ilustrar a pertinência e a utilidade do resultado, mostraremos como ele pode ser utilizado para garantir a existência de certas famílias clássicas de grupos, como os quatérnions generalizados Q_n e os grupos diedrais D_n. Além disso, apresentamos uma aplicação adicional do teorema, esta, no contexto da classificação de grupos: a partir dele é possível listar, a menos de isomorfismos, todos os grupos de ordem $2p$, com p primo ímpar. Esse resultado fornece uma descrição completa e elegante dos possíveis modelos de grupos para essa classe de ordens.

1º Aplicação: Sejam $n \in \mathbb{N} - \{0, 1, 2\}, m = 2, u = 0$ e $s = n - 1$, então $s^m = (n-1)^2 \equiv 1 \pmod{n}$ e $u(s-1) = 0(n-2) = 0 \equiv 0 \pmod{n}$. Logo, existe um grupo finito G de ordem $nm = 2n$ e $\alpha, \beta \in G$, tais que

$$(*) \begin{cases} G &= \langle \alpha, \beta \rangle \\ \alpha^n &= e \quad (e \text{ - elemento neutro de } G) \\ \beta^m &= \alpha^u \\ \beta\alpha &= \alpha^s\beta \end{cases}$$

O grupo G acima é único (a menos de isomorfismos) e, pela nossa demonstração anterior, $G = \mathbb{Z}_n \times \mathbb{Z}_2$ e a operação em G é dada por

$$(x, y) \odot (x_1, y_1) = (r_n(x + x_1(n-1)^y), r_2(y + y_1))$$

para todos $(x, y), (x_1, y_1) \in G$ e α e β são, respectivamente, $(1, 0)$ e $(0, 1)$.

Uma outra forma de se obter G é considerar α e β as permutações do grupo simétrico

S_n, dadas por

$$\begin{array}{rcl} \alpha, \beta : \{1, 2, \cdots, n\} & \longrightarrow & \{1, 2, \cdots, n\} \\ i & \longmapsto & \alpha(i) = r_n(i) + 1 \\ i & \longmapsto & \beta(i) = \delta_{i1} + (1 - \delta_{i1})(n + 2 - i) \end{array}$$

em que $\delta_{ij} = \begin{cases} 1, & i = j \\ 0, & i \neq j \end{cases}$, ou seja,

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & \cdots & n-1 & n \\ 2 & 3 & 4 & \cdots & n & 1 \end{pmatrix} \quad e \quad \beta = \begin{pmatrix} 1 & 2 & 3 & \cdots & n-1 & n \\ 1 & n & n-1 & \cdots & 3 & 2 \end{pmatrix}$$

e tomar G como o subgrupo de S_n gerado por α e β, i.e., $G = \langle \alpha, \beta \rangle$. Além disso, temos:

(I) $\beta \neq id$ e $\beta^2 = id$.

(II) Para todo $i \in \{1, 2, \cdots, n\}$ e todo $k \in \mathbb{N}$, temos $\alpha^k(i) = r_n(i + (k - 1)) + 1$. Consequentemente, obtemos:

(i) $\alpha^k \neq id$, para $0 < k < n$;

(ii) $\alpha^n = id$

Segue-se que n e $m = 2$ são mínimos satisfazendo as igualdades $\alpha^n = id$ e $\beta^m \in \langle \alpha \rangle$. Portanto, a ordem de $G = \langle \alpha, \beta \rangle$ é $2n$.

Mostraremos agora que as afirmações em (I) e (II) são válidas e, portanto, que valem (i) e (ii).

(I) $\beta(2) = \delta_{2i} + (1 - \delta_{2i})(n + 2 - 2) = 0 + (1 - 0)n = n \neq id(2)$. Logo, $\beta \neq id$. Dado $i \in \{1, 2, \cdots, n\}$, temos: $\beta^2(i) = \beta(\beta(i)) = \beta(\delta_{i1} + (1 - \delta_{i1})(n + 2 - i))$. Então,

$$\begin{aligned} \beta^2(i) &= \begin{cases} \beta(1), & \text{se } i = 1 \\ \beta(n + 2 - i), & \text{se } i \neq 1 \end{cases} \\ &= \begin{cases} 1, & \text{se } i = 1 \\ \beta(j), & \text{se } i \neq 1, \text{ com } j = n + 2 - i \end{cases} \\ &= \begin{cases} 1, & \text{se } i = 1 \\ \delta_{j1} + (1 - \delta_{j1})(n + 2 - j), & \text{se } i \neq 1 \end{cases} \\ &= \begin{cases} 1, & \text{se } i = 1 \\ 0 + (1 - 0)(n + 2 - j) & \text{pois } i \neq 1 \text{ implica } j \geq 2 \end{cases} \\ &= \begin{cases} 1, & \text{se } i = 1 \\ n + 2 - (n + 2 - i), & \text{se } i \neq 1 \end{cases} \end{aligned}$$

$$\beta^2(i) = \begin{cases} 1, & \text{se } i = 1 \\ i, & \text{se } i \neq 1 \end{cases}$$

Segue-se que $\beta^2(i) = i = id(i)$, para todo $i \in \{1, 2, \cdots, n\}$. Portanto, $\beta^2 = id$.

(II) Dado $i \in \{1, 2, \cdots, n\}$, temos $\alpha(i) = r_n(i) + 1 = r_n(i + (1 - 1)) + 1$. Dado $k \in \mathbb{N}$, suponhamos que $\alpha^k(i) = r_n(i + (k - 1)) + 1$. Daí,

$$\begin{aligned} \alpha^{k+1}(i) &= \alpha^k(\alpha(i)) \\ &= \alpha^k(r_n(i) + 1) \\ &= \alpha^k(j), \qquad \text{com } j = r_n(i) + 1 \\ &= r_n(j + (k - 1)) + 1 \\ &= r_n(r_n(i) + 1 + (k - 1)) + 1 \\ &= r_n(r_n(i) + k) + 1 \\ &= r_n(r_n(r_n(i)) + r_n(k)) + 1 \\ &= r_n(r_n(i) + r_n(k)) + 1 \\ &= r_n(i + k) + 1 \\ &= r_n(i + ((k + 1) - 1)) + 1. \end{aligned}$$

Pelo Princípio de Indução, segue-se que $\alpha^k(i) = r_n(i+(k-1))+1$, para todo $k \in \mathbb{N}$ e todo $i \in \{1, 2, \cdots, n\}$. Como consequência, se $0 < k < n$, então $\alpha^k(1) = r_n(1 + (k - 1)) + 1 = r_n(k) + 1 = k + 1 \neq 1 = id(1)$. Logo, $\alpha^k \neq id$.

Agora, dado $i \in \{1, 2, \cdots, n\}$, temos:

$$\begin{aligned} \alpha^n(i) &= r_n(i + (n - 1)) + 1 \\ &= \begin{cases} r_n(1 + (n - 1)) + 1, & \text{se } i = 1 \\ r_n((i - 1) + n) + 1 & \text{se } i \neq 1 \end{cases} \\ &= \begin{cases} r_n(n) + 1, & \text{se } i = 1 \\ r_n(r_n(i - 1) + r_n(n)) + 1 & \text{se } i \neq 1 \end{cases} \\ &= \begin{cases} 0 + 1, & \text{se } i = 1 \\ r_n(i - 1) + 1 & \text{se } i \neq 1 \end{cases} \end{aligned}$$

$$\alpha^n(i) = \begin{cases} 1, & \text{se } i = 1 \\ (i-1)+1 & \text{se } i \neq 1 \end{cases}$$
$$= \begin{cases} 1, & \text{se } i = 1 \\ i, & \text{se } i \neq 1 \end{cases}$$
$$= i = id(i)$$

Portanto, $\alpha^n = id$.
Para completar, mostremos que $\beta\alpha = \alpha^{n-1}\beta$. Dado $i \in \{1, 2, \cdots, n\}$, então

$$(\beta\alpha)(i) = \beta(\alpha(i)) = \beta(r_n(i)+1)$$
$$= \begin{cases} \beta(i+1), & \text{se } i \neq n \\ \beta(1), & \text{se } i = n \end{cases}$$
$$= \begin{cases} \delta_{(i+1)1} + (1-\delta_{(1+i)1})((n+2)-(i+1)), & \text{se } i \neq n \\ 1, & \text{se } i = n \end{cases}$$
$$= \begin{cases} (n+2)-(i+1), & \text{se } i \neq n \\ 1, & \text{se } i = n \end{cases}$$
$$= \begin{cases} n+1-i, & \text{se } i \neq n \\ 1, & \text{se } i = n \end{cases}$$
$$= \delta_{in} + (1-\delta_{in})(n+1-i)$$

Logo, $(\beta\alpha)(i) = \delta_{in} + (1-\delta_{in})(n+1-i)$. Por outro lado, temos:

$$(\alpha^{n-1}\beta)(i) = \alpha^{n-1}(\beta(i))$$
$$= \alpha^{n-1}(\delta_{i1} + (1-\delta_{i1})(n+2-i))$$
$$= \begin{cases} \alpha^{n-1}(1), & \text{se } i = 1 \\ \alpha^{n-1}(n+2-i), & \text{se } i \neq 1 \end{cases}$$
$$= \begin{cases} r_n(1+((n-1)-1))+1, & \text{se } i = 1 \\ r_n((n+2-i)+((n-1)-1))+1, & \text{se } i \neq 1 \end{cases}$$

$$
\begin{aligned}
(\alpha^{n-1}\beta)(i) &= \begin{cases} r_n(n-1)+1, & \text{se } i=1 \\ r_n(n+(n-i))+1, & \text{se } i\neq 1 \end{cases} \\
&= \begin{cases} (n-1)+1, & \text{se } i=1 \\ r_n(n-i)+1, & \text{se } i\neq 1 \end{cases} \\
&= \begin{cases} (n-1)+1, & \text{se } i=1 \\ (n-i)+1, & \text{se } i\neq 1 \end{cases} \\
&= (n-i)+1 \\
&= \delta_{in}+(1-\delta_{in})(n-i+1) \\
&= \delta_{in}+(1-\delta_{in})(n+1-i) \\
&= (\beta\alpha)(i)
\end{aligned}
$$

Segue-se que $(\beta\alpha)(i) = (\alpha^{n-1}\beta)(i)$, para todo $i \in \{1, 2, \cdots, n\}$. Logo, $\beta\alpha) = \alpha^{n-1}\beta$. Temos, portanto, que G é um grupo finito de ordem $2 \cdot n$, gerado por α e β satisfazendo

$$
\begin{cases} \alpha^n &= id \\ \beta^2 &= id \\ \beta\alpha &= \alpha^{n-1}\beta \end{cases}
$$

O grupo G, neste caso, é chamado de Grupo Diedral de ordem $2n$, o qual é denotado por D_n e coincide (i.e., isomorfo) com o grupo das simetrias de um polígono regular de n lados.

2ª Aplicação: Seja $n \in \mathbb{N}-\{0,1,2\}$. Pondo $n' = 2^{n-1}, m = 2, u = 2^{n-2}$ e $s = 2^{n-1}-1$, temos:

$$s^m = (2^{n-1}-1)^2 = 2^{2n-2} - 2^{n-1} + 1 = 2^{n-1}(2^{n-1}-1)+1 \qquad (I)$$

$$u(s-1) = 2^{n-2}(2^{n-1}-1-1) = 2^{n-2}(2^{n-1}-2) = 2^{n-1}(2^{n-2}-1) \qquad (II)$$

De (I) e (II), pelo nosso teorema principal, existe um grupo G de ordem $n'm = 2^n$, gerado por dois elementos $\alpha, \beta \in G$, tais que:

$$
\begin{cases} \alpha^{2^{n-1}} &= e \\ \beta^2 &= \alpha^{2^{n-2}} \\ \beta\alpha &= \alpha^{2^{n-1}-1}\beta \end{cases}
$$

O grupo G acima é chamado dos *quatérnions generalizados* e é denotado por Q_n. Também podemos obter este grupo como um subgrupo de $GL_2(\mathbb{C})$ das matrizes quadradas de ordem 2 com entradas complexas, chamado de o *grupo linear geral sobre* $\mathbb{C}$, do seguinte

modo.

Sejam $a = e^{\frac{2\pi i}{2^{n-1}}}, \alpha = \begin{bmatrix} a & 0 \\ 0 & a^{-1} \end{bmatrix}$ e $\beta = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$. Temos que

$$\begin{cases} \alpha^{2^{n-1}} & = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \\ \beta^2 & = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} = \alpha^{2^{n-2}} \\ \beta\alpha & = \alpha^{2^{n-1}-1}\beta \end{cases}$$

Por indução, temos que $\alpha^k = \begin{bmatrix} a^k & 0 \\ 0 & a^{-k} \end{bmatrix}$, para todo $k \in \mathbb{N}$. Mas, para todo $k \in \mathbb{N}$; com $0 < k < 2^{n-1}$, temos $a^k = e^{\frac{2\pi ki}{2^{n-1}}} = \cos(\frac{2\pi k}{2^{n-1}}) + i\sin(\frac{2\pi k}{2^{n-1}}) \neq 1$. Daí, concluímos que $n = 2^{n-1}$ e $m = 2$ são mínimos satisfazendo $\alpha^n = e$ e $\beta^m \in \langle\alpha\rangle$. Logo, $|Q_n| = nm = 2^n$.

Observação 18. *$Q_n \ncong D_{2^{n-1}}$, pois, Q_n possui um único elemento de ordem 2, o elemento $\begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}$, enquanto que em $D_{2^{n-1}}$, todos os elementos $\beta, \alpha\beta, \alpha^2\beta, \cdots, \alpha^{2^{n-1}-1}\beta$ (as rotações espaciais, caso $D_{2^{n-1}}$ seja o grupo de simetria de um polígono regular de 2^{n-1} lados) têm ordem 2.*

3º Aplicação: Seja $p \in \mathbb{N}$ um número primo ímpar. Mostraremos que $\mathbb{Z}_{2p}$ e D_p são os únicos grupos de ordem $2p$, a menos de isomorfismos.

Seja G um grupo de ordem $2p$. Inicialmente, mostraremos que: (i) G possui um elemento a de ordem p e (ii) G possui um elemento b de ordem 2.

Se G for cíclico gerado por γ, tome $a := \gamma^2$. Se G não for cíclico, então, pelo Teorema de Lagrange, temos $o(g) \in \{2, p\}, \forall g \in G - \{e\}$. Suponha por absurdo que G não possui elemento de ordem p, então G é abeliano. Daí, Se $a \in G$ e $b \in G - \langle a\rangle$, então

$$\begin{cases} a^2 & = e \\ b^2 & = e \in \langle a\rangle \\ ba & = a^1 b \end{cases}$$

E portanto, $|\langle a, b\rangle| = 2 \cdot 2 = 4$, uma contradição, pois $4 \not| 2p$. Isso mostra que G admite elemento de ordem p, o qual representaremos por a.

Seja $H := \langle a\rangle$, como $|H| = p$, então $(G : H) = 2$. Pelo exercício 21, concluímos que $H \trianglelefteq G$. Seja $g \in G - H$. Como $gH \in (G/H)$ e $|(G/H)| = 2$, então $(gH)^2 = eH$. Daí, $g^2 \in H$. Logo,

$$|\langle g^2\rangle| \big| |H| \Rightarrow |\langle g^2\rangle| \in \{1, p\}$$

Temos, então, dois casos a analisar:

$1^{\underline{o}}$ Caso: $o(g^2) = 1$. Neste caso, $g^2 = (g^2)^1 = e$ e, como $g \neq e$, concluímos que $o(g) = 2$. Daí, ponha $b := g$.

$2^{\underline{o}}$ Caso: $o(g^2) = p$. Neste caso, $(g^2)^p = e$, isso implica que $o(g^p) = 2$. Daí, ponha $b := g^p$.

Portanto, G possui um elemento de ordem 2 em ambos os casos. Seja b este elemento.

Em síntese, já obtemos $n := p, m := 2$ e, como $b^2 = e = a^0$, escolheremos $u = 0$. Assim, basta determinar s para que seja possível utilizar o teorema principal deste trabalho.

Recordemos que, se $\langle a, b\rangle$ é um grupo de nm elementos satisfazendo as relações em $(*)$, então deve ocorrer $s^m \equiv 1 \pmod{p}$, isto é $p \big| s^2 - 1 = (s+1)(s-1)$. Sendo p primo, concluímos que $p|(s+1)$ ou $p|(s-1)$. Isso nos leva a escolher $s = p-1$ ou $s = 1$. Daí, temos

$$\begin{cases} G &= \langle a, b\rangle \\ a^p &= e \\ b^2 &= a^0 \\ ba &= a^{p-1}b \end{cases} \quad \text{ou} \quad \begin{cases} G &= \langle a, b\rangle \\ a^p &= e \\ b^2 &= a^0 \\ ba &= a^1 b \end{cases}$$

No caso em que $s = p-1$, temos que $G \simeq D_p$. Para o caso em que $s = 1$, temos que a e b comutam. Além disso, $\text{mdc}(o(a), o(b)) = \text{mdc}(p, 2) = 1$. Pela proposição 16, concluímos que $o(ab) = o(a)o(b) = 2p$. Logo, G é cíclico e, portanto, isomorfo a $\mathbb{Z}_{2p}$.

4 Considerações Finais

O estudo desenvolvido ao longo deste trabalho teve como propósito provar, por meio de uma demonstração fundamentada principalmente em resultados elementares da teoria dos grupos, que as congruências $s^m \equiv 1 \pmod{n}$ e $u(s-1) \equiv 0 \pmod{n}$, além de necessárias, são condições suficientes para a existência de grupos finitos da forma $G = \langle a, b\rangle$, definidos pelas relações $a^n = e$, $b^m = a^u$ e $ba = a^s b$. A motivação para essa abordagem decorreu da lacuna expositiva identificada na literatura consultada, na qual o caso $u \neq 0$ é mencionado, mas não demonstrado.

A partir dessa lacuna, buscamos construir uma argumentação que, além de rigorosa, fosse pedagogicamente transparente. A estratégia de apresentar primeiro as implicações algébricas das relações dadas, seguida da construção explícita do grupo como um conjunto de pares ordenados dotado de uma operação cuidadosamente definida, revelou-se adequada para alcançar esse objetivo.

As aplicações apresentadas ao final do Capítulo 3 reforçam o potencial do Teorema Principal como ferramenta para a compreensão de classes importantes de grupos finitos. Em particular, mostramos como os quatérnions generalizados Q_n e o grupo diedral D_n emergem naturalmente como casos especiais das relações $(*)$, e como o resultado obtido permite ainda uma classificação direta e elegante de todos os grupos de ordem $2p$, com p

primo ímpar. Essas aplicações ilustram a utilidade, abrangência e simplicidade estrutural que a apresentação estudada pode oferecer no contexto da classificação de grupos de pequena ordem.

Do ponto de vista didático, acreditamos que o material desenvolvido contribui para tornar mais acessível um tema que, frequentemente, é apresentado por meio de técnicas mais sofisticadas ou com motivações pouco explicitadas. A demonstração construída procura não apenas estabelecer a validade do resultado, mas também oferecer ao leitor o encadeamento conceitual que naturalmente leva às escolhas feitas ao longo do processo.

Como possível desdobramento desta pesquisa, identificamos que Garcia (1985) afirma que, com os mesmos métodos utilizados no caso de dois geradores, pode-se obter um resultado análogo para grupos finitos gerados por três elementos. Ressaltamos, entretanto, que no texto consultado o autor não apresenta demonstração desse fato, limitando-se a enunciar as condições envolvidas.

Mais precisamente, Garcia (1985, p.386-387) afirma que, se $n, m, p, u, t, s, r \in \mathbb{N}$, então, existe um grupo $G = \langle a, b, c \rangle$ de ordem nmp, satisfazendo as relações

$$a^n = e, \qquad b^m = a^u, \qquad c^p = e, \qquad ba = a^t b, \qquad ca = a^s c, \qquad cb = b^r c,$$

se, e somente se, as seguintes congruências abaixo são verificadas:

$$t^m \equiv 1 \pmod{n}, \qquad s^p \equiv 1 \pmod{n}, \qquad r^p \equiv 1 \pmod{(mn/\mathrm{mdc}(u,n))}$$

$$t^{r-1} \equiv 1 \pmod{n}, \qquad u\big(s^z t^y - r^z\big) \equiv 0 \pmod{n}, \qquad 0 \leq y < m, \quad 0 \leq z < p.$$

Assim, um desdobramento natural deste trabalho consiste em investigar se o método construtivo desenvolvido para o caso de dois geradores pode, de fato, ser estendido ao caso de três elementos, de modo a proceder de forma análoga ao que realizamos aqui, produzindo uma demonstração fundamentada e acompanhada da motivação que esclareça os raciocínios envolvidos na prova da afirmação em questão.

Referências

FERREIRA, J. **A construção dos Números**. 4. ed. Rio de Janeiro: SBM – Sociedade Brasileira de Matemática, 2022.

GARCIA, A. Grupos finitos a dois geradores. In: **Anais do 15º Colóquio Brasileiro de Matemática**. Rio de Janeiro: Instituto de Matemática Pura e Aplicada, 1985. p. 381–388. Trabalho apresentado no 15º Colóquio Brasileiro de Matemática, Poços de Caldas, 1985.

GARCIA, A.; LEQUAIN, Y. **Elementos de Álgebra**. 7. ed. Rio de Janeiro: IMPA, 2022.

GONÇALVES, A. **Introdução à Álgebra**. 6. ed. Rio de Janeiro: IMPA, 2017.

LIMA, E. L. **Análise Real: Funções de uma Variável**. 13. ed. Rio de Janeiro: IMPA, 2020.

MILIES, C. P. **História da Álgebra Abstrata: Uma introdução**. São Paulo: Livraria da Física, 2022.

MONTEIRO, L. H. J. **Elementos de Álgebra**. Rio de Janeiro: [s.n.], 1969.

VIEIRA, V. L. **Álgebra Abstrata Básica: Volume I**. 1. ed. São Paulo: Livraria da Física, 2021.