http://journal.unoeste.br/index.php/ce/index
DOI: 10.5747/ce.2020.v12.n3.e331
ISSN on-line 2178-8332

Colloquium Exactarum

Submetido:27/08/2020 Revisado: 20/09/2020 Aceito: 01/10/2020

ENUMERABILITY OF THE SET OF ALGEBRAIC NUMBERS

Fernanda Loureiro Honorio, Fernando Pereira de Souza

Universidade Federal de Mato Grosso do Sul – UFMS.
E-mail: honorio.fer@outlook.com

RESUMO - Através dos estudos da Teoria de Conjuntos tem-se que a cardinalidade dos conjuntos infinitos é classificada de acordo com a enumerabilidade dos mesmos, tornando assim notável a importância do tema. Sendo assim será abordado, neste trabalho, a Enumerabilidade do Conjunto dos Números Algébricos, através de estudos que foram realizados como parte do projeto de iniciação cientifica vinculado as atividades do grupo PET Conexões de Saberes Matemática da UFMS, Campus de Três Lagoas. Serão apresentados os conceitos necessários para o estudo do Conjunto dos Números Algébricos, expondo suas definições e propriedades, juntamente com exemplos e demonstrações de seus teoremas. Este trabalho além visar o aprofundamento dos estudos sobre o tema, objetiva também, na apresentação do mesmo, uma forma de tornar mais acessível sua compreensão. Dessa forma, encontra-se nos resultados dessa pesquisa a exposição de conceitos básicos sobre a Enumerabilidade de Conjuntos, que facilitam o entendimento das demonstrações mais complexas das proposições que se seguem.
Palavras-chave: números algébricos; enumerabilidade; conjuntos.

ABSTRACT - Through the studies of the Set Theory, the cardinality of the infinite sets is classified according to their enumerability, thus making the importance of the theme remarkable. Therefore, in this work, the enumerability of the Set of Algebraic Numbers will be approached, through studies that were carried out as part of the scientific initiation project linked as activities of the group PET Connections of Knowledge Mathematics at UFMS, Campus of Três Lagoas. The concepts defined for the study of the Algebraic Numbers Set will be conceptualized, exposing their definitions and properties, with examples and accounts of their theorems. This work, besides aiming to deepen the studies on the theme, also aims, in the presentation of the same, a way to make its understanding more accessible. In this way, it is found in the results of this research the exposure of basic concepts about the enumerability of sets, which facilitate the understanding of the most complex counts of the propositions that follow.
Keywords: algebraic numbers; enumerability; sets.

1. INTRODUÇÃO

O Conjunto dos Números Algébricos representa o conjunto dos números reais ou complexos que são solução de alguma equação polinomial com coeficientes inteiros. Sendo assim, torna-se notável a grande variedade de números que tal conjunto representa, sendo estes muitas vezes os mais comuns no dia-a-dia

de todos, como por exemplo, os números racionais. Em contrapartida, as definições e características que acompanham a formalização de tal conjunto não são de conhecimento geral.

Da mesma forma, dentro da Teoria de Conjuntos, encontra-se também a necessidade de estudo sobre a enumerabilidade, visto que através de suas definições obtém-se uma importante ferramenta para a classificação dos conjuntos infinitos em relação a sua cardinalidade. Um conjunto é enumerável quando é finito ou, no caso de conjuntos infinitos, quando existe uma bijeção entre este e o conjunto dos números naturais. Do mesmo modo, dois conjuntos possuem a mesma cardinalidade se existe uma bijeção entre eles. Sendo assim, tem-se que através da enumerabilidade dos conjuntos, sua cardinalidade pode ser classificada a partir do conjunto dos números naturais.

Tendo em vista a importância do estudo desses temas, este trabalho aborda o Conjunto dos Números Algébricos, apontando suas definições e propriedades através de exemplos e demonstrações, e a Enumerabilidade de Conjuntos, apresentando as proposições que surgem a partir de sua definição. Por fim, será abordado a Enumerabilidade do Conjunto dos Números Algébricos, através de demonstrações.

Dessa forma, o presente trabalho objetiva o aprofundamento nos estudos de ambos os temas, que abrem portas para muitas outras áreas da matemática. Além disso, ele visa também uma apresentação gradativa dos temas, que gere no primeiro momento, uma aproximação com os conceitos essenciais para a construção do conhecimento, que torne acessível a compreensão das demonstrações mais complexas apresentadas.

2. METODOLOGIA

O presente trabalho é resultado de pesquisas teóricas, desenvolvidas como parte de uma atividade de pesquisa individual pertencente ao grupo PET Conexões de Saberes Matemática da UFMS, Campus de Três Lagoas. O estudo foi elaborado mediante leituras e resoluções de exercícios para a melhor fixação do conteúdo. Além disso, foram feitas também discussões sobre o tema com o orientador, realizadas através de ferramentas digitais.

Foram estudados, no primeiro momento, as definições e conceitos do Conjunto dos Números Algébricos, e só após a compreensão do tema de forma efetiva a Enumerabilidade de Conjuntos foi abordada, juntamente com suas proposições e aplicações. Por fim, a demonstração da Enumerabilidade do Conjunto dos Números Algébricos foi desenvolvida a partir dos conceitos já estudados anteriormente.

3. RESULTADOS E DISCUSSÕES

Um número real ou complexo α é dito algébrico se é solução de uma equação polinomial da forma

$$a_0 + a_1x + \ldots + a_nx^n = 0,$$

em que $a_0, a_1, \ldots, a_n \in \mathbb{Z}$, não todos nulos.

O conjunto desses números será denotado por $\overline{\mathbb{Q}}$. Usaremos também a notação $P(x) \in \mathbb{Z}[x]$ para caracterizar $P(x) = a_0 + a_1x + \ldots + a_nx^n$, em que $a_0, a_1, \ldots, a_n \in \mathbb{Z}$.

3.1. Conjunto dos Números Algébricos

Definição 1. Sendo $\alpha \in \mathbb{R}$ (ou $\alpha \in \mathbb{C}$) dizemos que $\alpha \in \overline{\mathbb{Q}}$, se existe algum $P(x) \in \mathbb{Z}[x]$ tal que $P(\alpha) = 0$.

Exemplo 1. Todo número racional é algébrico.

Se $x \in \mathbb{Q}$, então $x = \frac{p}{q}$, com $p, q \in \mathbb{Z}$ e $q \neq 0$. Logo, x é raiz do polinômio $qx - p = 0$. Assim, de fato x é um número algébrico.

Exemplo 2. Nem todo número algébrico é racional.

(a) Seja $n \geq 2$ e p primo, então $\sqrt[n]{p}$ é irracional e algébrico.

Suponha que $\sqrt[n]{p}$ onde $n \geq 2$ é inteiro e p primo é racional. Fazendo $\sqrt[n]{p} = \frac{a}{b}$, com $(a, b) = 1$, teríamos

$$\sqrt[n]{p} = \frac{a}{b} \Rightarrow p = \frac{a^n}{b^n} \Rightarrow b^n p = a^n \Rightarrow p|a^n \Rightarrow p|a.$$

Logo, $a = k.p$ com $k \in \mathbb{Z}^*$. Se $b^n p = a^n$ então $b^n p = (k.p)^n = k^n p^n$, assim $b^n = k^n p^{(n-1)}$ implicando que $p|b^n$ de onde $p|b$. Obtemos então que $p|a$ e $p|b$, o que contradiz o fato de $(a, b) = 1$, já que $p \neq 1$. Dessa forma, temos que $\sqrt[n]{p}$ não é um número racional.

Agora, com $x = \sqrt[n]{p}$ tem-se que:

$$x = \sqrt[n]{p} \Rightarrow x^n = p \Rightarrow x^n - p = 0.$$

Logo, $\sqrt[n]{p}$ é raiz do polinômio $x^n - p = 0$ e, portanto, é algébrico.

(b) Sendo $i = \sqrt{-1}$ um número complexo, portanto não racional, tem-se

$$x = \sqrt{-1} \Rightarrow x^2 = -1.$$

Daí segue que i é solução da equação $x^2 + 1 = 0$, ou seja, é um número algébrico.

Definição 2. Um determinado número algébrico será inteiro algébrico (inteiro sobre $\mathbb{Z}$) se for raiz de um polinômio mônico, ou seja, for raiz de um polinômio onde o coeficiente líder de sua equação polinomial for igual a 1.

Exemplo 3. Vamos mostrar que o número $\sqrt{2+\sqrt{3}} \in \overline{\mathbb{Q}}$ é inteiro algébrico. Se $x = \sqrt{2+\sqrt{3}}$ temos que:

$$x^2 = 2+\sqrt{3} \Rightarrow x^2 - 2 = \sqrt{3} \Rightarrow x^4 - 4x^2 + 4 = 3,$$

ou seja, o número $\sqrt{2+\sqrt{3}}$ é solução da equação $x^4 - 4x^2 + 1 = 0$, que é um polinômio mônico.

Observação. Todo inteiro algébrico é um número algébrico, mas, em geral, a recíproca não é verdadeira.

Exemplo 4. Vamos mostrar que o número $\frac{22}{7}$ é algébrico, mas não é inteiro algébrico. De fato, com $x = \frac{22}{7}$ temos $7x = 22$, e assim é raiz da equação polinomial $7x - 22 = 0$. Suponha que $\frac{22}{7}$ é inteiro algébrico, ou seja, é raiz de um polinômio mônico

$$p(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0.$$

Desta forma temos que:

$$\left(\frac{22}{7}\right)^n + a_{n-1}\left(\frac{22}{7}\right)^{n-1} + \cdots + a_1\left(\frac{22}{7}\right) + a_0 = 0,$$

multiplicando por 7^n, obtemos que

$$22^n + a_{n-1}7 \cdot 22^{n-1} + \cdots + a_1 7^{n-1} \cdot 22 + a_0 7^n = 0,$$

ou ainda,

$$22^n = -a_{n-1}7 \cdot 22^{n-1} - \cdots - a_1 7^{n-1}22 - a_0 7^n$$
$$2^n 11^n = 7(-a_{n-1}22^{n-1} + \cdots + a_1 7^{n-2}22 + a_0 7^{n-1})$$

Portanto, $7|2^n 11^n$ e como 2 e 11 são primos então $7|2$ ou $7|11$ o que é um absurdo. Isto mostra que $\frac{22}{7}$ não é inteiro algébrico.

Definição 3. Seja $\alpha \in \mathbb{R}$, dizemos que α é um número algébrico de grau n, se existe $P(x) \in \mathbb{Q}[x]$ mônico, de menor grau n, que satisfaz $P(\alpha) = 0$.

Exemplo 5.

(a) $\sqrt{2}$ é um número algébrico de grau 2, pois é solução de $x^2 - 2 = 0$;

Suponha que $\sqrt{2}$ é raiz de um polinômio mônico de grau menor que 2, então $\sqrt{2}$ é raiz de um polinômio $p(x) = x - a$ com $a \in \mathbb{Z}$. Desta forma temos que

$$\sqrt{2} - a = 0 \Rightarrow \sqrt{2} = a \in \mathbb{Z},$$

o que é um absurdo.

Teorema 1. Todo número inteiro algébrico (inteiro sobre $\mathbb{Z}$) real ou é um número inteiro ou é um número irracional.

Demonstração. Suponha que $x \in \mathbb{Q}$ é um inteiro algébrico. Seja $x = \frac{p}{q}$ onde $p, q \in \mathbb{Z}$ e $q > 0$ com $(p, q) = 1$. Assim, o mesmo é solução de uma equação do tipo

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0,$$

ou seja,

$$\left(\frac{p}{q}\right)^n + a_{n-1}\left(\frac{p}{q}\right)^{n-1} + \cdots + a_1 \frac{p}{q} + a_0 = 0.$$

Desenvolvendo as potencias, temos que:

$$\frac{p^n}{q^n} + a_{n-1}\frac{p^{n-1}}{q^{n-1}} + \cdots + a_1 \frac{p}{q} + a_0 = 0,$$

multiplicando ambos os lados da equação por q^n, obtemos:

$$p^n + a_{n-1}.p^{n-1}.q + \cdots + a_1.p.q^{n-1} + a_0.q^n = 0.$$

Isolando p^n e colocando q em evidencia, teremos:

$$p^n = q(-a_{n-1}.p^{n-1} - \cdots - a_1.p.q^{n-2} - a_0.q^{n-1}).$$

Fazendo $A = (-a_{n-1}.p^{n-1} - \cdots - a_1.p.q^{n-2} - a_0.q^{n-1})$, temos que $A \in \mathbb{Z}$ e que $p^n = q.A$. Logo, $q|p^n$ e do fato de p ser primo temos que $q|p$, portanto, $q|(p, q) = 1$, o que é uma contradição.

Teorema 2. Para o conjunto dos números algébricos valem as seguintes propriedades:

(i) O simétrico $-a$ de um número algébrico a, é algébrico

(ii) O inverso a^{-1} de um número algébrico a, com a não nulo, é algébrico.

Demonstração. (i) Se a é algébrico, então ele é raiz de uma equação do tipo

$$a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0,$$

portanto $-a$ é raiz da equação:

$$(-1)^n a_n x^n + (-1)^{n-1}a_{n-1}x^{n-1} + \cdots + (-1)a_1 x + a_0 = 0.$$

Isso demonstra a propriedade (i).

(ii) Se a, não nulo, é algébrico, vamos mostrar que a^{-1} é solução de

$$a_0 x^n + a_1 x^{n-1} + \cdots + a_{n-1}x + a_n = 0.$$

Temos que se a, não nulo, satisfaz a equação

$$a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0,$$

então a^{-1} é raiz da equação

$$a_n \frac{1}{x^n} + a_{n-1}\frac{1}{x^{n-1}} + \cdots + a_1 \frac{1}{x} + a_0 = 0.$$

Multiplicando ambos os membros por x^n, tem-se:

$$a_n + a_{n-1}x + \cdots + a_1 x^{n-1} + a_0 x^n = 0.$$

Isso demonstra a propriedade (ii).

Exemplo 6.
(a) Sendo $a = 2$ um número algébrico, solução de

$$x^2 - 4x + 4 = 0,$$

temos, pela propriedade (i) do Teorema 2, que -2 é raiz da equação

$$(-1)^2x^2 - (-1)4x + 4 = 0 \Rightarrow x^2 + 4x + 4 = 0.$$

De fato,

$$(-2)^2 + 4(-2) + 4 = 0.$$

(b) Sendo $a = \sqrt{3}$ um número algébrico, solução de

$$x^4 - 5x^2 + 6 = 0,$$

temos que pela propriedade (ii) do Teorema 2, $(\sqrt{3})^{-1}$ será solução da equação

$$6x^4 - 5x^2 + 1 = 0.$$

De fato,

$$6.\frac{1}{(\sqrt{3})^4} - 5.\frac{1}{(\sqrt{3})^2} + 1 = \frac{6}{9} - \frac{5}{3} + 1 = 0.$$

Definição 4. Uma forma linear com coeficientes racionais é uma expressão da forma:

$$X = q_1x_1 + \cdots + q_nx_n,$$

onde $q_1, \ldots, q_n$ são todos racionais. Os x_i's são chamados indeterminados.

Definição 5. Dadas $n+1$ formas lineares representadas por $X_1, \ldots, X_{n+1}$, elas serão linearmente dependentes se existem $a_1, \ldots, a_n$ com pelo menos um a_i distinto de zero, tais que

$$a_1X_1 + \cdots + a_{n+1}X_{n+1} = 0.$$

Elas serão linearmente independentes se a equação acima admitir apenas a solução trivial, isto é, $a_1 = \cdots = a_{n+1} = 0$.

Lema 1. Dadas $n+1$ formas lineares

$$X_1 = q_{1,1}x_1 + \cdots + q_{n,1}x_n$$
$$\vdots$$
$$X_{n+1} = q_{1,n+1}x_1 + \cdots + q_{n,n+1}x_n$$

elas são linearmente dependentes sobre os racionais.

Demonstração: Se as $n+1$ formas lineares são linearmente dependentes sobre os racionais, então podemos dizer que existem $r_1, \ldots, r_{n+1} \in \mathbb{Q}$, com pelo menos um r_i distinto de zero, tais que

$$r_1X_1 + \cdots + r_{n+1}X_{n+1} = 0.$$

Substituindo os X_i's por suas expressões dadas no enunciado do Lema, vemos que

$$r_1(q_{1,1}x_1 + \cdots + q_{n,1}x_n) + \cdots + r_{n+1}(q_{1,n+1}x_1 + \cdots + q_{n,n+1}x_n) = 0.$$

Colocando $x_1, x_2, \ldots, x_n$ em evidencia, temos que

$$(r_1q_{1,1} + \cdots + r_{n+1}q_{1,n+1})x_1 + \cdots + (r_1q_{n,1} + \cdots + r_{n+1}q_{n,n+1})x_n = 0$$

estará satisfeita se os r_i's forem as soluções do sistema de equações lineares

$$r_1q_{1,1} + r_2q_{1,2} \ldots + r_{n+1}q_{1,n+1} = 0$$
$$\vdots$$
$$r_1q_{2,1} + r_2q_{2,2} + \cdots + r_{n+1}q_{2,n+1} = 0$$
$$r_1q_{n,1} + r_2q_{n,2} + \cdots + r_{n+1}q_{n,n+1} = 0.$$

Colocando no sistema de matrizes, temos

$$\begin{bmatrix} q_{1,1} & q_{1,2} \cdots q_{1,n+1} \\ q_{2,1} & q_{2,2} \cdots q_{2,n+1} \\ \vdots & \vdots & \vdots \\ q_{n,1} & q_{n,2} \cdots q_{n,n+1} \end{bmatrix} \begin{bmatrix} r_1 \\ r_2 \\ \vdots \\ r_{n+1} \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}$$

uma matriz de ordem $nx(n+1)$, ou seja, possui n equações com $n+1$ incógnitas. Logo, temos que o sistema acima possui soluções não nulas.

Teorema 3. Para o conjunto dos números algébricos, valem também as propriedades:
(i) A soma de dois números algébricos é um número algébrico
(ii) O produto de dois números algébricos é um número algébrico.

Demonstração. (i) Sejam a e b algébricos. Logo existem equações polinomiais:

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 = 0 \text{ (1.1)}$$
$$x^n + b_{m-1}x^{n-1} + \cdots + b_1x + a_0 = 0, \text{ (1.2)}$$

com coeficientes racionais (a equação da definição de números algébricos tem coeficientes inteiros, as equações acima são obtidas dividindo-se a equação original pelo coeficiente líder), tais que a seja raiz de (1.1) e b seja raiz de (1.2). De (1.1) obtemos:

$$a^n = -a_{n-1}a^{n-1} - \cdots - a_1a - a_0, \text{ (1.3)},$$

isto é, a^n está expresso como uma combinação linear de $1, a, \ldots, a^{n-1}$, usando coeficientes racionais.

Multiplicando (1.3) por a, tem-se:

$$a^{n+1} = -a_{n-1}a^n - \cdots - a_1a^2 - a_0a.$$

Substituindo o a^n obtido na expressão por seu valor dado em (1.3), temos:

$$a^{n+1} = -a_{n-1}(-a_{n-1}a^{n-1} - \cdots - a_1a - a_0) - a_{n-2}a^{n-1} - \cdots - a_1a^2 - a_0a.$$

Aplicando a distributiva obtemos:

$$a^{n+1} = {a_{n-1}}^2.a^{n-1} + \cdots + a_{n-1}a_1a + a_{n-1}a_0 - a_{n-2}a^{n-1} - \cdots - a_1a^2 - a_0a.$$

Colocando as incógnitas em evidência, temos:

$$a^{n+1} = ({a_{n-1}}^2 - a_{n-2})a^{n-1} + (a_{n-1}a_{n-2} - a_{n-3})a^{n-2} + \cdots + (a_{n-1}a_1 - a_0)a - a_{n-1}a_0.$$

Obtemos assim, a^{n+1} expresso como combinação linear dos mesmos $1, a, \ldots, a^{n-1}$, usando-se também coeficientes racionais. E assim, sucessivamente, todas as potências a^j, para $j \geq n$, são expressos como combinações lineares de $1, a, \ldots, a^{n-1}$ usando-se coeficientes racionais.

De modo análogo, podemos exprimir as potências b^k para $k \geq m$, como combinações de $1, b, \dots, b^{m-1}$, usando-se coeficientes racionais.

Agora vamos mostrar que $a+b$ satisfaz uma equação polinomial de grau $m.n$ com coeficientes racionais, implicando então que $a+b$ seja algébrico. Considere os $m.n+1$ números

$$1, a+b, (a+b)^2, \dots, (a+b)^{m.n}. \quad (1.4)$$

Desenvolvendo as várias potências, e usando o que se viu acima sobre a representação de potências $a^j, j \geq n$, e $b^k, k \geq m$, obtemos que os números em (1.4) podem ser expressos como combinações lineares de $m.n$ números $a^j b^k, 0 \leq j \leq n-1,\ 0 \leq k \leq m-1$, usando-se coeficientes racionais. Agora, aplicamos o Lema 1 acima: os X_i's são os $m.n+1$ números de (1.4), os x_i's são os $m.n$ números de $a^j b^k$. Logo, existem racionais $r_0, r_1, \dots, r_{m.n}$ tais que

$$r_0 + r_1(a+b) + \cdots + r_{m.n}(a+b)^{m.n} = 0,$$

o que mostra que $a+b$ satisfaz uma equação polinomial com coeficientes racionais. Isto demonstra a propriedade (iii).

(ii) Segue as mesmas linhas da demonstração da propriedade (iii). Em (1.4), entretanto, consideramos as potências

$$1, ab, (ab)^2, \dots, (ab)^{m.n}.$$

Isso demonstra a propriedade (ii).

Portanto, estão provadas todas as propriedades descritas neste teorema.

3.2. Enumerabilidade de Conjuntos

Definição 6. Um conjunto X diz-se enumerável quando é finito ou quando existe uma bijeção entre X e o conjunto dos naturais $\mathbb{N}$.

Exemplo 7. O conjunto dos números inteiros é enumerável.

De fato, associando os números naturais aos inteiros na seguinte ordem

0, 1, -1, 2, -2, 3, -3...

Podemos definir a função:

$$f: \mathbb{N} \to \mathbb{Z}$$

$$f(x) \begin{cases} \frac{x}{2} & \text{se } x \text{ é par} \\ -\frac{x-1}{2} & \text{se } x \text{ é ímpar} \end{cases}$$

Agora verificaremos a bijeção da função.

(i) f é injetora, isto é, $\forall\, x_1, x_2 \in N, x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2)$ ou $f(x_1) = f(x_2) \Rightarrow x_1 = x_2$.

- Se x_1 e x_2 são pares, temos que $f(x_1) = \frac{x_1}{2}$ e $f(x_2) = \frac{x_2}{2}$.

Assim, $\frac{x_1}{2} = \frac{x_2}{2} \rightarrow x_1 = x_2$.

- Se x_1 e x_2 são ímpares, temos que $f(x_1) = -\frac{x_1-1}{2}$ e $f(x_2) = -\frac{x_2-1}{2}$.

Assim, $-\frac{x_1-1}{2} = -\frac{x_2-1}{2} \Rightarrow (x_1-1) = -(x_2-1) \Rightarrow x_1 = x_2$.

- Se x_1 é par e x_2 é ímpar, temos que $x_1 \neq x_2$ então $f(x_1) \neq f(x_2)$.

De fato, $\frac{x_1}{2} \neq -\frac{x_2-1}{2}$.

- Se x_1 é ímpar e x_2 é par é análogo ao item anterior.

Portanto, pelos casos descritos acima, f é injetora.

(ii) f é sobrejetora, isto é, dado $y \in \mathbb{Z}, \exists\, x \in \mathbb{N}$ tal que $f(x) = y$.

- Dado $y \in Z$, se $y \geq 0$ definimos $x = 2y$.

Dessa forma, $f(2y) = \frac{2y}{2} = y$. Dado $y \in \mathbb{Z}, \exists\, x = 2y$ tal que $f(2y) = y$.

- Dado $y \in \mathbb{Z}$, se $y < 0$ definimos $x = -2y+1$.

Assim, $f(-2y+1) = -\frac{(-2y+1)-1}{2} = -\frac{(-2y)}{2} = y$. Dado $y \in \mathbb{Z}, \exists\, x = -2y+1$ tal que $f(-2y+1.) = y$.

Dessa forma, por (i) e (ii) temos que f é bijetora. Sendo assim, por definição, o conjunto dos números inteiros é enumerável.

Proposição 1. Se $f: X \to Y$ é injetiva e Y é enumerável, então X é finito ou enumerável.

Como Y é enumerável existe uma bijeção $g: Y \to \mathbb{N}$. Logo, podemos considerar a função composta $h = gof: X \to \mathbb{N}$. Como f e g são injetivas o mesmo ocorre com h, já que a composta de funções injetivas é injetiva. Dessa forma, restringindo o contradomínio de h, temos:

$$h: X \to h(x) \subset \mathbb{N}$$

uma bijeção.

Como $h(x) \subset \mathbb{N}$, ele é finito ou enumerável. Caso for finito, como h é bijetiva, X é finito. Caso for enumerável, temos uma bijeção $h(x) \subset \mathbb{N} \to \mathbb{N}$, logo teremos também uma bijeção de $X \to \mathbb{N}$. Dessa forma, temos que X é finito ou enumerável.

Proposição 2: Seja X enuméravel. Se $f: X \to Y$ é sobrejetiva, então Y é finito ou enumerável.

Como X é enumerável existe a bijeção $g: \mathbb{N} \to X$ e, portanto, a composta $fog: \mathbb{N} \to Y$ é sobrejetiva. Temos então que $(fog)^{-1}: Y \to \mathbb{N}$ é uma relação em que um mesmo y pode ter mais de uma imagem. Logo, definiremos a função $h: Y \to \mathbb{N}$, em que para todo $y \in Y$ teremos $h(y)$ como o menor elemento em $(fog)^{-1}(y)$. Note que h está bem definida, já que todo subconjunto dos naturais possui menor elemento. Ainda, h é

injetiva. Logo pela proposição 1, temos que Y é finito ou enumerável.

Lema 2: Todo número natural se decompõe de maneira única como produto de fatores primos.

Proposição 3: $\mathbb{N} \times \mathbb{N}$ é enumerável.

Definimos

$$f: \mathbb{N} \times \mathbb{N} \to \mathbb{N}$$
$$(n, m) \to 2^n 3^m$$

Temos, pelo lema anterior, que f é injetiva, pois:

$$2^{n_1}3^{m_1} = 2^{n_2}3^{m_2} \Rightarrow (n_1, m_1) = (n_2, m_2).$$

Logo, pela proposição 1, $\mathbb{N} \times \mathbb{N}$ é enumerável.

Proposição 4: Se X e Y são enumeráveis, então $X \times Y$ é enumerável.

Como X e Y são enumeráveis, existem $f: \mathbb{N} \to X$ e $g: \mathbb{N} \to Y$ bijeções. Definimos:

$$h: \mathbb{N} \times \mathbb{N} \to X \times Y$$
$$h(x, y) = (f(x), g(y))$$

Então h é sobrejetiva. Como, pela proposição 3, $\mathbb{N} \times \mathbb{N}$ é enumerável, temos pela proposição 2, que $X \times Y$ é enumerável.

Proposição 5: A reunião enumerável de conjuntos enumerável é enumerável.

Dados $X_1, X_2, \dots, X_n$ conjuntos enumeráveis, existem sobrejeções $f: \mathbb{N} \to X_1, f_2: N \to X_2, \dots, f_n: N \to X_n$. Sendo assim, temos a função sobrejetiva:

$$f_n: \mathbb{N} \to X_n$$
$$m \to f_n(m)$$

Tomando $\mathrm{X} = \bigcup_{n=1}^{\infty} X_n$, definimos a sobrejeção:

$$f: \mathbb{N} \times \mathbb{N} \to \mathrm{X}$$
$$(n, m) \to f_n(m)$$

Dado um x qualquer de X, temos que ele pertence a algum X_n. Como a função $f_n: \mathbb{N} \to X_n$ é sobrejetiva, x é igual a algum $f_n(m)$, portanto está na imagem. Logo $\bigcup_{n=1}^{\infty} X_n$ é enumerável.

3.3. Enumerabilidade do Conjuntos dos Números Algébricos

Proposição 6: Para todo $n \in \mathbb{N}$, existe apenas uma quantidade enumerável de polinômios, em $\mathbb{Z}[x]$, com grau n.

Demonstração: Considerando $X_n = \{Q \in \mathbb{Z}[x]; \partial Q = n\}$, tomaremos $f: \mathbb{Z} \times \dots \times \mathbb{Z} \times \mathbb{Z}^* \to X_n$ dado por

$$f(a_0, a_1, \dots, a_n) = a_0 + a_1 x + \dots + a_n x^n.$$

Notamos facilmente a sobrejeção já que o contradomínio é igual a imagem. Como $\mathbb{Z} \times \dots \times \mathbb{Z} \times \mathbb{Z}^*$ é enumerável, pois o produto cartesiano finito de conjuntos enumeráveis é enumerável, e a função é sobrejetiva, temos pela proposição 2 que X_n é enumerável.

Proposição 7: O conjunto dos números algébricos é enumerável.

Demonstração: Dado $P(x) = a_0 + a_1 x + \dots + a_n x^n$, o conjunto das raízes de P é denotado por R_p. Note que R_p tem no máximo n elementos, logo é um conjunto finito e, portanto, enumerável. Definindo $A_n = \bigcup_{\partial \mathrm{P} = \mathrm{n}} R_p$, como a união enumerável de conjuntos finitos é enumerável segue-se que A_n é enumerável. Agora, basta observar que

$$\overline{\mathbb{Q}} = \bigcup_{n \in \mathbb{N}} A_n.$$

Como, pela proposição 5 a união enumerável de conjuntos enumeráveis é enumerável, temos que $\overline{\mathbb{Q}}$ é enumerável.

4. CONSIDERAÇÕES FINAIS

Foi realizado, neste trabalho, o estudo sobre a Enumerabilidade do Conjunto dos Números Algébricos, abordando a princípio os dois temas separadamente. Ao ser exposto dessa forma, foi possível compreender a importância de ambos para o aprofundamento de estudos em outros campos da matemática, além da percepção de que muitos outros estudos podem ser desenvolvidos nessa área devido as diversas particularidades presentes em suas características.

Ademais, em decorrência da forma em que os temas foram estudados e expostos, se torna visível nos resultados deste trabalho, uma maior facilidade na apresentação da demonstração da Enumerabilidade do Conjunto dos Algébricos, já que para o seu desenvolvimento foram utilizados vários conceitos estudados preliminarmente.

Sendo assim, este trabalho cumpre seu papel na busca pelo aprofundamento dos conceitos do Conjunto dos Números Álgébricos, já que trabalha também sua Enumerabilidade de forma mais abrangente, e pode vir a se tornar um estímulo para a continuação da pesquisa nessa área.

REFERÊNCIAS

BIAZZI, R. N. **Polinômios Irredutíveis: Critérios e Aplicações.** 2014. Dissertação (Mestrado Profissional em Matemática em Rede Nacional) – Universidade Estadual Paulista, Rio Claro, SP, 2014.

GONÇASVES, M. B.; GONÇALVES, D. **Elementos da Análise**. 2.ed. Florianópolis: UFSC, 2012. p. 11-18.

PIO, S. G. **Números transcendentes e a classificação de Mahler com ênfase nos U-números.** 2019. Dissertação (Mestrado em Matemática) – Universidade Federal da Bahia, Salvador, BA, 2019.