PROFESSOR DE MATEMÁTICA ONLINE
Revista eletrônica da Sociedade Brasileira de Matemática

PMO v.10, n.3, 2022
ISSN: 2319-023X
https://doi.org/10.21711/2319023x2022/pmo1029

Uma fórmula para o número de permutações circulares com repetição via ações de grupos

Guilherme F. S. Silva João A. M. Gondim

Resumo

Na Análise Combinatória que é estudada nos cursos de segundo grau e de início de faculdade, muita ênfase é dada nas permutações. São tratadas permutações lineares simples e com repetição, bem como permutações circulares de elementos distintos, mas nada é mencionado sobre permutações circulares com elementos repetidos. O objetivo deste trabalho é fornecer uma referência em língua portuguesa para uma fórmula usada para tal problema, assim como sua demonstração, a qual passa pela Teoria de Ações de Grupos e pelo Lema de Burnside. Esses tópicos são, também, tratados de forma resumida ao longo deste texto para efeito de completude.

Palavras-chave: Permutações circulares com repetição; Ações de grupos; Lema de Burnside.

Abstract

In the Combinatorics studied in high school and in the early stages of college, a lot of emphasis is given to permutations. Linear permutations with either distinct or repeated elements are treated, as well as circular permutations with distinct elements, but nothing is mentioned regarding circular permutations with repeated elements. The goal of this work is to provide a reference in Portuguese for a formula that can be used in this problem, accompanied by its demonstration, which relies on the Theory of Group Actions and Burnside's Theorem. These topics are also briefly treated in this paper for completeness purposes.

Keywords: Circular permutations with repetitions; Group actions; Burnside's Lemma.

1. Introdução

Permutações são um dos principais conteúdos de Análise Combinatória estudados no Ensino Médio. Inicialmente, aprendemos que o número de formas de se ordenar n objetos distintos é n! e chamamos cada uma dessas ordenações de uma *permutação simples* dos n objetos. Em seguida, consideramos permutações com elementos repetidos, sendo β_i elementos do tipo i, $i \in \{1, \ldots, \ell\}$, com

$$\beta_1 + \ldots + \beta_\ell = n.$$

Nesse caso, o número de permutações desses n objetos é dado por

$$\frac{n!}{\beta_1! \cdot \ldots \cdot \beta_\ell!}.$$

Finalmente, os primeiros estudos de permutações costumam ser encerrados tratando das permutações circulares. Se n objetos distintos estão dispostos ao longo de um círculo, então as n! permutações simples acima contam cada uma das ordenações circulares n vezes, uma vez que, escolhida uma das posições, podemos girar o círculo e colocar qualquer um dos n objetos nessa posição. Assim, o número de permutações circulares de n objetos distintos é $(n-1)!$.

Todos esses conteúdos são tratados com profundidade em uma vasta literatura em português, da qual podemos destacar [1], [2] e [3]. No entanto, não há referências sobre permutações circulares com repetição. Seguindo a mesma linha de raciocínio dos casos acima, poderíamos imaginar que bastaria dividir o número de permutações lineares com as mesmas repetições de objetos por n, mas o seguinte exemplo mostra que esse raciocínio está incorreto.

Exemplo 1. Quantas permutações circulares distintas dos elementos da sequência ●●●● existem?

Existem $\dfrac{4!}{2!2!} = 6$ permutações lineares distintas desses quatro elementos. Dessa forma, dividindo 6 pelo número de objetos, um total de quatro, obtemos um número que não é nem inteiro, o que mostra que o raciocínio anterior não funciona. Por inspeção, as duas permutações circulares distintas são as duas da Figura 1.

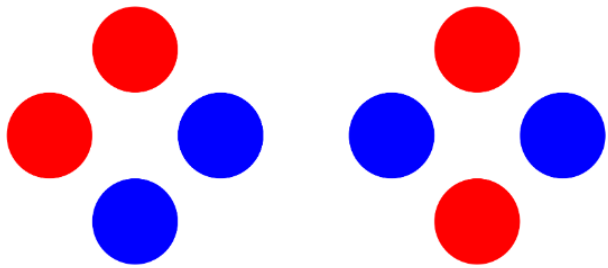

Figura 1: As duas permutações circulares distintas dos elementos ●●●●.

Como devemos proceder, então? Em [4], o autor apresenta uma fórmula. Considere n objetos de ℓ tipos distintos tais que há β_i objetos do tipo i para todo $i \in \{1, \ldots, \ell\}$. Se $\mathrm{PC}(\beta_1, \ldots, \beta_\ell)$ e $\mathrm{PL}(\beta_1, \ldots, \beta_\ell)$ são, respectivamente, os números de permutações circulares e lineares desses n objetos, sabemos que

$$\mathrm{PL}(\beta_1, \ldots, \beta_\ell) = \frac{n!}{\beta_1! \cdot \ldots \cdot \beta_\ell!}. \tag{1}$$

Então

$$\mathrm{PC}(\beta_1, \ldots, \beta_\ell) = \frac{1}{n} \sum_{d|N} \varphi(d) \mathrm{PL}\left(\frac{\beta_1}{d}, \ldots, \frac{\beta_\ell}{d}\right), \tag{2}$$

onde $N = \mathrm{mdc}(\beta_1, \ldots, \beta_\ell)$ e φ é a função totiente de Euler [5, Definição 2.6], a qual fornece o número de inteiros positivos $m \leq n$ tais que m e n são relativamente primos. De fato, no Exemplo 1 temos $\beta_1 = \beta_2 = 2$, logo $N = 2$. Os divisores de 2 são 1 e 2, portanto (2) diz-nos que

$$\mathrm{PC}(2,2) = \frac{1}{4}\left(\varphi(1)\mathrm{PL}(2,2) + \varphi(2)\mathrm{PL}(1,1)\right) = \frac{1 \cdot 6 + 1 \cdot 2}{4} = 2,$$

como queríamos.

Uma discussão mais profunda sobre problemas semelhantes a esse pode ser encontrada tanto em [6] quanto em [7]. O objetivo deste trabalho é apresentar uma demonstração para a fórmula (2). Para efeito de completude do trabalho, as principais técnicas envolvidas na argumentação são expostas nas próximas duas Seções. Primeiramente, ações de grupos são abordadas na Seção 2. Em seguida, o Lema de Burnside, principal resultado usado na prova de (2), é tratado na Seção 3. A demonstração é feita na Seção 4, a qual conclui o trabalho.

2. Grupos e Ações de grupos

Começamos esta seção com um resumo sobre os principais tópicos da Teoria de Grupos necessários para as Seções posteriores. Um grupo trata-se de conjunto G, munido de uma operação binária

$$\begin{array}{ccc} G \times G & \to & G \\ (g, h) & \mapsto & gh \end{array}$$

tal que

(i) $(g_1g_2)g_3 = g_1(g_2g_3)$ para todos $g_1, g_2, g_3 \in G$.

(ii) existe um elemento $e \in G$ (chamado *identidade*) tal que $ge = eg = g$ para todo $g \in G$.

(iii) para todo $g \in G$ existe $g^{-1} \in G$ tal que $gg^{-1} = g^{-1}g = e$.

Por exemplo, os inteiros, com a operação de adição, configuram um grupo. Um subconjunto não vazio H de um grupo G é um *subgrupo* de G se $g^{-1}h \in H$ para todos $g, h \in H$. Se H é subgrupo de G, chamamos o conjunto

$$gH = \{gh : h \in H\}$$

de *classe lateral à esquerda* de H. É sabido que as classes laterais à esquerda de um subgrupo H particionam o grupo G, e que $gH = hH$ se, e somente se, $g^{-1}h \in H$. O número de classes laterais à esquerda de H em G é chamado de *índice* de H em G e é denotado por $[G : H]$. A *ordem* de um grupo G, denotada por $|G|$, é dada pelo seu número de elementos. Quando G é finito, o Teorema de Lagrange [8, Teorema 1.2] garante que

$$|G| = [G : H]|H|.$$

Um importante conceito, fundamental para este trabalho, é definido a seguir.

Definição 1. Sejam G um grupo e X um conjunto. Uma *ação* de G sobre X é uma aplicação

$$\begin{array}{rccc} \phi : & G \times X & \to & X \\ & (g, x) & \mapsto & \phi(g, x) = g \cdot x \end{array}$$

satisfazendo

(i) $e \cdot x = x$ para todo $x \in X$, onde e é a identidade de G.

(ii) $g_1 \cdot (g_2 \cdot x) = (g_1g_2) \cdot x$ para todos $g_1, g_2 \in G$ e $x \in X$.

O leitor interessado pode encontrar ótimas introduções à Teoria de Grupos e às Ações de Grupos em [8], [9] e [10]. Nosso foco cairá sobre dois conceitos importantes que estão associados a toda ação.

Definição 2. Considere uma ação de um grupo G sobre um conjunto X. Dado $x \in X$, a *órbita* de X é o conjunto

$$\mathrm{Orb}_x = \{g \cdot x : g \in G\} \subset X.$$

O *estabilizador* de x é o conjunto

$$\mathrm{Stab}_x = \{g \in G : g \cdot x = x\} \subset G.$$

A relação das ações de grupos com esse trabalho aparece quando representamos cada permutação linear (com repetição) de n objetos como uma função

$$C : \{1, \ldots, n\} \longrightarrow \{1, \ldots, \ell\}$$

que leva cada um dos n elementos no tipo correspondente, de modo que

$$|C^{-1}(i)| = \beta_i, \quad i = 1, \ldots, \ell, \tag{3}$$

onde $C^{-1}(i)$ denota a imagem inversa de $\{i\}$ pela função C.

Seja X o conjunto de todas as funções C como acima. Vamos considerar a ação de $\mathbb{Z}_n = \{\overline{1}, \overline{2}, \ldots, \overline{n}\}$ sobre X tal que, se $\overline{k} \in \mathbb{Z}_n$ e $C \in X$, então $\overline{k} \cdot C$ é a função $\overline{k} \cdot C : \{1, \ldots, n\} \longrightarrow \{1, \ldots, \ell\}$ dada por

$$\overline{k} \cdot C(m) = C(r), \tag{4}$$

em que r é o resto da divisão de $m + k$ por n (a menos que $m + k$ seja múltiplo de n. Nesse caso, $r = n$ devido à forma como definimos $\mathbb{Z}_n$). Dessa forma, duas permutações lineares correspondem à mesma permutação circular se, e somente se, pertencerem à mesma órbita dessa ação.

Exemplo 2. Voltamos à mesma situação do Exemplo 1. Suponha que o tipo 1 corresponde a 🔴 e que o tipo 2 corresponde a 🔵. Nesse caso, o conjunto X possui seis elementos, que estão indicados na Tabela 1.

Permutação	C(1)	C(2)	C(3)	C(4)
🔴🔴🔵🔵	1	1	2	2
🔴🔵🔴🔵	1	2	1	2
🔴🔵🔵🔴	1	2	2	1
🔵🔵🔴🔴	2	2	1	1
🔵🔴🔵🔴	2	1	2	1
🔵🔴🔴🔵	2	1	1	2

Tabela 1: Uma outra maneira de representar permutações com elementos repetidos.

Observe que há apenas duas órbitas nesta ação. Uma delas é formada por 🔴🔴🔵🔵, 🔴🔵🔵🔴, 🔵🔵🔴🔴 e 🔵🔴🔴🔵, enquanto a outra é formada por 🔴🔵🔴🔵 e 🔵🔴🔵🔴. Essas órbitas correspondem às duas permutações circulares distintas desses elementos.

Basta-nos, portanto, contar o número de órbitas dessa ação, o que será feito na próxima seção. Antes disso precisaremos de mais alguns fatos sobre órbitas e estabilizadores.

Teorema 1. *Considere uma ação de um grupo* G *sobre um conjunto* X*. Então:*

(i) As órbitas da ação particionam X*.*

(ii) Para todo $x \in X$*,* $Stab_x$ *é subgrupo de* G*.*

(iii) Se $g, h \in G$ *e* $x \in X$*, então* $gStab_x = hStab_x$ *se, e somente se,* $g \cdot x = h \cdot x$*.*

(iv) Para todo $x \in X$ *vale*

$$|Orb_x| = [G : Stab_x].$$

Demonstração. Para o item (i), dado $x \in X$ temos $x = e \cdot x \in Orb_x$. Se $y \in Orb_x \cap Orb_{x'}$, então existem $g_1, g_2 \in G$ tais que $y = g_1 \cdot x = g_2 \cdot x'$. Se $g \cdot x \in Orb_x$, então $g \cdot x = g \cdot (g_1^{-1} \cdot y) = (gg_1^{-1}) \cdot y = (gg_1^{-1}) \cdot (g_2 \cdot x') = (gg_1^{-1}g_2) \cdot x' \in Orb_{x'}$, portanto $Orb_x \subset Orb_{x'}$. Analogamente, mostra-se que $Orb_{x'} \subset Orb_x$, logo duas órbitas quaisquer ou são iguais ou são disjuntas, como queríamos.

Para o item (ii), como $e \cdot x = x$, temos que $e \in Stab_x$. Se $g, h \in Stab_x$, então $g \cdot x = x$ e $h \cdot x = x$, logo $g^{-1} \cdot x = x$, e $(g^{-1}h) \cdot x = g^{-1} \cdot (h \cdot x) = g^{-1} \cdot x = x$, logo $g^{-1}h \in Stab_x$, o que prova que $Stab_x$ é subgrupo de G.

Para o item (iii), note que $gStab_x = hStab_x$ se, e somente se, $g^{-1}h \in Stab_x$, o que equivale a dizer que $(g^{-1}h) \cdot x = x$, ou seja, que $h \cdot x = g \cdot x$, como queríamos.

Finalmente, considere o mapa

$$\begin{array}{rccc} \phi: & Orb_x & \to & G/Stab_x \\ & g \cdot x & \mapsto & gStab_x \end{array}$$

Esse mapa é claramente sobrejetivo, e pelo item (iii), é injetivo, logo é uma bijeção. Daí, concluímos que

$$|Orb_x| = |G/Stab_x| = [G : Stab_x],$$

provando o item (iv).

□

Para finalizar esta seção note que, pelo item (iv) do Teorema 1 e pelo Teorema de Lagrange, podemos escrever

$$|Orb_x| = \frac{|G|}{|Stab_x|} \tag{5}$$

sempre que o grupo G for finito.

3. O Lema de Burnside

Agora que já sabemos contar quantos elementos há em cada órbita usando a equação (5), vamos determinar quantas órbitas existem.

Teorema 2 (Lema de Burnside)**.** *Dados um grupo finito* G*, um conjunto* X *e uma ação de* G *sobre* X*, o número de órbitas distintas é dado por*

$$|X/G| = \frac{1}{|G|} \sum_{g \in G} |X^g|, \tag{6}$$

onde $X^g = \{x \in X : g \cdot x = x\}$ *é o conjunto dos elementos de* X *que são fixados pela ação de* $g \in G$*.*

Demonstração. Primeiramente, note que

$$\sum_{g\in G}|X^g| = |\{(g,x)\in G\times X : g\cdot x = x\}| = \sum_{x\in X}|\mathrm{Stab}_x|. \tag{7}$$

Por (5),

$$\frac{1}{|G|}\sum_{x\in X}|\mathrm{Stab}_x| = \frac{1}{|G|}\sum_{x\in X}\frac{|G|}{|\mathrm{Orb}_x|} = \sum_{x\in X}\frac{1}{|\mathrm{Orb}_x|}. \tag{8}$$

O item (i) do Teorema 1 diz-nos que as órbitas da ação particionam X. Assim, vamos reescrever a equação (8) agrupando todos os elementos de uma mesma órbita. Se $O\in X/G$, então para todo $x\in O$ tem-se $|\mathrm{Orb}_x| = |O|$. Ficamos com

$$\sum_{x\in X}\frac{1}{|\mathrm{Orb}_x|} = \sum_{O\in X/G}\sum_{x\in O}\frac{1}{|O|} = \sum_{O\in X/G}1 = |X/G|. \tag{9}$$

Combinando (7), (8) e (9) obtemos (6). □

4. A fórmula para permutações circulares com repetição

Considere n objetos de ℓ tipos distintos tais que há β_i objetos do tipo i para todo $i\in\{1,\dots,\ell\}$. Se $PC(\beta_1,\dots,\beta_\ell)$ e $PL(\beta_1,\dots,\beta_\ell)$ são, respectivamente, os números de permutações circulares e lineares desses n objetos, sabemos que

$$PL(\beta_1,\dots,\beta_\ell) = \frac{n!}{\beta_1!\cdot\ldots\cdot\beta_\ell!}.$$

Nosso objetivo nesta seção é provar a fórmula (2), isto é, que

$$PC(\beta_1,\dots,\beta_\ell) = \frac{1}{n}\sum_{d|N}\varphi(d)PL\left(\frac{\beta_1}{d},\dots,\frac{\beta_\ell}{d}\right),$$

onde $N = \mathrm{mdc}(\beta_1,\dots,\beta_\ell)$ e φ é a função totiente de Euler. Comecemos, como na Seção 2, representando cada permutação linear dos n objetos como uma função

$$C : \{1,\dots,n\}\longrightarrow\{1,\dots,\ell\}$$

que leva cada um dos n elementos no tipo correspondente, de modo que

$$|C^{-1}(i)| = \beta_i,\quad i = 1,\dots,\ell. \tag{10}$$

Seja X o conjunto de todas as funções C como acima. Vamos novamente considerar a ação de $\mathbb{Z}_n$ sobre X dada por (4), ou seja, se $\overline{k}\in\mathbb{Z}_n$ e $C\in X$, então $\overline{k}\cdot C : \{1,\dots,n\}\longrightarrow\{1,\dots,\ell\}$ dada por

$$\overline{k}\cdot C(m) = C(r), \tag{11}$$

como definida na Seção 2. Note que as permutações C_1 e C_2 pertencem à mesma órbita dessa ação se, e somente se, correspondem à mesma permutação circular dos n elementos. Basta, portanto, calcular o número de órbitas $|X/\mathbb{Z}_n|$ dessa ação, que, pelo Lema de Burnside, é dado por

$$|X/\mathbb{Z}_n| = \frac{1}{n}\sum_{\overline{k}\in\mathbb{Z}_n}|X^{\overline{k}}|. \tag{12}$$

Sejam $\overline{k} \in \mathbb{Z}_n$ e $d = |\langle \overline{k} \rangle|$, isto é, a ordem do (subgrupo gerado pelo) elemento $\overline{k}$. Se a ação de $\overline{k}$ sobre C fixa C, isto é, se $\overline{k} \cdot C = C$, então

$$C(m) = C(m+k) = C(m+2k) = \cdots = C(m+(d-1)k) \tag{13}$$

para todo $m \in \{1, \ldots, n\}$. Observe que os d elementos de $\{1, \ldots, n\}$ indicados na equação acima são distintos. Com efeito, se dois deles fossem iguais, concluiríamos que $j_1 k \equiv j_2 k \mod n$, com $j_1, j_2 \in \{0, \ldots, d-1\}$ distintos, o que contradiz o fato de d ser a ordem de $\overline{k}$ em $\mathbb{Z}_n$. Daí, segue que o número de elementos de cada tipo é sempre um múltiplo de d, portanto d divide $N = \text{mdc}(\beta_1, \ldots, \beta_\ell)$.

Afirmamos que se $|\langle \overline{k_1} \rangle| = |\langle \overline{k_2} \rangle| = d$, então $X^{\overline{k_1}} = X^{\overline{k_2}}$. Com efeito, existe apenas um subgrupo de $\mathbb{Z}_n$ com ordem d [9, Theorem 7, Section 2.3]. Dessa forma, existe $n_0 \in \mathbb{Z}$ tal que $\overline{k_1} = n_0 \overline{k_2}$, ou seja, $k_1 \equiv n_0 k_2 \mod n$, o que nos permite escrever

$$k_1 = n_0 k_2 + \alpha n,$$

com $\alpha \in \mathbb{Z}$. Com isso, se $\overline{k_2}$ fixa C, então

$$C(m + k_1) = C(m + n_0 k_2 + \alpha n) = C(m + n_0 k_2) = C(m)$$

para todo $m \in \{1, \ldots, n\}$, ou seja, $\overline{k_1}$ fixa C, de modo que $X^{\overline{k_1}} \supset X^{\overline{k_2}}$. A outra inclusão é análoga e, com ela, a afirmação está provada.

Como há exatamente $\varphi(d)$ elementos de ordem d em $\mathbb{Z}_n$ [9, Proposition 6, Section 2.3], podemos calcular a quantidade de elementos fixados pela ação de $\overline{\frac{n}{d}}$ e multiplicar esse número por $\varphi(d)$ em (12). Note que, agora, faremos a soma sobre todos os divisores de $N = \text{mdc}(\beta_1, \ldots, \beta_\ell)$, ou seja, (12) torna-se

$$|X/\mathbb{Z}_n| = \frac{1}{n} \sum_{d|N} \varphi(d) |X^{\overline{n/d}}|. \tag{14}$$

Assim, podemos direcionar nossa atenção a $k = \frac{n}{d}$. De fato, esse é o motivo de consideramos os representantes das classes em $\mathbb{Z}_n$ de 1 a n ao invés da escolha usual de 0 a $n-1$, pois isso evita termos que tratar o caso $d = 1$ separadamente. Se $C \in X^{\overline{n/d}}$ e $m \in \{1, \ldots, n\}$, temos

$$C(m) = C\left(m + \frac{n}{d}\right) = C\left(m + 2\frac{n}{d}\right) = \cdots = C\left(m + (d-1)\frac{n}{d}\right). \tag{15}$$

Na equação acima, a função C é calculada em d elementos distintos de $\{1, \ldots n\}$, os quais formam uma progressão aritmética de razão $\frac{n}{d}$ quando escritos em ordem crescente. Logo, o menor desses elementos está entre 1 e $\frac{n}{d}$.

Com isso, segue de (15) que toda função $C \in X^{\overline{n/d}}$ fica totalmente determinada pelos elementos do conjunto

$$S_d = \left\{1, 2, \ldots, \frac{n}{d}\right\},$$

pois as imagens dos demais elementos são obtidas repetindo essa sequência inicial. Basta olhar, portanto, para a restrição

$$C_d = C|_{S_d} : \left\{1, 2, \ldots, \frac{n}{d}\right\} \longrightarrow \{1, \ldots, \ell\},$$

que é tal que $|C_d^{-1}(i)| = \frac{\beta_i}{d}$, $i = 1, \ldots, \ell$. Como há $PL\left(\frac{\beta_1}{d}, \ldots, \frac{\beta_\ell}{d}\right)$ dessas funções (por (1)), segue que

$$|X^{\overline{n/d}}| = PL\left(\frac{\beta_1}{d}, \ldots, \frac{\beta_\ell}{d}\right) \tag{16}$$

e, por (14),

$$PC(\beta_1, \ldots, \beta_\ell) = \frac{1}{n}\sum_{d|N} \varphi(d) PL\left(\frac{\beta_1}{d}, \ldots, \frac{\beta_\ell}{d}\right), \tag{17}$$

como queríamos.

Referências

[1] Santos, J. P. O.; Mello, M. P.; Murari, I. T. C. *Introdução à análise combinatória*. Campinas: Editora da Unicamp, 1995.

[2] Morgado, A. C. O. M.; Carvalho, J. B. P. C.; Carvalho, P. C. P.; Fernandez, P. *Análise Combinatória e Probabilidade*. 9ª ed. Rio de Janeiro: SBM, 2006.

[3] Hazzan, S. *Fundamentos de Matemática Elementar, 5: Combinatória, Probabilidade*. 8ª ed. São Paulo: Atual, 2013.

[4] MacMahon, P. A. *Applications of a Theory of Permutations in Circular Procession to the Theory of Numbers*. Proceedings of the London Mathematical Society, v. 1, n° 1, p. 305-318, 1891.

[5] Santos, J. P. O. *Introdução à Teoria dos Números*. 3ª ed. Rio de Janeiro: Impa, 2009.

[6] Kajimoto, H., Osabe, M. *Circular and necklace permutations*. Bulletin-Faculty of Education Nagasaki University Natural Science, v. 74, 2006.

[7] Mestrovic, R. *Different classes of binary necklaces and a combinatorial method for their enumerations*. arXiv preprint arXiv:1804.00992, 2018.

[8] Martin, P. A. *Grupos, Corpos e Teoria de Galois*. São Paulo: Editora Livraria da Física, 2010.

[9] Dummit, D. S.; Foote, R. M. *Abstract Algebra*. Hoboken: Wiley, 2013.

[10] Gonçalves, A. *Introdução à Álgebra*. 5ª ed. Rio de Janeiro: Impa, 2009.

Guilherme F. S. Silva
Universidade Federal de Pernambuco
Departamento de Matemática
<guilherme.fssilva@ufpe.br>

João A. M. Gondim
Universidade Federal Rural de Pernambuco
Unidade Acadêmica do Cabo de Santo Agostinho
<joao.gondim@ufrpe.br>

Recebido: 11/03/2022
Publicado: 18/08/2022

SBM
SOCIEDADE BRASILEIRA DE MATEMÁTICA