Sociedade Brasileira de Matemática - **SBM**
Universidade Federal do Acre - **UFAC**
Mestrado Profissional em Matemática - **PROFMAT**

Homomorfismos e Elementos Idempotentes de um Conjunto

Carlos Alberto Dantas da Silva

Rio Branco – Acre

2023

Carlos Alberto Dantas da Silva

Homomorfismos e Elementos Idempotentes de um Conjunto

Trabalho de conclusão de curso apresentado ao Mestrado Profissional de Matemática em Rede Nacional - PROFMAT, na cidade de Rio Branco, Acre, como requisito parcial para a obtenção do título de Mestre em Matemática.

Orientador: Prof. Dr. José Ivan da Silva Ramos

Rio Branco – Acre

2023

UNIVERSIDADE FEDERAL DO ACRE
PROGRAMA DE PÓS-GRADUAÇÃO STRICTO SENSU PROFISSIONAL EM MATEMÁTICA

FOLHA DE APROVAÇÃO

Titulo da Dissertação: Homomorfismos e elementos idempotentes de um conjunto.

Autor: Carlos Alberto Dantas da Silva
Orientador: José Ivan da Silva Ramos

Dissertação aprovada como parte das exigências para obtenção do título de Mestre pelo Programa de Mestrado Profissional em Matemática em Rede Nacional, pela Banca Examinadora:

DATA DA APROVAÇÃO: 14 de novembro de 2023.

BANCA EXAMINADORA:

Assinado Eletronicamente
JOSÉ IVAN DA SILVA RAMOS
Orientador
Universidade Federal do Acre - UFAC

Assinado Eletronicamente
CLEBER PEREIRA
Membro
Universidade Federal do Acre - UFAC

Assinado Eletronicamente
MARINALDO FELIPE DA SILVA
Membro externo
Universidade Federal de Rondônia - UNIR

Documento assinado eletronicamente por **Jose Ivan da Silva Ramos**, **Professor do Magisterio Superior**, em 20/11/2023, às 10:36, conforme horário de Rio Branco - AC, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **MARINALDO FELIPE DA SILVA**, **Usuário Externo**, em 20/11/2023, às 11:33, conforme horário de Rio Branco - AC, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Cleber Pereira**, **Professor do Magisterio Superior**, em 20/11/2023, às 11:53, conforme horário de Rio Branco - AC, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade do documento pode ser conferida no site https://sei.ufac.br/sei/valida_documento ou click no link Verificar Autenticidade informando o código verificador **1099090** e o código CRC **FB59B23B**.

Referência: Processo nº 23107.033976/2023-71 SEI nº 1099090

AGRADECIMENTOS

Em primeiro lugar, a Deus, que fez com que meus objetivos fossem alcançados, durante todos os meus anos de estudos, permitindo que eu tivesse saúde e determinação para não desanimar durante a realização deste trabalho e ultrapassar todos os obstáculos encontrados ao longo desta jornada.

Aos familiares, por todo o apoio, ajuda e incentivo incondicionais, que muito contribuiu para a realização deste trabalho.

Aos amigos, que sempre estiveram ao meu lado, pela amizade e pelo apoio demonstrado ao longo de todo o período de tempo em que me dediquei a este trabalho.

Ao professor Dr. José Ivan da Silva Ramos, por ter sido meu orientador e ter desempenhado tal função com dedicação e amizade.

Aos professores, pelas correções e ensinamentos que me permitiram apresentar um melhor desempenho no meu processo de formação profissional ao longo do curso.

Aos meus colegas de curso, com quem convivi intensamente durante os últimos anos, pelo companheirismo e pela troca de experiências que me permitiram crescer não só como pessoa, mas também como formando.

À Universidade Federal do acre, essencial no meu processo de formação profissional, pela dedicação, e por tudo o que aprendi ao longo dos anos do curso.

Universidade Federal do Acre
Biblioteca Central

S586h Silva, Carlos Alberto Dantas da, 1964-
Homomorfismos e elementos idempotentes de um conjunto / Carlos Alberto Dantas da Silva ; orientador: Prof. Dr. José Ivan da Silva Ramos. – Rio Branco, 2023.
40 p.

Trabalho de Conclusão de Curso (Mestrado) - Universidade Federal do Acre, Mestrado Profissional de Matemática em Rede Nacional - PROFMAT. Rio Branco, 2023.
Inclui referências bibliográficas.

1. Estrutura algébrica. 2. Conjuntos - Matemática. 3. Matemática. I. Ramos, José Ivan da Silva (orientador). II. Título.

CDD: 510.92

Bibliotecária: Alanna Santos Figueiredo - CRB 11°/1003

"A gravidade explica os movimentos dos planetas, mas não pode explicar quem colocou os planetas em movimento. Deus governa todas as coisas e sabe tudo que é ou que pode ser feito".

Isaac Newton

Resumo

Após um breve estudo das estruturas algébricas de determinados conjuntos $S \neq \Phi$, faremos uma contagem de possíveis endomorfismos de S, motivada pela existência de elementos idempotentes. A estratégia para estabelecermos esse pequeno controle será fixar uma operação $*$ definida nesse conjunto e identificar os elementos $s \in S \neq \Phi$ que satisfazem a igualdade $s^2 = s * s = s$ para, de maneira bem simples e intuitiva, explicitar listas dessas funções especiais.

Palavras chave: Conjuntos, operações, propriedades, idempotência e homomorfismos

Abstract

After a brief study of the algebraic structures of a given sets $S \neq \Phi$, we will count the possible endomorphisms of S, motivated by the existence of idempotent elements. The strategy for establishing this small control will be to fix an operation $*$ defined in this set and identify the elements $s \in S \neq \Phi$ that satisfy the equality $s^2 = s * s = s$ so that, in a very simple and intuitive way, we can explain lists of these special funcions.

Keywords: Sets, operations, properties, idempotency and homomorphisms.

Lista de Símbolos

$<$: menor do que.

$>$: maior do que.

$\leq$: menor do que ou igual a.

$\geq$: maior do que ou igual a.

$=$: igual a.

$\neq$: diferente.

$\forall$: para todo, qualquer que seja.

$\Rightarrow$: então, implica.

$\Leftrightarrow$: equivalente, se e somente se, se e só se.

∞: infinito (não é um número).

/: tal que.

$\exists$: existe.

$\nexists$: não existe.

$\in$: pertence a.

$\notin$: não pertence a.

$\subset$ e $\supset$: está contido e contém

$\subseteq$: subconjunto de ou igual a.

$\subsetneq$: subconjunto de e diferente de ou subconjunto próprio de.

$\not\subset$: não está contido.

$\cup$: união.

$\cap$: interseção.

#X: número de elementos do conjunto X.

$\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$: conjunto dos números naturais, inteiros, racionais, reais e complexos, respectivamente.

$n\mathbb{Z} = \{nk \ / \ k \in \mathbb{Z}\}$: conjunto dos múltiplos do número inteiro n.

$M_{mxn}\,(\mathbb{R})$: conjunto das matrizes de ordem mxn com entradas no corpo dos reais.

$M_n(\mathbb{R})$: conjunto das matrizes quadradas de ordem n com entradas em $\mathbb{R}$.

$\mathbb{F}_B^A$: conjunto de todas as funções que agem de A para B.

$\mathbb{F}(X)$: conjunto de todas as funções que agem de X em si mesmo.

Sumário

Introdução

Ao contrário da Aritmética e da Geometria, que são áreas da Matemática que se caracterizam pelo tipo de objeto estudado, a Álgebra é caracterizada pelos seus métodos. Os métodos, em Álgebra, seguem a ideia básica de estudar os objetos não isoladamente, mas observando a estrutura resultante da organização desses objetos em conjuntos com certas propriedades. Por exemplo, do ponto de vista da Álgebra, um polinômio não deve ser visto como um objeto isolado, mas, antes, como um elemento de um conjunto de polinômios onde os elementos possam ser somados e também multiplicados, numa estrutura chamada anel de polinômios. Faz sentido, portanto, falarmos em soma e em produto de matrizes, de polinômios e de funções, embora tais objetos não sejam números. Isso se dá porque tais objetos podem ser organizados em conjuntos munidos de uma ou mais operações, o que dá a cada um desses conjuntos uma estrutura algébrica. Podemos, então, estudar tais estruturas de modo abstrato, sem fazer referência à natureza dos seus elementos, obtendo resultados que valem em diferentes contextos.

Atualmente, quando estudamos conjuntos numéricos, temos interesse em conhecer propriedades das operações e relações nesses conjuntos. Esta maneira de tratar com conjuntos numéricos teve início com os trabalhos de Pitágoras de Samos, que viveu no século VI a.C.

Pitágoras tinha conhecimento que os egípcios e babilônios faziam cálculos usando regras que eram passadas de geração a geração. Analisando tais regras, ele passou a considerar os números como elementos abstratos (que não eram necessariamente associados a problemas práticos que envolvessem medidas ou quantidades), e deduziu propriedades das operações entre esses elementos.

Para ter certeza dos resultados obtidos, Pitágoras aperfeiçoou a prova científica ou prova matemática, que também chamamos simplesmente de demonstração. A demonstração matemática inicia com uma “verdade aceita” e através de argumentação lógica se chega a uma conclusão inegável. Essa é a ferramenta fundamental para o estudo da matemática.

Os conhecimentos sobre várias áreas da matemática são formalizados através do método axiomático, que consiste de conceitos primitivos e axiomas. Alguns dos conceitos primitivos são intuídos sem explicação formal, e os axiomas são proposições, envolvendo os conceitos primitivos, tomadas como verdadeiras por estarem baseadas

na intuição elementar. A partir dos axiomas provam-se novas proposições e, a partir dos axiomas e das novas proposições, provam-se outras proposições e, assim, sucessivamente, podemos construir a teoria sobre determinado assunto.

A geometria foi o primeiro ramo da matemática que teve sua teoria construída de forma axiomática. Isso se deve aos trabalhos de Euclides (século III a. C.), publicados na obra: *Os Elementos*.

A axiomatização da álgebra ocorreu bem mais tarde. A primeira tentativa foi feita pelo inglês Benjamin Peacok (1791-1858), em 1830, mas não se mostrou consistente. Nessa época, poucos matemáticos se dedicavam à tentativa de axiomatizar operações em conjuntos de forma geral, pois o objetivo principal era obter essa axiomatização nos conjuntos numéricos $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$.

O conjunto dos números complexos foi o primeiro a ter sua construção descrita pelo método axiomático. Isso ocorreu em 1833, com trabalhos de Willian R. Hamilton (1805-1865). O último foi o conjunto dos números naturais em 1899, graças aos estudos de Giuseppe Peano. Conjuntos com operações que satisfazem axiomas determinados previamente são chamados de estruturas algébricas. O conceito da estrutura algébrica chamada *anel*, surgiu como conseqüência da sistematização dos conjuntos numéricos. A definição formal de anel foi elaborada em 1914 pelo alemão A. Fraenkel (1891-1965).

O TCC que elaboramos está dividido em 2 capítulos. No primeiro momento descrevemos brevemente alguns conjuntos e relacionamos algumas de suas operações e propriedades. Incluímos, ao final, um pequeno parágrafo sobre *homomorfismos* que serão relacionados com os elementos *idempotentes* dos conjuntos sobre os quais eles agem.

Concentramos os nossos esforços no capítulo 2, mostrando que é possível estimarmos a quantidade de homomorfismos que agem sobre um conjunto, caso detectemos, nele, a existência de elementos idempotentes, além de averiguarmos que as operações admitem a comutatividade.

Nossas considerações finais mostram que terminamos por estabelecermos alguns resultados gerais sobre essa contagem que, de certa forma, pode ser observada em algumas passagens e contextos da Matemática básica.

Capítulo 1: Noções preliminares

1.1 Alguns conceitos ligados à teoria dos conjuntos

A teoria dos conjuntos é um ramo da matemática que estuda os conjuntos, que são coleções de objetos. Ela foi desenvolvida no início do século XX por Georg Cantor e se tornou uma base fundamental da matemática moderna. Aqui estão algumas definições e conceitos-chave da teoria dos conjuntos para o desenvolvimento de nosso trabalho:

i) **Conjunto:** é uma coleção contendo zero ou mais objetos distintos, chamados de elementos. Os conjuntos são geralmente representados por letras maiúsculas do nosso alfabeto.

ii) **Elemento:** é um objeto que faz parte de um conjunto. Se um elemento x *pertence* a um conjunto A, escrevemos $x \in A$. Caso contrário, se x *não pertence* ao conjunto A, escrevemos $x \notin A$.

iii) **Igualdade de conjuntos:** os conjuntos A e B são iguais se, e somente se, possuem exatamente os mesmos elementos. Isso é denotado por $A = B$.

iv) **Subconjunto:** um conjunto A é um *subconjunto* de um conjunto B (ou A está contido em um conjunto B) se todos os elementos de A também são elementos de B. Isso é denotado por $A \subset B$. Caso exista ao menos um elemento de A fora de B, anotamos $A \not\subset B$ que significa que A não está contido em B.

v) **Conjunto vazio:** o conjunto vazio, denotado por $\emptyset$, é um conjunto que não possui elementos.

Observamos que $\emptyset \subset B$, independentemente dos objetos que definem o conjunto B. Isso porque $\emptyset$ não possui sequer um elemento que não esteja em B.

Podemos definir, ainda, a partir de dois conjuntos A e B, os seguintes conjuntos:

vi) **União:** a união de A com B é o conjunto que contém todos os elementos de A e todos os elementos de B. Isso é denotado por $A \cup B = \{x / x \in A \text{ ou } x \in B\}$.

vii) **Interseção:** a interseção de A com B é o conjunto que contém todos os elementos que são comuns a A e B. Isso é denotado por $A \cap B = \{x / x \in A \text{ e } x \in B\}$.

viii) **Diferença:** a diferença entre dois conjuntos A e B (nessa ordem) é o conjunto formado pelos elementos de A que não pertencem a B. Isso é denotado por $A \backslash B = \{x / x \in A \text{ e } x \notin B\}$. Nessa ordem porque, em geral, $A \backslash B$ e $B \backslash A$ são distintos.

ix) **Conjunto complementar:** o complementar de um conjunto A em relação ao conjunto universo U (conjunto no qual estão contidos todos os imagináveis conjuntos) é o conjunto formado pelos elementos de U que não pertencem a A. Isso é denotado por $\mathcal{C}_U(A) = \{x/x \in U \text{ e } x \notin B\}$. Se $A \subset B$, então $B \backslash A = \mathcal{C}_B(A) = \{x/x \in B \text{ e } x \notin A\}$ que é o complementar de A em relação a B.

x) **Conjunto das partes:** $P(A) = \{X/X \subset A\}$, é o *conjunto das partes* de A, formado por todos os subconjuntos de A.

xi) **Produto cartesiano:** $A \times B = \{(a, b)/a \in A \text{ e } b \in B\}$, é o *produto cartesiano* entre A e B, formado pelos pares de elementos de A e B, nessa ordem.

Por fim, definimos:

xiii) **Conjuntos disjuntos:** termo usado para dois conjuntos A e B tais que $A \cap B = \emptyset$.

Além dessas definições básicas dessa teoria, que serão úteis para as nossas argumentações, queremos considerar as operações definidas em um conjunto não vazio e as propriedades gerais que delas decorrem.

1.2 Operações definidas em conjuntos e suas propriedades

Relacionaremos algumas propriedades que usualmente são consideradas para uma operação que define a estrutura de um conjunto.

Definição 01: Seja A um conjunto não vazio. Dizemos que uma operação $*$ está (*bem*) *definida* em A se, e somente se, $\forall\, x, y \in A$, vale que $x * y \in A$.

São exemplos de operações bem definidas em um conjunto não vazio: a operação de adição "+ " em $\mathbb{N}$, a união " $\cup$ " em $P(A)$, sendo A um conjunto não vazio; e a operação de multiplicação " $\cdot$ " em $\mathbb{Z}$.

Geralmente quando é definida uma regra de operacionalização em um conjunto não vazio A, surgem propriedades que terminam por definir a estrutura desse conjunto. Daremos destaque para as propriedades que julgamos mais importantes na fundamentação do nosso trabalho.

Definição 02: Seja $A \neq \emptyset$ um conjunto. Seja $*$ uma operação definida em A.

a) Dizemos que esta operação tem a *propriedade associativa* se, e somente se, $\forall\, x, y, z \in A$, valer que $x * (y * z) = (x * y) * z$.

b) Dizemos que esta operação tem a *propriedade comutativa* se, e só se, $\forall\, x, y \in A$, valer que $x * y = y * x$.

c) Dizemos que $e \in A$ é *elemento neutro* para a operação $*$ se, e somente se, $\forall\, x \in A$, valer que $x * e = e * x = x$.

d) Se a operação $*$ admite elemento neutro e, dizemos que um elemento a é *inversível* (ou *possui inverso*) em A, com respeito a operação $*$, se, e somente se, $\exists\, a^{-1} \in A$, de modo que $a * a^{-1} = a^{-1} * a = e$.

Exemplo 01:

a) Considerando a operação de adição $+$, temos que 0 é o elemento neutro e todo elemento possui inverso (aditivo) no conjunto $\mathbb{Z}$ dos números inteiros. Particularmente, temos $2^{-1} = -2$.

b) Considerando a operação de multiplicação $\cdot$, temos que 1 é elemento neutro e todo elemento não nulo possui inverso, no conjunto $\mathbb{Q}$ dos números racionais. Particularmente, temos $2^{-1} = \frac{1}{2}$.

c) Sejam A um conjunto não vazio e $P(A)$, o conjunto das partes de A. É fácil ver que as operações $\cap$ (interseção) e $\cup$ (união) estão definidas em $P(A)$. Além disso, A e Φ são, respectivamente, o elemento neutro para as operações $\cap$ e $\cup$.

Definição (Potências inteiras) 03: Sejam A um conjunto não vazio, $*$ uma operação bem definida em A, e o elemento neutro para essa operação. Então, definimos as *potências inteiras* para um elemento $a \in A$, da seguinte maneira:

$$a^0 = e$$
$$a^1 = a$$
$$a^2 = a * a$$
$$a^3 = a * a * a$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$a^n = \underbrace{a * a * \ldots * a}_{n\ vezes};\ \forall\ 4 \leq n \in \mathbb{Z};\ \text{e}$$

$$a^{-n} = (a^{-1})^n = \underbrace{a^{-1} * a^{-1} * a^{-1} \ldots * a^{-1}}_{n\ vezes};\ \forall\ 1 \leq n \in \mathbb{Z}$$

Exemplificando, calculemos algumas potências do número 4 com respeito à operação de adição em $\mathbb{Z}$, obtemos: $4^0 = 0$, $4^1 = 4$, $4^2 = 4 + 4 = 8$ e para todo inteiro $3 \leq n \in \mathbb{Z}$, temos $4^n = \underbrace{4 + 4 + \ldots + 4}_{n\ vezes} = 4n$.

O "valor" da expressão a^n está diretamente ligado à operação $*$ e, no caso de seu expoente ser $n = 0$, por definição, temos $a^0 = e$; onde e é o elemento neutro para essa operação (caso ele exista).

Definição 04: Se A é um conjunto não vazio, $*$ uma operação bem definida em A, e essa operação admite e como elemento neutro, definimos que:
a) $a \in A$ é um elemento *idempotente* se, e somente se, $a^2 = a * a = a$.
b) $e \neq a$ é um elemento *nilpotente* se, e somente se, existe um primeiro número inteiro positivo c tal que $a^c = e$.

O conceito de idempotência será explorado em nosso capítulo 2. A nilpotência pode ser perceptível no conjunto das matrizes como mostra o Exemplo 01, em 1.3.3.

1.3 Breves descrições de alguns conjuntos

Este parágrafo relaciona alguns conjuntos que comumente aparecem como assuntos da Matemática básica. Isso nos permitirá justificar as observações que faremos mais em frente.

1.3.1 O conjunto $\mathbb{R}$ dos números reais

A partir do conjunto $\mathbb{Z} = \{\ldots, -z, \ldots, -3, -2, -1, 0, 1, 2, 3, \ldots, z, \ldots\}$ dos números inteiros podemos construir um primeiro exemplo de um conjunto "mais completo", o conjunto das frações de $\mathbb{Z}$. Comumente denotado por $\mathbb{Q} = \left\{\frac{m}{n} \ / \ m, n \in \mathbb{Z} \text{ e } n \neq 0\right\}$, esse conjunto é denominado de conjunto dos *números racionais*.

Existem, no entanto, outros números que não podem ser expressos por meio de um quociente entre dois números inteiros. Se pensarmos um pouco sobre $\sqrt{2}$ podemos facilmente verificar que esse não é um número racional. Para fazer esta verificação, ou seja, que $\sqrt{2}$ é um número irracional, vamos usar o método da contradição (reductio ad absurdum). A ideia é supor o oposto, ou seja, que a raiz quadrada de 2 é um número racional e, em seguida, mostrar que essa suposição leva a uma contradição.

Portanto, suponha que $\sqrt{2}$ é um número racional. Isso significa que podemos escrever $\sqrt{2}$ na forma de uma fração irredutível, ou seja, na forma $\frac{m}{n}$, onde m e n são inteiros positivos sem fatores primos em comum.

Então, temos que $\sqrt{2} = \frac{m}{n}$ e, elevando ambos os lados dessa igualdade ao quadrado, obtemos $2 = \left(\frac{m}{n}\right)^2 \Rightarrow 2 = \frac{m^2}{n^2}$.

Multiplicando ambos os lados por n^2, temos $2 \cdot n^2 = \frac{m^2}{n^2} \cdot n^2 \Rightarrow 2 \cdot n^2 = m^2$.

Agora, podemos ver que m^2 é par e, se m^2 é par, então m também é par (o leitor pode facilmente verificar esse fato, também por contradição). Então, escrevendo $m = 2k$, onde k é um número inteiro positivo, temos que $2 \cdot n^2 = m^2 = (2k)^2 = 4k^2$. Fazendo uma simples simplificação, temos que $n^2 = 2k^2$ também é par. consequentemente, n é par e isso contradiz o fato de que m e n não têm fatores comuns além de 1.

Com isso, nossa suposição inicial de que $\sqrt{2}$ é um número racional está incorreta e resta que $\sqrt{2}$ é um número irracional.

Em geral, se p é um número primo, então $\sqrt{p}$ não pode ser escrito como um quociente entre números inteiros. Portanto, o conjunto $\mathbb{Q}[\sqrt{p}] = \{a + b\sqrt{p} \ / \ a, b \in \mathbb{Q}\}$, onde p é um número primo, é "maior" que $\mathbb{Q}$, no sentido de conter esse conjunto.

Escolhendo p e p' dois números primos distintos (e pares desse tipo de número existem aos montes), os conjuntos $\mathbb{Q}[\sqrt{p}]$ e $\mathbb{Q}[\sqrt{p'}]$ são também distintos. Claramente, maiores que $\mathbb{Q}$. Esse conjunto por sua vez é maior que $\mathbb{Z}$, que é maior que $\mathbb{N}$.

Com relação às operações usuais de adição e multiplicação definidas em $\mathbb{Q}$, podemos listar uma quantidade satisfatória de propriedades. Valem quase todas as propriedades listadas na Definição 02, em 1.2, é que, com relação à multiplicação, o número 0 não possui inverso.

Pense em como definir operações de adição e multiplicação em $\mathbb{Q}[\sqrt{p}] = \{a + b\sqrt{p} / a, b \in \mathbb{Q}\}$ e em que propriedades essas operações possuem.

O conjunto $\mathbb{R}$, denominado de *conjunto dos números* (*reais*) é a união do conjunto $\mathbb{Q}$ com o conjunto de todos os números irracionais. Comumente escrevemos o conjunto (diferença) $\mathbb{R}\backslash\mathbb{Q}$ para indicar o conjunto dos números irracionais.

Observação 01: As operações de adição e multiplicação definidas em $\mathbb{R}$ gozam das propriedades listadas na Definição 02, em 1.2. Sendo que 0, o elemento neutro da adição não possui inverso multiplicativo.

Essas operações se ligam da seguinte forma: (**Distributividade da multiplicação em relação à adição**): $\forall\, x, y, z \in \mathbb{R}$, vale que $x(y+z) = xy + xz = yx + zx = (y+z)x$.

A abundância de inverso multiplicativo tem por

Consequência 01: Em $\mathbb{R}$, se x, y são tais que $xy = 0$, então vale que $x = 0$ ou $y = 0$.

Claro é que, se $0 \neq x \in \mathbb{R}$ ou $\mathbb{Q}$, então, existe x^{-1} e seguem as equivalências $xy = 0 \Leftrightarrow x^{-1}(xy) = x^{-1}0 \Leftrightarrow (x^{-1}x)y = 0 \Leftrightarrow 1\, y = 0 \Leftrightarrow y = 0$. Supondo que $y \neq 0$, os mesmos argumentos mostram que $x = 0$.

Em geral, se temos definidas uma operação de adição com elemento neutro 0 (zero) e uma operação de multiplicação em um dado conjunto não vazio A, dizemos que A *não possui divisores de zero* se, e somente se, dados elementos a e b em A, se $ab = 0$ então, $a = 0$ ou $b = 0$. Portanto, não existem divisores de zero em $\mathbb{R}$. Essa propriedade também é herdada pelos (sub) conjuntos $\mathbb{Q}\left[\sqrt{p}\right]$, $\mathbb{Q}$ e $\mathbb{Z}$.

Consequência 02: as únicas soluções da equação $x^2 = x$, no universo $\mathfrak{U} = \mathbb{R}$, são 0 e 1.

De fato, temos $x^2 = x \Leftrightarrow x(x-1) = 0$. E, claro, $x = 0$ é uma solução dessa equação. Além disso, se $x \neq 0$, em $\mathbb{Q}$ ou $\mathbb{R}$, existe o número x^{-1}, inverso multiplicativo de x e, podemos argumentar que, $x^2 = x \Leftrightarrow x^{-1}\, x^2 = x^{-1}x \Leftrightarrow x = 1$.

Várias outras propriedades e teorias estão relacionadas com os números. Podemos encerrar essa descrição, incluindo o ordenamento no conjunto $\mathbb{R}$:

Observação 02: Vale que $\mathbb{R}$ contém $\mathbb{R}_+^* = \{x \in \mathbb{R} \,/\, x > 0\}$ e,
i) se $x, y \in \mathbb{R}_+^*$, então $x + y \in \mathbb{R}_+^*$ e $x.y \in \mathbb{R}_+^*$,
ii) se $x \in \mathbb{R}$, exatamente uma das possibilidades ocorre: $x \in \mathbb{R}_+^*$, $-x \in \mathbb{R}_+^*$ ou $x = 0$.

1.3.2 O conjunto $\mathbb{C}$ dos números complexos

Os números complexos, historicamente, existem por duas razões principais, a saber: uma de natureza algébrica com a resolução da equação $x^2 + 1 = 0$, quando na Europa discutiam-se as "soluções impossíveis" de uma equação em torno dos números negativos e irracionais. Outra, com o desejo de criar um análogo aritmético do conceito de vetor, que surgiu dentro da Geometria e da Física, onde os números complexos aparecem como candidatos perfeitos para representar e permitir operar com vetores no plano.

Em $\mathbb{C} = \{z = x + yi \,/\, x, y \in \mathbb{R} \text{ e } i = \sqrt{-1}, \text{onde } i^2 = -1\}$, estão bem definidas as operações de adição e multiplicação, de acordo com as regras abaixo.

Para todos $z = a + bi$ e $h = c + di$ em $\mathbb{C}$; definimos:

$+: z + h = (a + bi) + (c + di) = (a + c) + (b + d)i;$

$\cdot : zh = (a + bi)(c + di) = ac - bd + (ad + bc)i.$

Definição 01: Sejam $z_1 = a + bi$ e $z_2 = c + di$ elementos em $\mathbb{C}$. Então:

a) dizemos que o número complexo $i = 0 + i$ é a *unidade imaginária*;

b) os números reais $a = \text{Re}(z_1)$ e $b = \text{Im}(z_1)$ são, respectivamente, a *parte real* e a *parte imaginaria* do número complexo z_1. A parte imaginária é a que acompanha a unidade imaginária i;

c) definimos $\bar{z_1} = a - bi$ como sendo o *conjugado* do número complexo z_1;

d) Diremos que os números complexos z_1 e z_2 são iguais, se e somente se, valer que $\text{Re}(z_1) = \text{Re}(z_2)$ e $\text{Im}(z_1) = \text{Im}(z_2)$.

Observação 01: Seja $0 \neq z = a + bi \in \mathbb{C}$. Então, vale que $z^{-1} = \frac{\bar{z}}{a^2+b^2} = \frac{a}{a^2+b^2} - \frac{b}{a^2+b^2}i$ é o inverso multiplicativo de z.

Isso pode ser verificado da seguinte forma: seja $z^{-1} = x + yi$. Então, vale a condição $z^{-1}z = 1 = 1 + 0i$. Usando a definição de multiplicação em $\mathbb{C}$, obtemos $z^{-1}z = (x + yi)(a + bi) = (ax - by) + (bx + ay)i = 1 = 1 + 0i$. Pela igualdade definida no item d) da definição anterior, temos o pequeno sistema linear $\begin{cases} ax - by = 1 \\ bx + ay = 0' \end{cases}$ nas variáveis x e y. Esse sistema é equivalente a $\begin{cases} a^2x - aby = a \\ b^2x + bay = 0 \end{cases}$. Somando essas equações e usando que $0 \neq z = a + bi \Leftrightarrow a^2 + b^2 \neq 0$, obtemos que $(a^2 + b^2)x = a \Leftrightarrow$

$x = \frac{a}{a^2+b^2}$. Substituindo esse valor na 2ª equação, verificamos que $\frac{b^2 a}{a^2+b^2} + bay = 0 \Leftrightarrow$ $y = -\frac{b^2 a}{a^2+b^2}\frac{1}{ba} = \frac{-b}{a^2+b^2}$. Portanto, vale que, $z^{-1} = \frac{\bar{z}}{a^2+b^2}$.

Exemplo 01: O inverso do número complexo $w = 4 - 7i$ é igual $w^{-1} = \frac{4}{65} + \frac{7}{65}i$.

Claro que $\mathbb{R} \subset \mathbb{C}$, já que para todo $r \in \mathbb{R}$, podemos escrever $r = r + 0i$. A ideia é a mesma de extender o conjunto dos números pela *unidade imaginária* $i = \sqrt{-1}$, temos $\mathbb{C} = \mathbb{R}[i]$.

Observação 02: As operações de adição e multiplicação definidas em $\mathbb{C}$ gozam das propriedades listadas na Definição 02, em 1.2. Sendo que 0, o elemento neutro da adição não possui inverso multiplicativo.

Essas operações se ligam da seguinte forma: (**Distributividade da multiplicação em relação à adição**): $\forall\, z, w, h \in \mathbb{C}$, vale que $z(w + h) = zw + zh = wz + hz = (w + h)z$.

A abundância de inverso multiplicativo, conforme a Observação 01 deste parágrafo, tem por

Consequência 01: Em $\mathbb{C}$, se z, w são tais que $zw = 0$, então vale que z= 0 ou w= 0.

Claro é que, se $0 \neq z \in \mathbb{C}$; então, existe z^{-1} e seguem as equivalências $zw = 0 \Leftrightarrow z^{-1}(zw) = z^{-1}0 \Leftrightarrow (z^{-1}z)w = 0 \Leftrightarrow 1\, w = 0 \Leftrightarrow w = 0$. Supondo que $w \neq 0$, os mesmos argumentos mostram que $z = 0$.

Consequência 02: as únicas soluções da equação $z^2 = z$; no universo $\mathfrak{U} = \mathbb{C}$, são $0 = 0 + 0i$ e $1 = 1 + 0i$.

De fato, temos $z^2 = z \Leftrightarrow z(z - 1) = 0$. E, claro, $z = 0 + 0i$ é uma solução dessa equação. Além disso, se $z \neq 0 + 0i$, existe o número z^{-1}, inverso multiplicativo de z e, podemos argumentar que, $z^2 = z \Leftrightarrow z^{-1} z^2 = z^{-1}z \Leftrightarrow z = 1 + 0i$.

Uma forma concreta de estudarmos esses "números abstratos" é identificarmos $\mathbb{C}$ com $\mathbb{R}^2$. Claro, alguns fatos geométricos surgem imediatamente. Como nosso objetivo está centrado nos elementos idempotentes, definidos, neste capítulo, em 1.2, encerramos este parágrafo neste ponto.

1.3.3 O conjunto $M_{m\text{xn}}(\mathbb{R})$ das matrizes de ordem $m$xn com entradas em $\mathbb{R}$

O presente parágrafo será dedicado a uma breve descrição do conjunto das matrizes reais. Seguiremos destacando algumas características de seus elementos, operações e propriedades que têm vínculo com as discussões que faremos. Começamos relembrando a seguinte

Definição 01: Digamos que m e n sejam dois números naturais não nulos. Definimos, assim, *matriz* de ordem m por n $(m \times n)$, a qualquer tabela de m linhas e n colunas, formada por números, os quais se chamam de *entradas da matriz.*

Usualmente, representamos uma matriz de ordem $m \times n$ por uma letra maiúscula de nosso alfabeto, da seguinte forma

$$A = [a_{ij}]_{m\times n} = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1m} \\ a_{21} & a_{22} & \cdots & a_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix}_{m\times n}.$$

Uma *matriz retangular* é toda matriz de ordem $m \times n$, onde temos $m \neq n$, é dita uma matriz retangular. Particularmente, as matrizes retangulares de ordens $1 \times n$ e $m \times 1$, são chamadas de *matriz linha* e *matriz coluna*, respectivamente.

Quando $m = n$, temos o caso de uma *matriz quadrada*, de ordem n (ou m). Denotaremos por $M_{m\text{xn}}(\mathbb{R})$ o conjunto das matrizes retangulares sobre $\mathbb{R}$ de ordem $m \times n$ e por $M_n(\mathbb{R})$, o conjunto das matrizes quadradas de ordem n sobre $\mathbb{R}$.

Algumas matrizes quadradas merecem destaque. Por exemplo, costumamos relacionar os tipos:

a) **Matriz diagonal:** é toda matriz quadrada $A = [a_{ij}]_{n\times n}$, cujas entradas a_{ij}'s são nulas para $i \neq j$ e $1 \leq i, j \leq n$.

b) **Matriz triangular inferior:** é toda matriz quadrada $A = [a_{ij}]_{n\times n}$, cujas entradas a_{ij}'s são nulas para $i < j$.

c) **Matriz triangular superior:** é toda matriz quadrada $A = [a_{ij}]_{n\times n}$, cujas entradas a_{ij}'s são nulas para $i > j$.

Definição 02: diremos que duas *matrizes* são *iguais* se, e somente se, elas possuem a mesma ordem e entradas correspondentes iguais.

Definição 03: Sejam $A = [a_{ij}]_{m\times n}$ e $B = [b_{ij}]_{m\times n}$ elementos de $M_{m\text{x}n}(\mathbb{R})$. Então, podemos definir a seguinte operação de adição:
$+: A + B = [a_{ij}]_{m\times n} + [b_{ij}]_{m\times n} = [a_{ij} + b_{ij}]_{m\times n}$.

Observação 01: A operação de adição definida em $M_{m\text{x}n}(\mathbb{R})$ goza das propriedades listadas na Definição 02, em 1.2. Sendo que $O = \begin{bmatrix} 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{bmatrix}_{m\times n}$ é o elemento neutro da adição e $-A = [-a_{ij}]_{m\times n}$ é o inverso aditivo da matriz A.

Definição 04: Consideremos as matrizes $A \in M_{m\text{x}l}(\mathbb{R})$ e $B \in M_{l\text{x}n}(\mathbb{R})$. Podemos definir a seguinte operação de multiplicação:
$\cdot: AB = C = [c_{ij}]_{m\times n}$, onde para todo $1 \leq i \leq m$ e para todo $1 \leq j \leq n$, cada entrada de C é dada por

$$c_{ij} = \sum_{k=1}^{l} a_{ik} b_{kj} = a_{i1}b_{1j} + \cdots + a_{il}b_{lj}.$$

É preciso entender que essa operação de multiplicação é feita, em geral, tomando matrizes em conjuntos distintos e a matriz produto cai fora desses conjuntos. Claro, em $M_n(\mathbb{R})$ tudo fica acomodado.

Observação 02: Sejam A, B e C matrizes tais que os produtos indicados abaixo são possíveis de serem calculados. Então, valem as seguintes propriedades da multiplicação:
$\mathbf{M_1}$: $A(B + C) = AB + AC$ (Distributiva à esquerda em relação à adição);
$\mathbf{M_2}$: $(A + B)C = AC + BC$ (Distributiva à direita em relação à adição);
$\boldsymbol{M_3}$: $A(BC) = (AB)C$ (Associatividade da multiplicação);
$\mathbf{M_4}$: *se* $A \in M_n(\mathbb{R})$, então $AI_n = I_nA = A$, onde $I_n = \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{bmatrix}_{n\times n}$ (Existe elemento neutro).

Essa é uma matriz diagonal: $I_n = [a_{ij}]_{n\times n}$, onde, para todo $i, j \in \{1, 2, \ldots, n\}$, temos $a_{ij} = 1$, se $i = j$ e $a_{ij} = 0$, se $i \neq j$. Ela é denominada de *identidade* de ordem n.

Essa multiplicação, em geral não comutativa, exige que, se A e B são matrizes que comutam, ou seja, se $AB = BA$, então A e B são matrizes quadradas (de mesma ordem).

Observação 03: Diferentemente das propriedades da operação de multiplicação definida em $\mathbb{C}$, temos em $M_n(\mathbb{R})$ que:

a) se A e B são matrizes tais que $AB = 0$, então, em geral não vale que $A = 0$ ou $B = 0$.

b) as soluções da equação $X^2 = X$, em geral, não são somente O e I_n.

Primeiramente, para as matrizes não nulas $A = \begin{bmatrix} p & 0 \\ q & 0 \end{bmatrix}_{2\times 2}, \forall\, p, q \in \mathbb{R}$, e $B = \begin{bmatrix} 0 & 0 \\ 7 & 3 \end{bmatrix}_{2\times 2}$, o produto que obtemos é $AB = 0$. Isso mostra que existem muitos divisores de zero em $M_2(\mathbb{R})$.

Agora, a matriz $E = \begin{bmatrix} 1 & 0 & s \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix}_{3\times 3}$, $\forall\, s \in \mathbb{R}$, que não é a matriz nula e nem a matriz I_3, é tal que $E^2 = E$ e isso mostra que existem infinitos elementos idempotentes em $M_3(\mathbb{R})$.

Exemplo 01: A matriz $O \neq N = \begin{bmatrix} 0 & 7 & 2 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{bmatrix}_{3\times 3}$ é tal que $O \neq N^2$ e $N^3 = 0$, ou seja, N é uma matriz nilpotente.

Definição 05: Uma matriz quadrada A de ordem n é *inversível* se, e somente se, existe uma matriz B tal que $AB = BA = I_n$.

Nesse caso, denotamos por $B = A^{-1}$, a inversa de A. Claro que a ordem de B é a mesma de A. Além disso, $B^{-1} = A$.

Exemplo 02: As matrizes $A = \begin{bmatrix} 3 & 5 \\ 1 & 2 \end{bmatrix}_{2\times 2}$ e $B = \begin{bmatrix} 2 & -5 \\ -1 & 3 \end{bmatrix}_{2\times 2}$ são tais que $AB = BA = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}_{2\times 2}$. Então, a matriz B é a inversa de A, e vice-versa.

Encerraremos esse assunto listando algumas propriedades comumente relacionadas à existência da inversa (multiplicativa) de uma matriz. Isso merece

destaque devido ao fato de que existem infinitas matrizes quadradas que não são inversíveis.

Observação 04: Sejam $A, B \in M_n(\mathbb{R})$, onde $1 \leq n \in \mathbb{N}$. Então:
a) se existir A^{-1}, a inversa da matriz A, ela é única.
b) se A é inversível, A^{-1} é também inversível e $(A^{-1})^{-1} = A$.
c) se A e B são inversíveis, AB também é inversível e $(AB)^{-1} = B^{-1}A^{-1}$.

Inicialmente, se A é uma matriz inversível, com inversas B e C, vale que $AB = BA = AC = CA = I_n$ e, assim, $AC = I_n \Leftrightarrow BAC = BI_n \Leftrightarrow I_nC = B \Leftrightarrow C = B$.

Agora, se A^{-1} é inversível, existe uma matriz X para a qual $A^{-1}X = XA^{-1} = I_n$. Porém, temos que $A^{-1}A = AA^{-1} = I_n$ e o item a) diz que $(A^{-1})^{-1} = A$.

Usando a associatividade, $(AB)(B^{-1}A^{-1}) = A(BB^{-1})A^{-1} = AI_nA^{-1} = AA^{-1} = I_n$ e $(B^{-1}A^{-1})(AB) = B^{-1}(A^{-1}A)B = B^{-1}I_nB = B^{-1}B = I_n$. Então, AB é inversível com (única) inversa $(AB)^{-1} = B^{-1}A^{-1}$.

1.3.4 O conjunto $\mathbb{Z}_n$ das classes residuais módulo n

Fixado um inteiro $2 \leq n \in \mathbb{Z}$, podemos definir uma *relação de equivalência*, denominada *congruência módulo n*, da seguinte forma:

$$\forall\, x, y \in \mathbb{Z}, x \equiv y (\text{mod}\, n) \Leftrightarrow x - y = kn, \text{onde}\, k \in \mathbb{Z} \Leftrightarrow x - y \in n\mathbb{Z}.$$

Como toda relação de equivalência, o *conjunto quociente* (de todas as classes de equivalência) ${}^{\mathbb{Z}}/_{\equiv (\text{mod}\, n)} = \mathbb{Z}_n = \{\bar{x} \,/\, x \in \mathbb{Z}\}$ é uma partição do conjunto $\mathbb{Z}$.

Para ver os detalhes da construção da álgebra que esse conjunto oferece, o leitor pode consultar a referência bibliográfica [4], parágrafo 2.6 do capítulo 2, págs. 30, 31 e 32. Todas as afirmações que vamos incluir aqui são de fácil verificação.

Observação 01: O conjunto das classes determinadas pela relação $\equiv (\text{mod}\, n)$ possui n elementos. Precisamente, temos $\mathbb{Z}_n = \{\bar{0}, \bar{1}, \bar{2}, \cdots, \overline{n-1}\}$ e podemos definir as seguintes operações de adição e multiplicação, de acordo com as regras abaixo.

Para todos $\bar{x}, \bar{y} \in \mathbb{Z}_n$, definimos:
$+: \bar{x} + \bar{y} = \overline{x + y}$.
$\cdot: \bar{x}\bar{y} = \overline{xy}$.

Observação 02: A operação de adição definida em $\mathbb{Z}_n$ goza das propriedades listadas na Definição 02, em 1.2. Sendo que $\overline{0}$ é o elemento neutro da adição e $\overline{-x}$ é o inverso aditivo da classe $\bar{x}$.

Com relação à operação de multiplicação, valem as propriedades listadas na

Observação 03: Sejam $\bar{x}, \bar{y}$ e $\bar{z}$ elementos quaisquer em $\mathbb{Z}_n$. Então, valem:
$\boldsymbol{M_1}$: $\bar{x}(\bar{y}\bar{z}) = (\bar{x}\bar{y})\bar{z}$ (Associatividade);
$\boldsymbol{M_2}$: $\bar{x}\bar{y} = \bar{y}\bar{x}$ (Comutatividade);
$\mathbf{M_3}$: $\overline{1}\bar{x} = \bar{x}\overline{1} = \bar{x}$ (Existe elemento neutro).

Essas operações se ligam da seguinte forma: (**Distributividade da multiplicação em relação à adição**): $\forall\, \bar{x}, \bar{y}, \bar{z} \in \mathbb{Z}_n$, vale que $\bar{x}(\bar{y} + \bar{z}) = \bar{x}\bar{y} + \bar{x}\bar{z} = \bar{y}\bar{x} + \bar{z}\bar{x} = (\bar{y} + \bar{z})\bar{x}$.

Observação 04: Diferentemente das propriedades da operação de multiplicação definida em $\mathbb{C}$, em $\mathbb{Z}_n$ podemos ter que:
a) se $\bar{x}$ e $\bar{y}$ são classes tais que $\bar{x}\bar{y} = \overline{0}$, em geral não valha que $\bar{x} = \overline{0}$ ou $\bar{y} = \overline{0}$.
b) as soluções da equação $\bar{x}^2 = \bar{x}$, em geral, não sejam somente $\overline{0}$ e $\overline{1}$.

Primeiramente, para as classes não nulas $\overline{2}$ e $\overline{3}$, em $\mathbb{Z}_6 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}\}$, o produto que obtemos é $\overline{2}\overline{3} = \overline{6} = \overline{0}$. Isso mostra que também existem divisores de zero em $\mathbb{Z}_6$.

Agora, a classe $\overline{3}$, que não é a classe $\overline{0}$ e nem a classe $\overline{1}$, é tal que $\overline{3}^2 = \overline{9} = \overline{3}$ e isso mostra que existem mais elementos idempotentes em $\mathbb{Z}_6$ do que em $\mathbb{C}$, por exemplo.

Observação 05: Quando é que em $\mathbb{Z}_n$ um elemento $\bar{x}$ é idempotente? Quando $x^2 = qn + x$, já que, passando a barra, temos $\bar{x}^2 = \overline{x^2} = \overline{qn + x} = \overline{qn} + \bar{x} = \bar{q}\overline{0} + \bar{x} = \bar{x}$.

Exemplo 01: Em $\mathbb{Z}_{72}$ temos que $x^2 - x = 72q \Leftrightarrow x(x-1) = 72q$. Então, dado que $9(9-1) = 72.1$ e $64(64-1) = 72.56$, temos que, além $\overline{0}$ e $\overline{1}$, também são idempotentes os elementos $\overline{9}$ e $\overline{64}$ de $\mathbb{Z}_{72}$.

Encerramos as discussões deste parágrafo acreditando que o leitor também vai perceber que elas já são suficientes para justificar as observações do Capítulo 2 que envolve os elementos idempotentes de $\mathbb{Z}_n$.

1.3.5 O conjunto $P(\Omega) = \{X \,/\, X \subset \Omega\}$ e as operações união e interseção

Quando pensamos em escrever sobre os elementos idempotentes de um conjunto, quase deixamos de fora aqueles conjuntos mais gerais em que os divisores de zero existem em grandes quantidades ou aqueles conjuntos em que esse conceito não influencia na abordagem que queremos fazer logo em frente.

A equação $X^2 = X$, já no conjunto das matrizes, como mostramos no item b) da Observação 03, no parágrafo 1.3.3, pode possuir infinitas soluções, mostrando a abundância de elementos idempotentes em $M_3(\mathbb{R})$. O que também vai acontecer no conjunto que vamos definir a seguir.

Observação 01: Em $P(\Omega) = \{X \,/\, X \subset \Omega\}$ estão bem definidas as operações $\cup$ (união) e $\cap$ (interseção) (ver definições em vi) e vii), em 1.1, na pág. 13 deste Capítulo) e, além disso, vale a seguinte

Observação 02: As operações de união e interseção definidas em $P(\Omega)$ gozam das propriedades listadas na Definição 02, em 1.2. Sendo que Φ é o elemento neutro da união e Ω é o elemento neutro da interseção.

Essas operações se ligam da seguinte forma: (**Distributividade da união em relação à interseção**): $\forall\, X, Y, Z \in P(\Omega)$, vale que $X \cup (Y \cap Z) = (X \cup Y) \cap (X \cup Z)$. Também vale que $X \cap (Y \cup Z) = (X \cap Y) \cup (X \cap Z)$.

Observação 03: Em $P(\Omega) = \{X \,/\, X \subset \Omega\}$ temos que:

a) se A e B são conjuntos tais que $A \cap B = \Phi$, então, em geral não vale que $A = \Phi$ ou $B = \Phi$. E, por uma aceitável analogia, podemos ter divisores de zero em $P(\Omega)$.

b) as soluções das equações (1): $X^2 = X \cup X = X$ e (2): $X^2 = X \cap X = X$, não são somente Φ e Ω. E temos, mais uma vez, abundância de elementos idempotentes, independentemente da escolha de uma dessas operações.

Primeiro, se $\Omega = \{a, b, c\}$, temos $P(\Omega) = \{\Phi, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \Omega\}$ e para os conjuntos não vazios $A = \{b\}$ e $B = \{a, c\}$, a interseção é o conjunto $A \cap B = \Phi$. Isso mostra que existem divisores de zero em $P(\Omega)$.

Agora, $\forall\, E \in P(\Omega)$, vale que $E^2 = E \cup E = E$ e $E^2 = E \cap E = E$ e isso mostra que existem muitos elementos idempotentes em $P(\Omega)$. Na verdade, independente da operação, seja união ou interseção, todos os elementos de $P(\Omega)$ são idempotentes.

1.4 Homomorfismos

A palavra homomorfismo é de origem grega. É um combinado das palavras “homos” que significa "mesmo" e “morphe” que significa "formato". Os homomorfismos são funções especiais que nos permitem comparar dois conjuntos, nos quais operações como a adição e a multiplicação estão definidas.

Vamos exemplificar isso, mostrando que, de fato, $\mathbb{C}$ e o plano $\mathbb{R}^2$ possuem a mesma estrutura algébrica.

Mas, o principal objetivo deste TCC é, a partir do número de elementos idempotentes de um conjunto $F \neq \Phi$, estimar o número de seus endomorfismos, que são os homomorfismos de F em si mesmo.

Definição 01: Sejam X e Y conjuntos não vazios. Suponha que $*$ é uma operação bem definida em X e $\square$ é uma operação bem definida em Y.

Dizemos que uma função

$$\begin{aligned} \varphi: X &\longrightarrow Y \\ x &\rightsquigarrow \varphi(x) \end{aligned}$$

é um *homomorfismo* se, e somente se, $\forall\, a, b \in X$, vale que $\varphi(a * b) = \varphi(a) \square \varphi(b)$.

Se as operações $*$ e $\square$ forem operações de adição é comum dizer que φ é um *homomorfismo aditivo* e que φ é um *homomorfismo multiplicativo*, se $*$ e $\square$ forem operações de multiplicação.

Contudo, existem homomorfismos que agem transformando somas em produtos e, vice versa. Exemplos comuns são as funções elementares

$$\begin{aligned} exp:\ \mathbb{R} &\longrightarrow \mathbb{R}_+\backslash\{0\} \\ r &\rightsquigarrow exp(r) \end{aligned} \qquad \text{e} \qquad \begin{aligned} ln:\ \mathbb{R}_+\backslash\{0\} &\longrightarrow \mathbb{R} \\ r &\rightsquigarrow ln(r) \end{aligned}$$

Um homomorfismo injetivo é denominado de *monomorfismo*. Se for sobrejetivo é denominado *epimorfismo*. Se for bijetivo é denominado *isomorfismo*.

Observação 01: Se φ é um isomorfismo de X em Y, valem as seguintes propriedades:

a) Se e é o elemento neutro para uma operação $*$ definida em X, e' o elemento neutro para uma operação $\square$ definida em Y e em Y valem as *leis do cancelamento* (ver definição 1.1.7 em [2]) para esta operação, então $\varphi(e) = e'$.

b) Se x^{-1} é o inverso de um elemento x em X, então $\varphi(x^{-1}) = (\varphi(x))^{-1}$.

Podemos escrever $e * e = e$. Daí vem que $e' \square \varphi(e) = \varphi(e) = \varphi(e * e) = \varphi(e) \square \varphi(e)$, já que φ é um homomorfismo. Cancelando $\varphi(e)$ em ambos os membros da igualdade, vemos que $\varphi(e) = e'$.

Agora, sendo $x * x^{-1} = e$, vale que $\varphi(x * x^{-1}) = \varphi(e)$. Como φ é um homomorfismo, conforme o que provamos anteriormente, $\varphi(e) = e'$, vem que $\varphi(x) \square \varphi(x^{-1}) = e'$. Isto mostra que $\varphi(x^{-1}) = (\varphi(x))^{-1}$.

Pense se podemos enfraquecer essa observação, considerando que φ seja somente um homomorfismo.

Exemplo 01: Consideremos o conjunto $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R} = \{(a, b) / a, b \in \mathbb{R}\}$, munido das seguintes operações: $\forall (a, b), (c, d) \in \mathbb{R}^2$,

$+: (a, b) + (c, d) = (a + c, b + d)$

$\therefore (a, b).(c, d) = (ac - bd, ad + bc)$.

É fácil ver que valem as mesmas propriedades das operações da adição e da multiplicação definidas em $\mathbb{C}$. Além disso, a função

$$\delta: \mathbb{C} \longrightarrow \mathbb{R} \times \mathbb{R}$$
$$a + bi \quad \rightsquigarrow \delta(a + bi) = (a, b)$$

é um isomorfismo.

Primeiramente, $\forall\, a + bi, c + di \in \mathbb{C} = D(\delta)$, se $\delta(a + bi) = \delta(c + di)$, vale que $(a, b) = (c, d) \Leftrightarrow a = c$ e $b = d$. Isso mostra que $a + bi = c + di$ e, assim, δ é injetiva.

Para toda dupla (a, b) em $\mathbb{R} \times \mathbb{R} = CD(\delta)$, $\exists$ um número complexo $a + bi$ em $\mathbb{C} = \mathrm{D}(\delta)$, tal que $\delta(a + bi) = (a, b)$. Portanto, δ é sobrejetiva.

Por fim, temos $\delta\big((a + bi) + (c + di)\big) = \delta\big((a + c) + (b + d)i\big) = (a + c, b + d) = (a, b) + (c, d) = \delta(a + bi) + \delta(c + di), \forall\, a + bi, c + di \in \mathbb{C} = D(\delta)$, ou seja, δ é um homomorfismo aditivo. Com relação a operação de multiplicação, temos também que $\delta\big((a + bi)(c + di)\big) = \delta\big((ac + bd).(ad + bc)i\big) = (ac - bd, ad + bc) = (a, b)(c, d) = \delta(a + bi)\delta(c + di)$, para quaisquer $a + bi, c + di$ em $\mathbb{C} = D(\delta)$. Daí, δ é também um homomorfismo multiplicativo. Isso mostra que $\mathbb{C}$ é isomorfo a $\mathbb{R}^2$, o que indicamos por $\mathbb{C} \cong \mathbb{R}^2$.

Nessas argumentações admitimos conhecida a definição de igualdade entre os vetores de $\mathbb{R}^2$. Elas mostram que os objetos de $\mathbb{C}$ têm uma forma mais concreta, vistos exatamente como vetores do plano.

O conceito de homomorfismo é usado na Álgebra abstrata para descrever uma relação entre duas estruturas algébricas. Esse tipo de função aparece, por exemplo, quando desenvolvemos estudos sobre grupos, anéis ou espaços vetoriais.

É importante notar que em todos os conjuntos descritos nesta parte de nosso trabalho todas as operações que foram relacionadas admitem a associatividade. A comutatividade, que não vale para a multiplicação de matrizes, implica diretamente na contagem dos homomorfismos que vamos definir sobre o conjunto $M_3(\mathbb{R})$ das matrizes quadradas de ordem 3 (com entradas em $\mathbb{R}$).

Isso aponta que a qualidade dessas funções que relacionamos aqui em nosso trabalho também está ligada à estrutura de seus domínios.

Capítulo 2: Idempotência e endomorfismos

Associatividade, comutatividade e idempotência são propriedades de uma operação $*$ definida em um conjunto e que aparecem nos assuntos envolvidos com a Matemática básica.

Este capítulo vai deixar claro que o número de elementos do conjunto $\mathfrak{E}(S)$, dos *endomorfismos* de um conjunto $S \neq \Phi$, no qual uma operação $*$ esteja definida, que são homomorfismos de S em si mesmo, podem ser contados a partir do número de elementos do conjunto $\mathcal{I}_{d_*}(S)$, dos elementos idempotentes de S com relação à operação $*$. Isso, a depender das propriedades dessa operação.

Então, o que se deve perceber é que a problemática de nosso trabalho é a de considerar uma operação $*$, definida em um conjunto $S \neq \Phi$, e verificar de que forma um elemento $s \in S$, tal que $s^2 = s$, está ligado a uma função φ que age de S para S e que satisfaz a condição: $\forall\, m, n \in S$, vale que $\varphi(m * n) = \varphi(m) * \varphi(n)$.

Exemplo 01: Vamos olhar para a função real elementar

$$f: \mathbb{R} \longrightarrow \mathbb{R}$$
$$r \rightsquigarrow f(r) = a * r, \text{ onde } a \in \mathbb{R} \text{ e } * \text{ é uma operação definida em } \mathbb{R}.$$

Nesse caso, vamos admitir o valor $a = 0$ o que equivale a admitirmos que, em um dos casos, $f = \mathcal{O}$ seja a função identicamente nula.

Podemos relacionar alguns casos de homomorfismos, conforme a lista a seguir.

i) Se $a = 0$ e $* = +$ é a operação de adição, podemos definir

$$f: \mathbb{R} \longrightarrow \mathbb{R}$$
$$r \rightsquigarrow f(r) = 0 + r = r$$

Observamos que, para quaisquer $x, y \in \mathbb{R}$, vale $f(x + y) = x + y = f(x) + f(y)$ e que $0 = 0^2 = 0 + 0$ é o único elemento idempotente de $\mathbb{R}$, com respeito à operação de adição. Nesse caso, $f = i_{\mathbb{R}}$ é a função identidade em $\mathbb{R}$.

ii) Se $a = 0$ ou 1 e $* = \cdot$ é a operação de multiplicação, podemos definir

$$\mathcal{O}: \mathbb{R} \longrightarrow \mathbb{R} \qquad \text{e} \qquad i_{\mathbb{R}}: \mathbb{R} \longrightarrow \mathbb{R}$$
$$r \rightsquigarrow f(r) = 0 \cdot r = 0 \qquad\qquad r \rightsquigarrow f(r) = 1 \cdot r = r$$

Então, para quaisquer $x, y \in \mathbb{R}$, vale que $\mathcal{O}(x \cdot y) = 0 = 0 \cdot 0 = \mathcal{O}(x) \cdot \mathcal{O}(y)$, $i_{\mathbb{R}}(x \cdot y) = x \cdot y = i_{\mathbb{R}}(x) \cdot i_{\mathbb{R}}(y)$ e que $0 = 0^2 = 0 \cdot 0$ e $1 = 1^2 = 1 \cdot 1$ são os únicos

elementos idempotentes de $\mathbb{R}$, com respeito à operação de multiplicação. Nesse caso, $f = \mathcal{O}$ é a função identicamente nula ou $f = i_{\mathbb{R}}$ é a função identidade em $\mathbb{R}$.

Agora, olhemos para a conhecida função (real) linear que relacionamos no

Exemplo 02: Consideremos a função (real)

$$f: \mathbb{R} \longrightarrow \mathbb{R}$$
$$r \rightsquigarrow f(r) = ar, \text{onde } 0 \neq a \in \mathbb{R}.$$

Claro, $\forall\, 0 \neq a \in \mathbb{R}$, vale que $f(m+n) = a(m+n) = am + an = f(m) + f(n)$, $\forall\, m, n \in \mathbb{R}$. Então, esse é mais um endomorfismo de $\mathbb{R}$!

Mas, a pode ser qualquer número real, inclusive, um número tal que $a^2 \neq a$; ou seja, um elemento que não seja idempotente.

Por exemplo, se $a = 7$, temos $7^2 = 14$ ou $7^2 = 49$, a depender da operação que for escolhida, adição ou multiplicação. Portanto, 7 não é idempotente e, mesmo assim, definindo $f(r) = 7r$, $\forall\, r \in \mathbb{R}$, ainda temos um endomorfismo de $\mathbb{R}$.

Definição 01: Seja $S \neq \Phi$ um conjunto no qual uma operação $*$ esteja definida.
i) Dizemos que φ é um endomorfismo de S, que é "$*$ *dependente*" se, e somente se, a ação homomórfica de φ só depende da operação $*$.
ii) Se também, $\square$ está definida em S, dizemos que φ é um endomorfismo de S, que é "$*, \square$ *dependente*" se, e somente se, a ação homomórfica de φ depende das operação $*$ e $\square$ (nessa ordem).

Podemos classificar os seguintes endomorfismos

Exemplo 03:
i) A aplicação do exemplo 02 que é dada por $f(r) = ar, \text{onde } 0 \neq a \in \mathbb{R}$ satisfaz a condição de que $f(m+n) = a(m+n) = am + an = f(m) + f(n)$, $\forall\, m, n \in \mathbb{R}$. Então, f é um endomorfismo de $\mathbb{R}$, que é $+, \cdot$ *dependente*.
ii) A aplicação $i_{\mathbb{R}}$ é um endomorfismo simultaneamente $+$ *dependente* e $\cdot$ *dependente*, já que $i_{\mathbb{R}}(m+n) = m+n = i_{\mathbb{R}}(m) + i_{\mathbb{R}}(n)$ e, também $i_{\mathbb{R}}(m \cdot n) = m \cdot n = i_{\mathbb{R}}(m) \cdot i_{\mathbb{R}}(n)$, $\forall\, m, n \in \mathbb{R}$.

Observação 01: Os únicos endomorfismos de $\mathbb{Z}$ simultaneamente $\cdot$ *dependente* e $+$ *dependente* são: $\mathcal{O}$, a função identicamente nula, e $i_{\mathbb{Z}}$, o homomorfismo identidade em $\mathbb{Z}$.

Isso pode ser verificado da seguinte maneira: suponhamos que φ é um endomorfismo de $\mathbb{Z}$ simultaneamente $\cdot$ *dependente* e $+$ *dependente*. Segue, então, que

$$\forall\, m, n \in \mathbb{Z}, \text{temos } \varphi(m \cdot n) = \varphi(m) \cdot \varphi(n) \text{ e } \varphi(m+n) = \varphi(m) + \varphi(n).$$

Por conseguinte, vale que

a) $\varphi(0) = 0$

b) $\varphi(-1) = -\varphi(1)$.

c) $\varphi(1) = 1$ ou $\varphi(1) = 0$

O resultado do item a) e do item c), com relação a $\varphi(1) = 1$, já sabemos que valem pelo item a), da Observação 01, em 1.4.

Argumentando que

$$\varphi(1) = \varphi(1 \cdot 1) = \varphi(1) \cdot \varphi(1) = \varphi(1)^2 \Leftrightarrow \varphi(1)^2 - \varphi(1) = 0$$

Pela Consequência 02, da Observação 01 em 1.3.1, fazendo $\mathfrak{U} = \mathbb{Z}$, podemos ver que $\varphi(1) = 1$ ou $\varphi(1) = 0$.

A soma $\varphi(-1) + \varphi(1) = \varphi(-1+1) = \varphi(0) = 0$ significa que $\varphi(-1) = -\varphi(1)$ e o item b) também está justificado.

Por fim, $\forall\, m \in \mathbb{Z}$, temos

$\varphi(m) = \varphi(1 \cdot m) = \varphi(1) \cdot \varphi(m) = 0 \cdot \varphi(m) = 0$, o que mostra que $\varphi = \mathcal{O}$ é a função identicamente nula.

De outra forma, $\forall\, 0 < m \in \mathbb{Z}$, temos

$$\varphi(m) = \varphi\left(\underbrace{1 + 1 + \ \ldots\ + 1}_{m\ vezes}\right) = \varphi(1) + \varphi(1) + \ldots\ \varphi(1) = 1 + 1 + \ \ldots\ + 1 = m.$$

Agora, se $m < 0$, vale que $0 < -m \in \mathbb{Z}$ e, pelo exposto acima, $\varphi(-m) = -m$. Segue, portanto que

$$\varphi(m) = \varphi\big((-1) \cdot (-m)\big) = \varphi(-1) \cdot \varphi(-m) = \big(-\varphi(1)\big) \cdot (-m) = (-1) \cdot (-m) = m.$$

Concluímos, então que, se $\varphi(1) = 1$, que é a outra possibilidade, temos $\varphi = i_{\mathbb{Z}}$.

Não serão demonstradas, mas o leitor deve imaginar uma forma de justificar a validade das seguintes observações

Observação 02: Os únicos endomorfismos de $\mathbb{Q}$ simultaneamente $\cdot$ *dependente* e $+$ *dependente* são: $\mathcal{O}$, a função identicamente nula e $i_{\mathbb{Q}}$, a aplicação identidade em $\mathbb{Q}$.

Observação 03: Os únicos endomorfismos de $\mathbb{R}$ simultaneamente $\cdot$ *dependente* e $+$ *dependente* são: $\mathcal{O}$, a função identicamente nula e $i_{\mathbb{R}}$, a aplicação identidade em $\mathbb{R}$.

Justificados esses fatos, pode ser perguntado sobre os endomorfismos de $\mathbb{C}$ simultaneamente $\cdot$ *dependente* e $+$ *dependente*. Provavelmente, pelo fato de não usarmos o ordenamento na justificativa da Observação 01. O leitor pode investigar se isso é necessário para justificar as observações 2 e 3. Caso não seja preciso, o não ordenamento dos números complexos não deve influenciar na investigação dos endomorfismos de $\mathbb{C}$.

2.1 Contando endomorfismos

Um bom resultado à respeito do número de endomorfismo de um conjunto $S \neq \Phi$ seria se, precisamente, esse número coincidisse com o número de elementos idempotentes de S.

Nos conjuntos numéricos que exibimos anteriormente, como por exemplo, no conjunto $\mathbb{Z}$, a equação $x^2 = x$ fornece 0 como elemento idempotente com relação a adição e

$$\begin{aligned} i_{\mathbb{Z}} &: \mathbb{Z} \longrightarrow \mathbb{Z} \\ z &\rightsquigarrow i_{\mathbb{Z}}(r) = 0 + z = z \end{aligned}$$

é um endomorfismo de $\mathbb{Z}$, $+$ *dependente*, que pode ser contado.

Agora, 0 e 1 são elementos idempotentes com relação a multiplicação. Pela observação 1, na página 32 deste trabalho, podemos contar $\mathcal{O}$ e $i_{\mathbb{Z}}$ como endomorfismos de $\mathbb{Z}$, $\cdot$ *dependentes*. Essas funções podem ser denotadas por

$$\begin{aligned} \mathcal{O}&: \mathbb{Z} \longrightarrow \mathbb{Z} \\ z &\rightsquigarrow \mathcal{O}(r) = 0 \cdot z = 0 \end{aligned} \qquad \text{e} \qquad \begin{aligned} i_{\mathbb{R}}&: \mathbb{Z} \longrightarrow \mathbb{Z} \\ z &\rightsquigarrow i_{\mathbb{R}}(r) = 1 \cdot z = z \end{aligned}$$

Ainda,

$$\begin{aligned} \varphi_a &: \mathbb{Z} \longrightarrow \mathbb{Z} \\ z &\rightsquigarrow \varphi_a(z) = az, \text{com } a \in \mathbb{Z}. \end{aligned}$$

é um endomorfismo de $\mathbb{Z}$, que é $+$, $\cdot$ *dependente*, para todo $a \in \mathbb{Z}$. Temos que: $\forall\, m, n \in \mathbb{Z}$, vale que $\varphi_a(m+n) = a(m+n) = am + an = \varphi(m) + \varphi(n)$, $\forall\, a \in \mathbb{Z}$.

Portanto, temos infinitos endomorfismos de $\mathbb{Z}$, $+$, $\cdot$ *dependentes*. Nesse caso, a generalidade de $a \in \mathbb{Z}$ já inclui os elementos 0 e 1 que são os idempotentes em $\mathbb{Z}$ (claro, levando em consideração a operação $+$ e $\cdot$, conforme já mencionamos).

Vamos destacar mais um exemplo de contagem. Vejamos o

Exemplo 01: Em $\mathbb{Z}_{12} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4} \cdots, \overline{11}\}$ estão bem definidas uma adição $+$ e uma multiplicação $\cdot$, conforme a observação 01, em 1.3.4 e

a) com relação a essa adição, $\bar{0}$ é o único elemento idempotente. Podemos contar 1 endomorfismo $+$ *dependente* que é

$$\begin{aligned} i_{\mathbb{Z}_{12}}\colon \mathbb{Z}_{12} &\longrightarrow \mathbb{Z}_{12} \\ x &\rightsquigarrow i_{\mathbb{Z}_{12}}(x) = \bar{0} + x = x \end{aligned}$$

b) com relação a essa multiplicação, $\bar{0}$,$\bar{1}$ e $\bar{4}$ são os 3 elementos idempotentes. Podemos, pelo menos, contar 3 endomorfismos $\cdot$ *dependentes*, que são:

$$\begin{aligned} \mathcal{O}\colon \mathbb{Z}_{12} &\longrightarrow \mathbb{Z}_{12} \\ x &\rightsquigarrow \mathcal{O}(x) = \bar{0} \cdot x = \bar{0} \end{aligned} \quad ; \quad \begin{aligned} i_{\mathbb{Z}_{12}}\colon \mathbb{Z}_{12} &\longrightarrow \mathbb{Z}_{12} \\ x &\rightsquigarrow i_{\mathbb{Z}_{12}}(x) = \bar{1} \cdot x = x \end{aligned} \quad \text{e}$$

$$\begin{aligned} \xi\colon \mathbb{Z}_{12} &\longrightarrow \mathbb{Z}_{12} \\ x &\rightsquigarrow \xi(x) = \bar{4} \cdot x \end{aligned}$$

Notemos que a ação de ξ é da seguinte forma: $\forall\, x, y \in \mathbb{Z}_{12}$, temos que $\xi(x \cdot y) = \bar{4} \cdot (x \cdot y) = \bar{4} \cdot \bar{4} \cdot (x \cdot y) = \bar{4} \cdot (\bar{4} \cdot x) \cdot y = \bar{4} \cdot (x \cdot \bar{4}) \cdot y = (\bar{4} \cdot x) \cdot (\bar{4} \cdot y)$.

Ainda,

$$\begin{aligned} \xi_t\colon \mathbb{Z}_{12} &\longrightarrow \mathbb{Z}_{12} \\ x &\rightsquigarrow \xi_t(x) = t \cdot x, \text{com } t \in \mathbb{Z}_{12}. \end{aligned}$$

é um endomorfismo de $\mathbb{Z}_{12}$, que é $+$, $\cdot$ *dependente*, para todo $t \in \mathbb{Z}_{12}$. Temos que: $\forall\, x, y \in \mathbb{Z}_{12}$, vale que $\xi_t(x + y) = t \cdot (x + y) = t \cdot x + t \cdot y = \xi_t(x) + \xi_t(y), \forall\, t \in \mathbb{Z}_{12}$.

Portanto, temos, pelo menos, 12 endomorfismos de $\mathbb{Z}_{12}$, $+$, $\cdot$ *dependentes*. Nesse caso, a lista dos elementos $t \in \mathbb{Z}_{12}$ já inclui os elementos $\bar{0}$,$\bar{1}$ e $\bar{4}$ que são os idempotentes em $\mathbb{Z}_{12}$ (claro, levando em consideração a operação $+$ e $\cdot$, conforme já mencionamos).

2.2 Endomorfismos de conjuntos não numéricos

Vamos ampliar nossos exemplos de contagem, olhando para $P(\Omega) = \{X \,/\, X \subset \Omega\}$ e considerando as operações $\cup$ (união) e $\cap$ (interseção) e suas propriedades apresentadas no parágrafo 1.3.5.

Conforme a observação 3, em 1.3.5, todos os elementos de $P(\Omega)$ são idempotentes, não importando se a operação considerada é $\cup$ ou $\cap$. Podemos contar, então, $\#P(\Omega)$ endomorfismos de $P(\Omega)$, que são $\cup$ *dependentes* e também $\#P(\Omega)$ endomorfismos de $P(\Omega)$, que são $\cap$ *dependentes*, conforme os itens a) e b) do

Exemplo 01: Com relação a $P(\Omega) = \{X \,/\, X \subset \Omega\}$ temos que:

a) $\lambda_L : P(\Omega) \longrightarrow P(\Omega)$
$X \quad \rightsquigarrow \lambda_L(X) = L \cup X, \text{com } L \in P(\Omega)$

é um endomorfismo de $P(\Omega)$, que é $\cup$ *dependente*, $\forall\, L \in P(\Omega)$; já que: $\forall\, X, Y \in P(\Omega)$, $\lambda_L(X \cup Y) = L \cup (X \cup Y) = (L \cup L) \cup (X \cup Y) = L \cup (L \cup X) \cup Y = L \cup (X \cup L) \cup Y = (L \cup X) \cup (L \cup Y) = \lambda_L(X) \cup \lambda_L(Y)$.

b) $\gamma_L : P(\Omega) \longrightarrow P(\Omega)$
$X \quad \rightsquigarrow \gamma_L(X) = L \cap X, \text{com } L \in P(\Omega)$

é um endomorfismo de $P(\Omega)$, que é $\cap$ *dependente*, $\forall\, L \in P(\Omega)$, já que: $\forall\, X, Y \in P(\Omega)$, $\gamma_L(X \cap Y) = L \cap (X \cap Y) = (L \cap L) \cap (X \cap Y) = L \cap (L \cap X) \cap Y = L \cap (X \cap L) \cap Y = (L \cap X) \cap (L \cap Y) = \gamma_L(X) \cap \gamma_L(Y)$.

c) Os λ_L, para todo $L \in P(\Omega)$, são endomorfismos $\cap$, $\cup$ *dependentes*, pois $\forall\, X, Y \in P(\Omega)$, $\lambda_L(X \cap Y) = L \cup (X \cap Y) = (L \cup X) \cap (L \cup Y) = \lambda_L(X) \cap \lambda_L(Y)$.

d) Os γ_L, para todo $L \in P(\Omega)$, são endomorfismos $\cup$, $\cap$ *dependentes*, pois $\forall\, X, Y \in P(\Omega)$, $\gamma_L(X \cup Y) = L \cap (X \cup Y) = (L \cap X) \cup (L \cap Y) = \gamma_L(X) \cup \gamma_L(Y)$.

Pelos itens c) e d), podemos contar, então, $\#P(\Omega)$ endomorfismos de $P(\Omega)$, que são $\cap$, $\cup$ *dependentes* e também $\#P(\Omega)$ endomorfismos de $P(\Omega)$, que são $\cup$, $\cap$ *dependentes*.

Claro que, nos itens a) e b), temos, respectivamente, que $\lambda_\Phi = i_{P(\Omega)}$ é a identidade em $P(\Omega)$ e $\gamma_\Phi = \Phi$ é uma espécie de função identicamente nula.

A observação 3, em 1.3.3, mostra que, com relação à operação de multiplicação, um conjunto de matrizes pode conter muitos elementos idempotentes. Vamos tentar fazer, então, uma contagem dos endomorfismos de um conjunto dessa natureza.

Exemplo 02: No conjunto $M_3(\mathbb{R})$, das matrizes quadradas de ordem 3, já mencionamos que toda matriz $E = \begin{bmatrix} 1 & 0 & s \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix}_{3\times 3}$, onde $s \in \mathbb{R}$, é uma matriz idempotente, com relação à operação de multiplicação, definida em $M_3(\mathbb{R})$. Com relação à adição em $M_3(\mathbb{R})$, somente $O = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}_{3\times 3}$ é idempotente.

Agora,

a) $i_{M_3(\mathbb{R})}: M_3(\mathbb{R}) \longrightarrow M_3(\mathbb{R})$
$A \quad \rightsquigarrow \quad i_{M_3(\mathbb{R})}(A) = 0 + A = A$

é um endomorfismo de $M_3(\mathbb{R})$, que é $+$*dependente*.

b) Também, podemos contar os 2 endomorfismos

$\mathcal{O}: M_3(\mathbb{R}) \longrightarrow M_3(\mathbb{R})$
$A \quad \rightsquigarrow \mathcal{O}(A) = 0 \cdot A = O$

e $i_{M_3(\mathbb{R})}: M_3(\mathbb{R}) \longrightarrow M_3(\mathbb{R})$
$A \quad \rightsquigarrow \quad i_{M_3(\mathbb{R})}(A) = I_3 \cdot A = A$

que são $\cdot$ *dependentes*.

Mas, além de O e I_3 existem infinitos elementos idempotentes com relação à operação de multiplicação.

Então, podemos tentar contar mais endomorfismos que sejam $\cdot$ *dependentes* e do tipo

$\psi_S: M_3(\mathbb{R}) \longrightarrow M_3(\mathbb{R})$
$A \quad \rightsquigarrow \quad \psi_S(A) = S \cdot A, \text{com } S \in M_3(\mathbb{R}) \text{ e } \mathrm{S}^2 = \mathrm{S}\,.$

Acontece que, se $A, B \in M_3(\mathbb{R})$, temos que $\psi_S(A \cdot B) = S(A \cdot B) = \mathrm{S}^2(A \cdot B) = (S \cdot S) \cdot (A \cdot B) = S \cdot (S \cdot A) \cdot B$.

Agora, como prosseguir se, em geral $S \cdot A \neq A \cdot S$? Isso é um forte impedimento. Mas, ainda podemos fazer mais uma contagem. Temos

c) $\delta_M: M_3(\mathbb{R}) \longrightarrow M_3(\mathbb{R})$
$A \quad \rightsquigarrow \quad \delta_M(A) = M \cdot A, \text{com } M \in M_3(\mathbb{R}).$

é um endomorfismo de $M_3(\mathbb{R})$, que é $+, \cdot$ *dependente*, para todo $M \in M_3(\mathbb{R})$. Temos que: $\forall\, A, B \in\ M \in M_3(\mathbb{R})$, vale $\delta_M(A+B) = M \cdot (A+B) = M \cdot A + M \cdot B = \delta_M(A) + \delta_M(B)$.

É preciso notar que são imprescindíveis as propriedades de associatividade e comutatividade das operações envolvidas na definição dos endomorfismos que contamos até aqui, excetuados os nulos e os que são identidades.

Depois do que foi apresentado, encerramos nossas discussões com o seguinte resultado

Observação 01: Seja $S \neq \Phi$ um conjunto. Seja $*$ uma operação bem definida em S e tal que possua todas as propriedades listadas na definição 02, em 1.2. Então:
a) vale que $\mathfrak{E}(S) \neq \Phi$;
b) se $\mathcal{I}_{d_*}(S) = \{s \in S / s^2 = s * s = s\} \neq \Phi$, vale que $\mathfrak{E}(S) \neq \Phi$ e $\#\mathfrak{E}(S) \geq \#\mathcal{I}_{d_*}(S) \geq 1$;
c) se outra operação $\square$ definida S é distributiva em relação à operação $*$, podemos exibir pelo menos $\#S$ endomorfismos de S que sejam $*, \square$ *dependentes*.

Notemos que no item a), a existência de elemento neutro e, a associatividade e comutatividade, permitem que contemos a partir de $e^2 = e * e = e \in \mathcal{I}_{d_*}(S)$ o endomorfismo i_S. Com relação ao item b), podemos contar $\#\mathcal{I}_{d_*}(S) \geq 1$ endomorfismos que são $*$ *dependentes*. E, considerando que, para todo $a \in S$, vale que $\varphi_a(s) = a \square s$ define um endomorfismo de S, o item c) está justificado.

Essa observação encerra nossas discussões. Cada um de seus itens pode ser justificado pelo leitor que acompanhou as nossas contagens a partir dos exemplos dados.

Considerações finais

Voltemos ao exemplo 3, na página 31, item i). A aplicação definida por $f(r) = ar$, onde $0 \neq a \in \mathbb{R}$, é um endomorfismo de $\mathbb{R}$, que é $+,\cdot$ *dependente*. Porém, f não é um endomorfismo de $\mathbb{R}$, $\cdot, +$ *dependente*. Temos, em geral, $f(m \cdot n) = a(m \cdot n) \neq (am) \cdot (an) = f(m) \cdot f(n)$, para $m, n \in \mathbb{R}$.

Isso reforça a necessidade de incluirmos a frase "nessa ordem", no item ii) da definição 1, na página 31.

Associatividade, comutatividade e outras propriedades de operações definidas num conjunto podem influenciar diretamente na "qualidade" de uma aplicação que age sobre ele. Por exemplo, agindo sobre $\mathbb{N}$, onde a adição não admite existência de inversos, não faz sentido discutir se uma aplicação é par ou ímpar.

No exemplo 2, em 2,2, a não comutatividade da multiplicação de matrizes, impede que se possa definir endomorfismos $\cdot$ *dependentes* que agem sobre $M_3(\mathbb{R})$.

O exemplo 1, em 2.2, e a observação 1, na página 32, sugerem que a lista dos endomorfismos de um conjunto é maior à medida que esse conjunto possua mais elementos idempotentes.

Notadamente, existem muitos endomorfismos agindo sobre um conjunto $S \neq \Phi$. Muitas construções foram apontadas na primeira avaliação deste trabalho. Porém, acreditamos que, a partir dos elementos do conjunto $\mathcal{I}_{d_*}(S) = \{s \in S / s^2 = s * s = s\}$, fizemos uma boa contagem dessas funções.

Referências Bibliográficas

1. DOMINGUES, Hygino H. e Iezzi, Gelson. Álgebra Moderna; 4ª Edição; Ed. Atual; 2003.

2. GABRIEL Noah D. S.; Herança de Propriedades; TCC - PROFMAT (Mestrado em Mestrado em Rede Nacional em Matemática); SBM; 2023;

3. GARCIA, Arnaldo; LEQUAIN, Yves. Elementos de álgebra. 3. ed. Rio de Janeiro: IMPA, 2005. 326 p. (Série: Projeto Euclides).

4. GONÇALVES, Adilson; Introdução à álgebra; Projeto Euclides; IMPA; Rio de Janeiro -RJ; 2001.

5. HEFEZ, Abramo. Curso de álgebra vol. 1; IMPA; Rio de Janeiro; 2016.