RMAT
ISSN: 2237-8103
REVISTA DE MATEMÁTICA DA UFOP

OPEN ACCESS
Volume 2, Número 1, 2024
https://doi.org/10.5281/zenodo.14563303
Recebido: 11/07/2024
Publicado: 27/12/2024

Grupos de permutação e números de Mersenne: uma interface entre a Teoria dos Grupos e sequências numéricas recorrentes

Permutation groups and Mersenne numbers: an interface between Group Theory and recurring numerical sequences

Grupos de permutación y números de Mersenne: una interfaz entre la teoría de grupos y las secuencias numéricas recurrentes

Renata Teófilo de Sousa
<rtsnaty@gmail.com>
Doutoranda em Ensino da Rede Nordeste de Ensino (RENOEN-Polo IFCE), Fortaleza, CE, Brasil
<https://orcid.org/0000-0001-5507-2691>

Renata Passos Machado Vieira
<re.passosm@gmail.com>
Doutoranda em Ensino da Rede Nordeste de Ensino (RENOEN-Polo UFC), Fortaleza, CE, Brasil
<https://orcid.org/0000-0002-1966-7097>

Francisco Regis Vieira Alves
<fregis@gmx.fr>
Instituto Federal de Educação Ciência e Tecnologia do Estado do Ceará, Fortaleza, CE, Brasil
<https://orcid.org/0000-0003-3710-1561>

Resumo

Este artigo examina grupos de permutação associados a números de Mersenne, especificamente focando em grupos de ordem $2^n - 1$. A investigação aborda as propriedades algébricas e comportamentos especiais desses grupos, destacando suas simetrias e implicações teóricas. Utilizando métodos de análise teórica e exemplos concretos, demonstramos que todos os subgrupos desses grupos são cíclicos e normais, e exploramos os homomorfismos internos e para grupos fator. A análise revela novas perspectivas sobre a interseção entre teoria dos grupos e números de Mersenne, com implicações importantes para a matemática aplicada.

Palavras-chave: *Grupos de Permutação. Números de Mersenne. Teoria dos Grupos.*

Abstract

This article examines permutation groups associated with Mersenne numbers, specifically focusing on groups of order $2^n - 1$. The investigation addresses the algebraic properties and special behaviors of these groups, highlighting their symmetries and theoretical implications. Using theoretical analysis methods and concrete examples, we demonstrate that all subgroups of these groups are cyclic and normal, and we explore internal and factor group homomorphisms. The analysis reveals new perspectives on the intersection between group theory and Mersenne numbers, with important implications for applied mathematics.

Keywords: *Permutation Groups. Mersenne numbers. Group Theory.*

Resumen

Este artículo examina los grupos de permutaciones asociados con los números de Mersenne, centrándose especí-

camente en los grupos de orden $2^n - 1$. La investigación aborda las propiedades algebraicas y comportamientos especiales de estos grupos, destacando sus simetrías e implicaciones teóricas. Utilizando métodos de análisis teóricos y ejemplos concretos, demostramos que todos los subgrupos de estos grupos son cíclicos y normales, y exploramos homomorfismos internos y de grupos factoriales. El análisis revela nuevas perspectivas sobre la intersección entre la teoría de grupos y los números de Mersenne, con importantes implicaciones para las matemáticas aplicadas.

Palabras-Clave: *Grupos de permutación. Números de Mersenne. Teoría de grupos.*

1. INTRODUÇÃO

Os números de Mersenne, expressos na forma 2^n-1, para todo n natural, têm sido objeto de estudo em várias áreas da matemática devido às suas propriedades e aplicações (Alves; Catarino; Mangueira, 2019; Mangueira *et al.*, 2021). Esses números são particularmente relevantes em Teoria dos Números, no que diz respeito ao estudo dos números primos (Vittorio, 1989) e em problemas de fatoração, além de encontrarem aplicação em criptografia e na geração de números pseudoaleatórios (Pizzamiglio; Dorneles; Martinotto, 2008). No entanto, a importância dos números de Mersenne transcende estas aplicações tradicionais, estendendo-se à Teoria dos Grupos, pois eles podem ser relacionados a estruturas algébricas específicas, o que abordamos neste trabalho.

Grupos de permutação são estruturas algébricas formadas por um conjunto de permutações de um conjunto dado, onde a operação binária definida é a composição dessas permutações. Em outras palavras, os elementos de um grupo de permutação são as diferentes formas de rearranjar os elementos de um conjunto, e a operação do grupo consiste em aplicar uma permutação seguida de outra (Garcia; Lequain, 2015; Goncalves, 2017; Herstein, 1970). A ordem de um grupo de permutação é o número total de permutações possíveis, que para este estudo é dada na forma $2^n - 1$, um número de Mersenne. Grupos de permutação de ordem $2^n - 1$ aparecem naturalmente em contextos de simetria e são de particular interesse devido às suas propriedades algébricas e padrões simétricos.

Estudos prévios exploraram números de Mersenne no contexto de números primos e criptografia, conforme mencionado, enquanto trabalhos sobre grupos de permutação têm focado em suas propriedades simétricas. No entanto, uma conexão específica entre grupos de permutação de ordem $2^n - 1$ e números de Mersenne é um campo pouco explorado. Nesse sentido, a motivação para estudar grupos de permutação de ordem $2^n - 1$ reside no interesse de compreender melhor como as propriedades dos números de Mersenne se manifestam em estruturas algébricas. Assim, busca-se investigar novas propriedades desses grupos, contribuir para a Teoria dos Grupos e expandir o entendimento sobre a relação entre números de Mersenne e simetria algébrica.

O objetivo deste artigo é examinar grupos de permutação de ordem $2^n - 1$, investigando suas propriedades e comportamentos simétricos. Pretende-se identificar padrões, simetrias e propriedades algébricas que emergem desses grupos. Buscamos abordar alguns problemas de pesquisa, que podem ser resumidos nas seguintes questões: (a) Quais são as propriedades algébricas específicas dos grupos de permutação de ordem $2^n - 1$? (b) Como esses grupos se comportam em termos de simetria e subestruturas internas?

Aqui abordaremos, exploraremos e analisaremos exemplos concretos de grupos de per-

mutação para diferentes valores de n, analisando suas estruturas e propriedades. Utilizamos subsídio teórico de Mehraban, Deveci e Hincal (2024), Garcia e Lequain (2015), Goncalves (2017) e Herstein (1970) para realizar esta análise, buscando identificar padrões e simetrias que caracterizam esses grupos, bem como alguns trabalhos que incluem Alves (2020), Alves, Catarino e Mangueira (2019), Catarino, Campos e Vasco (2016), Mangueira *et al.* (2021), entre outros estudos relacionados.

2. OS NÚMEROS E A SEQUÊNCIA DE MERSENNE

Os números de Mersenne podem ser obtidos pela expressão, fórmula de Binet para os números de Mersenne, $M_n = 2^n - 1$, onde n é um número natural. Esses números foram nomeados em homenagem ao monge francês Marin Mersenne, que estudou suas propriedades no século XVII. Eles são de particular interesse na teoria dos números e na criptografia, especialmente devido à sua relação com os números primos (Ribenboim, 1996; Koblitz, 1994).

Acerca dos números de Mersenne, uma definição e algumas propriedades podem ser delineadas, como:

Definição 1. *(Números primos de Mersenne). Um número de Mersenne é dito primo se M_n é um número primo. Estes números têm a forma $2^p - 1$, onde p também é um número primo (Ribenboim, 1996).*

Propriedade 2. *(Fatoração e primalidade). Se n é um número composto, então $M_n = 2^n - 1$ não é um número primo e pode ser fatorado. Para que $2^n - 1$ seja primo, n deve ser um número primo. Caso contrário, se n for composto, $2^n - 1$ pode ser fatorado de acordo com a seguinte identidade (Hardy; Wright, 1979; Guy, 2004):*

$$2^{ab} - 1 = (2^a - 1)(2^{a(b-1)} - 1 + 2^{a(b-2)} - 1 + \ldots + 1).$$

Teorema 3. *(Primalidade e Teste de primalidade Lucas-Lehmer). Se p é um número primo, então $2^p - 1$ é divisível por p conforme estabelecido pela teoria dos números e o pequeno teorema de Fermat (Burton, 2010). Além disso, um número de Mersenne da forma $M_p = 2^p - 1$ é primo se, e somente se, o $(p-2)$-ésimo termo da sequência de Lucas-Lehmer for congruente a 0 módulo M_p (Lehmer, 1956).*

Essas duas afirmações estão interligadas no estudo dos números primos, pois tanto a propriedade de divisibilidade quanto o teste de primalidade Lucas-Lehmer exploram a estrutura específica de números que são expressos na forma $2^p - 1$.

Para o teste do Teorema 3, deve-se definir a sequência $s_0 = 4$. Em seguida, calcula-se $s_{(i+1)} = (s_i)^2 - 2$, para $i = 0, 1, 2 \ldots, p-2$. Dito isto, tem-se que $M_p = 2^p - 1$ é primo se, e somente se, $s_{(p-2)} \equiv 0 \pmod{M_p}$.

2.1. Sequência de Mersenne e algumas propriedades

A sequência de Mersenne, composta pelos números $2^n - 1$, com $n \in \mathbb{N}$ (Ribenboim, 1996), pode ser definida por uma relação de recorrência, o que facilita o estudo de suas propriedades.

Conforme Catarino, Campos e Vasco (2016), a relação de recorrência é dada por $M_n = 3M_{n-1} - 2M_{n-2}, n \geq 2$, com os valores iniciais $M_0 = 0, M_1 = 1$.

Desse modo, podemos representar a sequência de Mersenne usando para módulo m, obtendo uma sequência repetida denotada por:

$$\left\{M^{(m)}(n)\right\} = \left\{M^{(m)}(0), M^{(m)}(1), M^{(m)}(2), \ldots, M^{(m)}(n)\right\},$$

em que $M^{(m)}(i) = M(i) \pmod m$ com base na relação $M_n = 3M_{n-1} - 2M_{n-2}$.

Teorema 4. $\left\{M^{(m)}(n)\right\}$ *forma uma sequência simplesmente periódica.*

Demonstração. A sequência se repete, pois há apenas um número finito m^2 de duplos termos possíveis, e a recorrência da dupla resulta na recorrência de todos os termos seguintes. Da definição da sequência de Mersenne temos $M(n) = 3M(n-1) - 2M(n-2)$, então se $M^{(m)}(i+1) = M^{(m)}(j+1), M^{(m)}(i) = M^{(m)}(j)$ logo $M^{(m)}(i-j+1) = M^{(m)}(1), M^{(m)}(i-j) = M^{(m)}(0)$, o que implica que a sequência $\left\{M^{(m)}(n)\right\}$ é periódica. Considerando a notação $kM(m)$ como sendo o menor período de $\left\{M^{(m)}(n)\right\}$ denominando de período da sequência de Mersenne de módulo m. □

A exemplo disso, temos $\left\{M^{(m)}(3)\right\} = \{0, 1, 0, 1, 0, 1, 0, 1, 0, \ldots\}$. Logo $kM(3) = 2$, aparecendo somente números binários, compactuando com a sua fórmula primitiva $2^n - 1$.

É interessante destacar que ao converter a sequência de Mersenne em formato decimal para binário, resulta em: $0, 1, 11, 111, 1111, 11111, 111111, \ldots$ Observa-se o padrão já ocorrendo na sua forma primitiva, seguindo a sequência de números 1s.

Tratando-se da forma matricial estudada por Catarino, Campos e Vasco (2016), temos que $Q = \begin{pmatrix} 0 & 1 \\ -2 & 3 \end{pmatrix}$ e $Q^n = \begin{pmatrix} -2M_{n-1} & M_n \\ -2M_n & M_{n+1} \end{pmatrix}$. Com isso ao elevar a matriz Q, é possível obter os termos da sequência de Mersenne.

Desse modo, seja uma matriz $A = [a_{ij}]_{(k+1)\times(k+1)}$ com a_{ij} números inteiros. Assim $A \pmod m$, significa que todas as entradas de A são reduzidas ao módulo m, ou seja, $A \pmod m \equiv (a_{ij} \pmod m)$. Considere $\langle Q\rangle_{p^\alpha} = \left\{Q^i(\mod p^\alpha) | i \geq 0\right\}$ um grupo cíclico e $|\langle Q\rangle_{p^\alpha}|$ denotando a ordem de $\langle Q\rangle_{p^\alpha}$. Da matriz Q^n, percebe-se que $kM(p^\alpha) = |\langle Q\rangle_{p^\alpha}|$.

Teorema 5. *Seja t o maior inteiro positivo tal que $kM(p) = kM(p^t)$. Então $kM(p^\alpha) = p^{\alpha-t}kM(p)$ para todo $\alpha > t$. Em particular, tem-se que se $kM(p) \neq kM(p^2)$, então $kM(p^\alpha) = p^{\alpha-1}kM(p)$ para todo $\alpha > 1$.*

Demonstração. Seja $kM(p^\alpha)$ uma função que depende de um número primo p e de uma potência α. Desse modo, queremos entender como $kM(p^\alpha)$ se relaciona com $kM(p)$ à medida que α varia.

Assim, t é definido como o maior inteiro positivo, tal que $kM(p) = kM(p^t)$. Isso significa que até o ponto t, a função $kM(p^\alpha)$ não muda o seu valor. Quando $\alpha \geq 1$, observamos que $kM(p^\alpha) = p^{\alpha-t} \cdot kM(p)$. Indicando que para α maiores ou iguais a t, o valor de $kM(p^\alpha)$ é uma multiplicação $kM(p)$ por $p^{\alpha-t}$.

Se $kM(p) \neq kM(p^2)$, implica que a relação $kM(p^\alpha) = p^{\alpha-1} \cdot kM(p)$ vale para todo $\alpha > 1$. Assim, considere um inteiro positivo q. Suponha que $Q^{kM(p^{q+1})} \equiv I \pmod{p^{q+1}}$, onde Q é a matriz geradora de Mersenne e I é a matriz identidade, significando que $Q^{kM(p^{q+1})}$

é congruente a 1 módulo p^{q+1}. Por definição da função, temos $A^{kM(p^{q+1})} \equiv I \pmod{p^q}$, indicando que $kM(p^q)$ divide $kM(p^{q+1})$.

Portanto, o padrão estabelecido mostra como as potências de p afetam a relação $kM(p^\alpha)$ e $kM(p)$, levando à conclusão de que, após um certo ponto, a função $kM(p^\alpha)$ cresce proporcionalmente com $p^{\alpha-t}$.

□

A exemplo, temos para $p = 3$, $q = 1$ e $kM(9) \equiv Q^6 \equiv I \pmod{9}$

$$Q^6 = \begin{pmatrix} 0 & 1 \\ -2 & 3 \end{pmatrix}^6 = \begin{pmatrix} -62 & 63 \\ -126 & 127 \end{pmatrix} \underset{(\mathrm{mod}\ 9)}{} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Seja G um grupo e $x, y \in G$. Se cada elemento de G pode ser escrito como:

$$x^{u_1} y^{u_2} x^{u_3} y^{u_4} \dots x^{u_{m-1}} y^{u_m},$$

onde $u_i \in \mathbf{Z}, 1 \geq i \geq m$. Então dizemos que x, y geram G e que G é um grupo de 2 geradores. Seja G um grupo finito de 2 geradores e X seja o subconjunto de $G \times G$ tal que $(x, y) \in X$ se e somente se G for gerado por x, y. Chamamos (x, y) de par gerador para G.

Teorema 6. *Uma órbita Mersenne de um grupo finito é simplesmente periódico.*

Demonstração. Vamos considerar a órbita de Mersenne de ordem 2 e seja n a ordem de G. Como existem n^2 2-tuplas distintas de elementos de G, pelo menos uma das 2-tuplas aparece duas vezes em uma órbita de Mersenne de ordem 2 de G. Assim, a subsequência após estas 2-tuplas. Por causa da repetição, a órbita generalizada de ordem 2 de Mersenne é periódica. □

3. GRUPOS DE PERMUTAÇÃO E ALGUMAS PROPRIEDADES RELACIONADAS

O Grupo S_n é o grupo de permutações em conjunto de n elementos. Em outras palavras, é o grupo de todas as possíveis maneiras de reordenar n objetos distintos. Este tipo de grupo possuo propriedades algébricas que são utilizadas para modelar simetrias em diversas estruturas matemáticas (Garcia; Lequain, 2015). Nesta seção, exploramos a definição, exemplos e propriedades dos grupos de permutação, com ênfase nos grupos cuja ordem é um número de Mersenne.

Um grupo de permutação S_n é regido pela operação de composição de permutações, e a identidade é a permutação que não altera a posição de nenhum elemento do conjunto (Herstein, 1970). De modo formal temos:

Definição 7. *(Grupo de permutações). Seja X um conjunto de n elementos. Uma permutação de X é uma bijeção $\sigma : X \to X$. O conjunto de todas as permutações de X, com a operação de composição, forma o grupo de permutação S_n.*

As permutações são frequentemente representadas em notação cíclica. Para ilustrar o conceito de grupos de permutação, consideremos um exemplo simples com o conjunto $X = \{1, 2, 3\}$. As permutações deste conjunto são as diferentes maneiras de rearranjar os elementos.

Por exemplo, a permutação que troca o 1 pelo 2, o 2 pelo 3, e o 3 pelo 1 pode ser denotada por $\sigma : 1 \to 2$, $2 \to 3$ e $3 \to 1$ é representada em notação cíclica como $(1\ 2\ 3)$.

De modo análogo, temos a permutação $(1\ 3\ 2)$, que mapeia 1 para 3, 3 para 2, e 2 para 1. Esses exemplos ajudam a visualizar como as permutações operam dentro de um grupo de permutação. Em grupos mais complexos, como S_n, a notação cíclica se torna uma maneira prática para descrever de forma concisa as permutações.

Propriedade 8. *(Ordem). A ordem do grupo S_n é $n!$ (fatorial de n). Isto é, há $n!$ permutações diferentes de n elementos (Dummit; Foote, 2003).*

Demonstração. O número total de maneiras de permutar n elementos é $n!$, pois há n escolhas para a primeira posição, $n-1$ para a segunda, e assim por diante, até 1 escolha para a última posição. Assim, $|S_n| = n!$. □

Propriedade 9. *(Transitividade). Um grupo de permutação G agindo sobre um conjunto X é dito transitivo se, para qualquer par de elementos $x, y \in X$, existe uma permutação $\sigma \in G$ tal que $\sigma(x) = y$ (Dummit; Foote, 2003).*

Exemplo 10. *O grupo S_3 é transitivo, pois qualquer elemento pode ser permutado para qualquer outro elemento por alguma permutação em S_3. Por exemplo, podemos permutar o elemento 1 para o elemento 2 usando a permutação $(1\ 2)$, o elemento 1 para o elemento 3 usando a permutação $(1\ 3)$, e assim por diante.*

Antes de adentrarmos à propriedade 11, explicaremos brevemente o que é um grupo cíclico. Um grupo é chamado de cíclico se existe um elemento dentro dele que pode gerar todos os outros elementos do grupo através da operação do grupo. Em outras palavras, se G é um grupo e existe um elemento g em G tal que qualquer elemento h em G pode ser escrito como uma potência (ou múltiplo, dependendo da operação do grupo) de g, então G é cíclico, e g é chamado de gerador do grupo.

Propriedade 11. *(Ciclicidade). Em geral, S_n não é cíclico para ≥ 3, mas contém subgrupos cíclicos (Dummit; Foote, 2003).*

Demonstração. Um grupo cíclico de ordem n tem exatamente n elementos. Como S_n tem $n!$ elementos para $n \geq 3$, ele não pode ser cíclico. No entanto, subgrupos cíclicos de S_n podem ser formados por permutações de ciclos únicos. □

Considerando um grupo de permutação de ordem $2^n - 1$, as permutações são ainda mais estruturadas, com propriedades específicas que exploraremos na seção a seguir.

4. UMA CARACTERIZAÇÃO DE GRUPOS DE ORDEM $2^n - 1$ E SUAS PARTICULARIDADES

Grupos de permutação de ordem $2^n - 1$ são particularmente interessantes devido à sua conexão com os números de Mersenne. Nesta seção exploramos algumas das suas propriedades específicas.

(i) *Estrutura e Simetria:* Esses grupos exibem uma estrutura simétrica única. Primeiro delinearemos isto a partir de um exemplo: vejamos o caso do grupo de permutação de ordem 7 que é um número de Mersenne, pois $2^3 - 1 = 7$.

Considere o conjunto $X = \{1, 2, 3, 4, 5, 6, 7\}$. As permutações que mantêm a estrutura cíclica de X formam um grupo de ordem 7. No grupo de permutação cíclico C_7 cada elemento é uma permutação dos elementos de X.

Seja g uma permutação definida como $g(i) = i + 1 \pmod 7$. As permutações sucessivas geradas por g são:

$$\begin{aligned} g(1) &= 2 \\ g(2) &= 3 \\ &\cdots \\ g(6) &= 7 \\ g(7) &= 1 \end{aligned}$$

Assim, g gera todas as permutações cíclicas de X, mostrando que C_7 é cíclico e de ordem 7, com uma estrutura que exibe uma simetria cíclica, onde cada permutação é uma rotação dos elementos. Esta estrutura cíclica pode ser generalizada para qualquer grupo cíclico de ordem $2^n - 1$, mostrando padrões simétricos que podem ser úteis para a Teoria dos Grupos e em suas aplicações práticas, como em criptografia.

Generalização da estrutura cíclica: Para demonstrar que C_n é cíclico e de ordem n, vamos considerar a definição de um grupo cíclico de Garcia e Lequain (2015) e mostrar que a permutação g gera todas as permutações cíclicas de X.

Definição 12. *Dado $g : X \to X$, definido por $g(i) = (i \mod n) + 1$. Isso significa que g aplica a seguinte transformação aos elementos de X:*

$$g(i) = \begin{cases} 1 + i, \textit{se } i < n \\ 1, \textit{se } i = n \end{cases}$$

Consideremos as sucessivas aplicações de g:

$$\begin{aligned} g^1(i) &= g(i) = (i \mod n) + 1 \\ g^2(i) &= g(g(i)) = (g(i) \mod n) + 1 \\ &\vdots \\ g^n(i) &= g^{n-1}(g(i)) = i + n \pmod n = i. \end{aligned}$$

Observamos que $g^n(i) = i$, o que significa que a permutação g retorna ao elemento inicial após n aplicações. Isso mostra que g gera todas as permutações cíclicas de X. Além disso, como g gera todas as permutações cíclicas de X, C_n é cíclico e de ordem n. A simetria cíclica é exibida porque cada permutação é uma rotação dos elementos de X. Em outras palavras, g aplica uma rotação que move cada elemento para a posição seguinte, com o último elemento retornando à primeira posição.

Assim, podemos generalizar a demonstração para qualquer grupo cíclico C_n:

$$C_n = \left\{ g^0, g^1, g^2, \ldots, g^{n-1} \right\},$$

onde cada g^k é uma permutação cíclica dos elementos de X.

Quando aplicamos essa estrutura cíclica a grupos de permutação cuja ordem é $2^n - 1$, estamos considerando um conjunto X com $2^n - 1$ elementos. A permutação g definida por $g(i) = (i \mod (2^n - 1)) + 1$ gera todas as permutações cíclicas de X, mostrando que o grupo cíclico $C_{(2^n-1)}$ tem uma estrutura que exibe uma simetria cíclica de ordem $2^n - 1$. De modo formal, tem-se que:

Definição 13. *Dado $g : X \to X$ por $g(i) = (i \mod (2^n - 1)) + 1$. Isso significa que g aplica a seguinte transformação aos elementos de X:*

$$g(i) = \begin{cases} 1 + i, \text{se } i < 2^n - 1 \\ 1, \text{se } i = 2^n - 1 \end{cases}$$

Agora consideremos as sucessivas aplicações de g:

$$\begin{aligned} g^1(i) &= g(i) = (i \mod 2^n - 1) + 1 \\ g^2(i) &= g(g(i)) = (g(i) \mod (2^n - 1)) + 1 = ((i + 1) \mod (2^n - 1)) + 1 \\ &\vdots \\ g^{2^n-1}(i) &= g^{2^n-2}(g(i)) = (i + (2^n - 1)) \mod (2^n - 1) = i \end{aligned}$$

Observamos que $g^{(2^n-1)}(i) = i$, o que significa que a permutação g retorna ao elemento inicial após $2^n - 1$ aplicações, o que mostra que g gera todas as permutações cíclicas de X. Como g gera todas as permutações cíclicas de X, $C_{(2^n-1)}$ é cíclico e de ordem $2^n - 1$. A simetria cíclica é exibida porque cada permutação é uma rotação dos elementos de X.

(ii) *Subgrupos*: Analisar os subgrupos de grupos de permutação de ordem $2^n - 1$ revela especificidades sobre suas simetrias internas. Neste ponto, consideramos especificamente os subgrupos desses grupos de permutação e suas propriedades gerais.

Dado um grupo de permutação G de ordem $2^n - 1$, seus subgrupos podem ser classificados com base nas propriedades cíclicas e nas simetrias envolvidas na estrutura do grupo. Em um grupo cíclico G de ordem $2^n - 1$, todos os subgrupos também são cíclicos. Cada divisor d de $2^n - 1$ corresponde a um subgrupo único de ordem d.

Teorema 14. *Se G é um grupo cíclico de ordem n, então para cada divisor d de n, existe um subgrupo de ordem d.*

Demonstração. Seja $G = \langle g \rangle$ um grupo cíclico gerado por g com ordem $2^n - 1$. Para cada divisor d de $2^n - 1$, consideramos a permutação g^k onde $k = \dfrac{2^n - 1}{d}$. O subgrupo gerado por g^k tem ordem d porque $(g^k)^d = g^{kd} = g^{2^n-1} = e$. □

Proposição 15. *(Subgrupos normais) Em um grupo cíclico, todos os subgrupos são normais. Isso significa que, para qualquer subgrupo $H \leq G$ e para qualquer $g \in G$, temos $ghg^{-1} \in H, \forall h \in H$.*

Demonstração. Seja $G = \langle g \rangle$ um um grupo cíclico gerado por g, e considere $H = \langle g^k \rangle$ como um subgrupo de G, onde k é um divisor de $|G| = 2^n - 1$.

Para mostrar que H é um subgrupo normal de G, precisamos provar que, para qualquer elemento $g^m \in G$ e qualquer elemento $g^{ki} \in H$, a conjugação $g^m g^{ki} g^{-m}$ ainda pertence a H.

Consideremos a conjugação:

$$g^m g^{ki} g^{-m} = g^{m+ki-m} = g^{ki} \in H.$$

Aqui, vemos que a operação de conjugação apenas desloca os expoentes e, em um grupo cíclico, isso não altera a natureza do elemento, que continua sendo um elemento do subgrupo H. Assim, $ghg^{-1} \in H$, para quaisquer $g \in G$ e $h \in H$. Portanto, H é normal em G.

□

Proposição 16. *(Subgrupos de índice 2) Um subgrupo de índice 2 de um grupo G é um subgrupo H tal que $|G : H| = 2$. Isso significa que o grupo fator G/H tem ordem 2. Em um grupo cíclico G de ordem $2^n - 1$, o subgrupo de índice 2 é gerado pelos elementos de G que são quadrados perfeitos no sentido multiplicativo.*

Demonstração. Considere $G = \langle g \rangle$ de ordem $2^n - 1$.

O subgrupo de índice 2 é gerado por g^2, ou seja, consiste em todos os elementos g^{2k} onde k é um inteiro. Isso significa que o subgrupo H de índice 2 é $H = \left\{e, g^2, g^4, g^6, g^8, \ldots, g^{2(2^n-2)}\right\}$. Para mostrar que H tem índice 2, observamos que existem duas classes laterais de H em $G : H$ e gH. Assim, G/H tem ordem 2. □

Exemplo 17. *O grupo C_{15} é um grupo cíclico de ordem 15. Seja g o gerador de C_{15}. Então, $C_{15} = \left\{e, g, g^2, g^3, \ldots, g^{14}\right\}$, onde e é o elemento identidade.*

Os divisores de 15 são $1, 3, 5$ e 15. Portanto, C_{15} tem subgrupos de ordens $1, 3, 5$ e 15.

Considere o subgrupo de ordem 3, gerado por g^5:

$$\langle g^5 \rangle = \left\{e, g^5, g^{10}\right\}.$$

Considere o subgrupo de ordem 5, gerado por g^3:

$$\langle g^3 \rangle = \left\{e, g^3, g^6, g^9, g^{12}\right\}.$$

Considere o subgrupo de índice 2, gerado por g^2:

$$H = \langle g^2 \rangle = \left\{e, g^2, g^4, g^6, g^8, g^{10}, g^{12}, g^{14}\right\}.$$

Esse subgrupo H tem ordem 8 e índice 2, pois há duas classes laterais de H em $C_{15} : H$ e gH. Note que a classe lateral $H = \left\{e, g^2, g^4, g^6, g^8, g^{10}, g^{12}, g^{14}\right\}$ e a classe lateral $gH = \left\{g, g^3, g^5, g^7, g^9, g^{11}, g^{13}\right\}$. O grupo fator C_{15}/H é de ordem 2, consistindo das classes laterais $\{H, gH\}$.

Proposição 18. *(Homomorfismos para Grupos Fator) Considere o homomorfismo $\phi : G \to G/H$ onde H é um subgrupo normal de G. O grupo fator G/H terá ordem $|G|/|H|$ (Herstein, 1970).*

Homomorfismos: Um homomorfismo de grupos é uma função entre dois grupos que preserva a operação do grupo. Para grupos de permutação de ordem $2^n - 1$, podemos explorar algumas propriedades dos homomorfismos.

Demonstração. Seja $G = \langle g \rangle$ de ordem $2^n - 1$ e $H = \langle g^d \rangle$ de ordem d.

O grupo fator G/H é gerado pela classe lateral gH. Como G é cíclico de ordem $2^n - 1$, H é cíclico de ordem d, e G/H será cíclico de ordem $(2^n - 1)/d$. □

Para ilustrar de forma mais detalhada, considere o grupo cíclico $G = C_{15}$ e o subgrupo H gerado por g^3, onde G tem ordem 15 e H tem ordem 5.

Temos que $G = \langle g \rangle$ onde $|G| = 15$. O subgrupo H é gerado por g^3, logo:

$$H = \langle g^3 \rangle = \left\{ e, g^3, g^6, g^9, g^{12} \right\}.$$

Vamos definir um homomorfismo $\phi : G \to G/H$. O grupo fator G/H terá ordem $15/5 = 3$. As classes laterais de H em G são:

$$\begin{aligned} H &= \left\{ e, g^3, g^6, g^9, g^{12} \right\} \\ gH &= \left\{ g, g^4, g^7, g^{10}, g^{13} \right\} \\ g^2H &= \left\{ g^2, g^5, g^8, g^{11}, g^{14} \right\} \end{aligned}$$

Se g é o gerador de G, então a imagem de g em G/H será uma das classes laterais: $\phi(g) = gH$. Para $g^2 \in G : \phi(g^2) = g^2H$.

Verificamos se ϕ preserva a operação do grupo. Para isso, verificamos a multiplicação:

$$\begin{aligned} \phi(g \cdot g) &= \phi(g^2) = g^2H \\ \phi(g) \cdot \phi(g) &= (gH) \cdot (gH) = g^2H. \end{aligned}$$

Isso mostra que $\phi(g \cdot g) = \phi(g) \cdot \phi(g)$, então ϕ é um homomorfismo.

Os subgrupos de grupos de permutação de ordem $2^n - 1$ são todos cíclicos e normais. Homomorfismos entre esses grupos preservam as propriedades cíclicas e podem ser analisados com base nas imagens dos geradores, o que torna essa estrutura fundamental para compreender a simetria e as propriedades algébricas desses grupos.

5. CONSIDERAÇÕES FINAIS

Neste estudo, investigamos algumas propriedades e a estrutura dos grupos de permutação, com foco especial nos grupos de ordem $2^n - 1$. A análise das propriedades desses grupos mostra que eles são cíclicos e possuem subgrupos normais que também são cíclicos. Demonstramos como os homomorfismos podem ser aplicados a esses grupos, preservando suas características estruturais.

Os resultados apresentados têm implicações importantes na Teoria dos Grupos e suas aplicações, permitindo a análise de simetrias destes grupos. Os grupos de permutação de ordem $2^n - 1$ oferecem um campo de investigações adicionais, particularmente em relação à decomposição de grupos e ao estudo de suas simetrias internas.

As propriedades investigadas neste estudo, especialmente a ciclicidade e a normalidade dos subgrupos em grupos de permutação de ordem $2^n - 1$, têm implicações práticas em áreas como a criptografia. A estrutura cíclica desses grupos pode ser explorada no desenvolvimento de algoritmos criptográficos mais eficientes, que dependem fortemente da Teoria dos Números e da Teoria dos Grupos.

Além das aplicações em criptografia, as propriedades dos grupos de permutação de ordem $2^n - 1$ também podem ter implicações na teoria dos códigos, particularmente na construção de

códigos de correção de erros baseados em estruturas algébricas. A periodicidade e ciclicidade desses grupos podem ser exploradas para desenvolver códigos que aproveitam essas características para melhorar a eficiência dos sistemas de comunicação, por exemplo. Além disso, uma análise computacional pode ser conduzida para explorar como as simetrias desses grupos podem ser aplicadas em algoritmos de criptografia e geração de números pseudoaleatórios. Outro possível caminho de pesquisa seria a análise de grupos de permutação em espaços de dimensão superior, explorando como as propriedades cíclicas se manifestam em contextos mais complexos. Essa conexão ainda é pouco explorada e poderia ser um campo fértil para uma pesquisa futura.

AGRADECIMENTOS

A segunda autora agradece ao apoio financeiro da Fundação Cearense de Apoio ao Desenvolvimento Científico e Tecnológico (Funcap). O terceiro autor agradece ao apoio financeiro do Conselho Nacional de Desenvolvimento Científico e Tecnológico - CNPq.

6. REFERÊNCIAS

ALVES, F. R. V. Bivariate mersenne polynomials and matrices. **Notes on Number Theory and Discrete Mathematics**, v. 26, n. 3, p. 83–95, 2020.

ALVES, F. R. V.; CATARINO, P.; MANGUEIRA, M. Discovering theorems about the gaussian mersenne sequence with the maples help. **Annals. Computer Science Series**, v. 17, n. 2, p. 125–133, 2019.

BURTON, D. M. **Elementary Number Theory**. [S.l.]: McGraw-Hill, 2010.

CATARINO, P.; CAMPOS, H.; VASCO, P. On the mersenne sequence. **Annales Mathematicae et Informaticae**, v. 46, p. 37–53, 2016.

DUMMIT, D. S.; FOOTE, R. M. **Abstract Algebra**. [S.l.]: Wiley, 2003.

GARCIA, A.; LEQUAIN, Y. **Elementos de Álgebra**. [S.l.]: Rio de Janeiro: IMPA, 2015.

GONCALVES, A. **Introdução à Álgebra**. 6. ed. [S.l.]: Rio de Janeiro: IMPA, 2017.

GUY, R. K. **Unsolved Problems in Number Theory**. [S.l.]: Springer-Verlag, 2004.

HARDY, G. H.; WRIGHT, E. M. **An Introduction to the Theory of Numbers**. [S.l.]: Oxford University Press, 1979.

HERSTEIN, I. **Tópicos de Álgebra**. [S.l.]: São Paulo: Polígono, 1970.

KOBLITZ, N. **A Course in Number Theory and Cryptography**. [S.l.]: Springer-Verlag, 1994.

LEHMER, D. H. Lucas' test for the primality of mersenne numbers. **Journal of the Australian Mathematical Society**, v. 32, n. 62, p. 12–21, 1956.

MANGUEIRA, M.; VIEIRA, R. P. M.; ALVES, F. R. V.; CATARINO, P. As generalizações das formas matriciais e dos quatérnios da sequência de mersenne. **Revista de Matemática de Ouro Preto**, v. 1, n. 2, p. 1–17, 2021.

MEHRABAN, E.; DEVECI, O.; HINCAL, E. The generalized order (k, t)-mersenne sequences in groups. **Notes on Number Theory and Discrete Mathematics**, v. 30, n. 2, p. 217–282, 2024.

PIZZAMIGLIO, F.; DORNELES, R. V.; MARTINOTTO, A. L. Uma solução paralela para a busca de números primos de mersenne. **Hífen**, v. 32, n. 62, p. 213–220, 2008.

RIBENBOIM, P. **The New Book of Prime Number Records**. [S.l.]: Springer-Verlag, 1996.

VITTORIO, B. **Marin Mersenne: educator of scientists**. 1989. Tese (Doutorado), 1989.