PRELIMINARES: MATEMÁTICA & ETC.

Referências Históricas Gerais:

M.Kline-*Mathematical Thought from Ancient to Modern Times*, Oxford UP 1974

J.Stillwell-*History of Mathematics*, Springer

I-INTRODUÇÃO

Os pilares básicos da Matemática Contemporânea são constituídos por quatro conceitos:

1-**Números Naturais** (Grécia Antiga, Hindus, Chineses e Árabes Medievais), de onde vem as Estruturas Numéricas Real e Complexa.

2-**Funções** (Século XVII em diante)

3-**Conjuntos** (Sec.XIX-XX)

4-**Algoritmos** (Grécia Antiga, Al-Kwarizmi)

O Conceito e a Linguagem da Teoria Elementar de Conjuntos é hoje a mais fundamental da Matemática muito embora a sua elaboração precisa e incorporação ao corpo formal da Matemática tenha se iniciado no final do século XIX e se consolidado somente na segunda metade do século XX. (A introdução da Teoria de Conjuntos na Matemática deve-se ao trabalho pessoal de Georg Cantor que experimentou uma resistência inicial tão renhida às suas idéias, que, provavelmente,foi a principal causa da doença mental que lhe vitimou. A sua incorporação à Matemática atual é resultado em grande parte da influencia do grupo Bourbaki- Ref. M.Kline, J.Stillwell).

Exercicio:

1-Descreva em poucas palavras o papel histórico de Georg Cantor no desenvolvimento da Teoria dos Conjuntos.

2-O mesmo para o papel histórico de Nicholas Bourbaki no estabelecimento da Matemática "Moderna".

Em virtude do seu papel fundamental como linguagem e fundamento conceitual da Matemática, uma familiaridade com a Teoria elementar dos Conjuntos torna-se, portanto, indispensável para a formulação e registro de qualquer Tópico da Matemática Contemporânea.

II-CONJUNTOS

O conceito intuitivo de conjunto está associado à idéia de uma coleção de "objetos" (elementos), cada um deles identificável, ou caracterizável, por algum critério bem determinado.

O Conjunto vazio $\emptyset$, que representa o conjunto que não contem *nenhum* elemento, por incrível que pareça, é o mais fundamental de todos.

O outro extremo seria um "Conjunto Universal" que conteria "todos os elementos", mas esta é uma "definição" muito vaga que leva a inconsistências lógicas que não devemos abarcar. Por esta razão, o conjunto "Universo" é definido em cada caso e representa simplesmente um grande conjunto que engloba todos os elementos de interesse. (A idéia de um "Universo" absoluto que abranja todos os elementos leva a dificuldades lógicas desnecessárias para o presente contexto.(Kline,Stilwell)

Operações entre conjuntos

Uma vez definida uma classe de objetos matemáticos, o próximo passo natural no desenvolvimento de uma teoria a respeito dos mesmos consiste em estabelecer um arsenal de relações binárias e operações que podem ser efetuadas entre eles que visam à construção de uns em termos de outros objetos do mesmo tipo. (O sucesso que experimentamos com esta estratégia aplicada aos números naturais tem sido repetido ao longo da história e sempre com igual sucesso). A seguir definiremos algumas operações em conjuntos que são subconjuntos de um Universo que denotaremos por E.

A operação de **União *entre*** dois conjuntos quaisquer é denotada por $A \cup B$ e produz o conjunto que contem exatamente os elementos que comparecem nos dois conjuntos.

A operação de **Intersecção entre** dois conjuntos, denotada por $A \cap B$ produz o conjunto que contem exatamente os elementos que são simultaneamente pertencentes aos dois conjuntos.

A operação de **Complementação** é efetuada **sobre** os subconjuntos do conjunto Universo E , denotada por $A^c = E - A$ e representa o conjunto cujos elementos são exatamente aqueles que ***não pertencem*** a A .

A **operação Produto** $A \times B = C$ entre dois conjuntos A, B produz um conjunto de pares $C = \{(a, b), a \in A, b \in B\}$.

A operação **Exponenciação** entre dois conjuntos $A, \neq \emptyset, B$ é denotado e descrito como o conjunto de funções $A^B = \{f: B \to A\}$.

Exercícios: Obtenha uma expressão para $\#(A \times B\ )$ e $\#A^B$ em que $\#A < \infty,\ e\ \#B < \infty$

Definiremos agora uma operação de "Quociente", ou "Divisão" entre subconjuntos de *E*. Para isto é necessário apresentar uma das idéias mais úteis à construção de objetos matemáticos.

Relação de Equivalência:

Uma das estratégias mais fundamentais da Matemática que possibilita a construção de novos conjuntos é o conceito de **Relação de Equivalência** que poderíamos denominar de "Igualdade fraca" ou "Igualdade parcial".

Uma relação de equivalência " ~" no conjunto C é definida entre pares $(a, b) \in C \times C$ de elementos de C , denotada na forma $a{\sim}b$ se as seguintes propriedades forem satisfeitas:

1- Reflexiva: $a{\sim}a$ para todo $a \in C$
2- Simétrica: Se $a{\sim}b$, então $b{\sim}a$
3- Transitiva: Se $a{\sim}b$, e $b{\sim}c$, então $a{\sim}c$.

Classes de Equivalência:

Um conjunto C em que é definida uma Relação de Equivalência "~" entre seus elementos pode ser *Particionado* em uma família de subconjuntos disjuntos $\{S_\lambda \subset C\}$ de tal forma que cada um deles é constituído de todos os elementos equivalentes entre si, ou seja:

1-$C = \bigcup_\lambda S_\lambda$, **2-** Se $S_\lambda \cap S_\gamma \neq \phi$ então $S_\lambda = S_\gamma$, **3-** Se $a \in S_\lambda$, então $S_\lambda = \{c \in C\ ; c{\sim}a\}$.

Neste caso, cada subconjunto S_λ é denominado de uma **Classe de Equivalencia.**

O Conjunto formado por todas as classes de Equivalência é denominado **Conjunto Quociente** que é denotado pelo símbolo $C/_\sim = \{S_\lambda\}$

A cada elemento $a \in C$ é possível atribuir **uma e única** classe de equivalência que denotaremos por $[a] \in C/\sim$ constituída de todos os elementos de C que são relacionados com o elemento a, ou seja, $[a] = \{b \in C\ ; b \sim a\}$.

Portanto, também é possível definir a função $c: C \to \frac{C}{\sim}, c(a) = [a]$.

Exercicio:

Mostre que cada classe de Equivalência é completamente determinada por algum (qualquer) de seus elementos

Relação de Ordem Parcial-

O conceito de Relação de Ordem Parcial generaliza o conceito de ordem numérica. Uma **Relação de Ordem** entre os elementos de um conjunto X , denotada por " $x \preccurlyeq y$ " é caracterizada pelas seguintes propriedades:

1-$x \preccurlyeq y$ **e** $y \preccurlyeq x$, **se e somente se** $x = y$ (reflexividade)

2-Se $x \preccurlyeq y$ e $y \preccurlyeq z$, então $x \preccurlyeq z$ (transitividade)

Diz-se que uma Ordem $\preccurlyeq$ em X é **Total** se para quaisquer pares $x, y \in X$ tenhamos uma das duas seguintes possibilidades cumpridas: $x \preccurlyeq y$, ou $y \preccurlyeq x$.

Uma Ordem $\prec$ em X se diz **Estrita** se $x \prec y$ implica que $x \neq y$.

O protótipo do conceito de Relação de Ordem Parcial e a mais fundamental é definida pela relação de continência entre subconjuntos de um conjunto universal E e denotada por $A \subset B$ e que significa; " $a \in A \Rightarrow a \in B$".

Obviamente o protótipo da relação de ordem Total é a ordem numérica definida entre os Naturais, $\mathbb{N}$ e herdada sucessivamente por $\mathbb{Z}, \mathbb{Q}, e\ \mathbb{R}$, mas não por $\mathbb{C}$.

Em $\mathbb{R}^n$define-se uma ordem parcial, que provará sua utilidade, da seguinte maneira: $x = (x_1, \dots, x_n) \le y = (y_1, \dots, y_n)$ se $x_k \le y_k$, $1 \le k \le n$.

GLOSSÁRIO:

-Cardinalidade de um Conjunto Finito: *Número de elementos do conjunto*

-Cardinalidade de Conjunto Infinito: *Diz-se que dois conjuntos tem a mesma cardinalidade se existe uma função bijetora entre eles.*

-Cardinalidade Contável/Enumerável- *Diz-se que um conjunto é Contável / Enumerável se existe uma bijeção entre este conjunto e o conjunto de Números Naturais* $\mathbb{N}$

-Partição de um Conjunto *A* **:** *É uma coleção C_λ de* ***1)****-Subconjuntos Disjuntos de A ,(isto é, $C_\lambda \subset A$ e $C_\lambda \cap C_\gamma \neq \emptyset$, implica $C_\lambda = C_\gamma$)* ***2-*** *Cuja união é todo $A = \bigcup_\lambda C_\lambda$.*

-O conjunto das partes de um conjunto C , denotado por $\wp(C)$ é o conjunto de todos os subconjuntos de C , isto é, $\wp(C) = \{A; A \subset C\}$.

Exercícios:

1-Mostre que se #*A*={*Cardinalidade do conjunto finito A*}= "*Números de elementos de A"*, então $\#(A \cup B) = \#A + \#B - \#(A \cap B)$

2-Obtenha uma Fórmula análoga para a cardinalidade da união de três conjuntos finitos A, B, C.

3-Geneneralize o resultado acima para *n* conjuntos finitos $\{A_k\}_{1 \le k \le n}$: $\# \bigcup_{k=1}^{n} A_k$.

4-Mostre que $A \times (B \cup C) = (A \times B) \cup (A \times C)$, onde o sinal " $\times$ " representa o Produto Cartesiano entre dois conjuntos: $A \times B = \{(a, b); a \in A \; e \; b \in B\}$

5-Obtenha uma expressão para $(A \cup B) \times (A \cup B)$

6-Mostre que o termo "Quociente" é justificado quando C for finito e as Classes de Equivalência S_λ tem a mesma cardinalidade, ou seja, neste caso, $\#C = \#\left(C/\sim\right)\#(S_\lambda)$.

7-Mostre que vale a recíproca do Teorema de Partição, ou seja, se um conjunto C é particionado por uma família de subconjuntos disjuntos é possível definir uma Relação de Equivalencia cujas Classes de Equivalencia são exatamente estes subconjuntos.

8-Analise o sentido e as propriedades da operação de diferença entre conjuntos definida na forma: $A - B = A \cap B^c$ e a operação de ***diferença simétrica***

$A \ominus B = A - B \cup B - A$ e se forem conjuntos finitos obtenha uma expressão para $\#(A - B)$.

9-Obtenha expressões para $\#\wp(C)$ e $\#(A^B)$ para conjuntos finitos A, B, C.

Um conjunto é **finito** se for isomorfo a algum conjunto de números naturais $I_n = \{1,2, \dots, n\}$.

Mostre que não é possível que um conjunto não nulo seja isomorfo a conjuntos $I_n = \{1,2, \dots, n\}$ distintos. Por esta razão é possível definir sem ambigüidade a função cardinalidade para conjuntos finitos.

Observação: O estudo da função "cardinalidade", denotada por " # " com domínio em Partes de um conjunto finito E e com valores naturais, $\#: \wp(E) \to \mathbb{N}$, é o tema fundamental da importante área matemática denominada "Combinatória" **.**

REFERÊNCIA:

Os elementos básicos desta Teoria podem ser encontrados e bem expostos na referencia "baliza":

G.Birkhoff-S.McLane-*Álgebra Moderna*, (edições em todas línguas)

-

III-FUNÇÕES

O Conceito geral de função é intuitivamente representado pela idéia de ***associação*** entre objetos de dois conjuntos.

A sua incorporação formal à Matemática foi um longo processo que se iniciou com R.Dedekind (Sec.XIX) embora Isaac Newton (sec.XVII-XVII) já a tenha utilizado em um sentido específico no contexto do Cálculo Diferencial e Integral.

A caracterização de uma Função f como ***objeto matemático*** (e não como uma mera regra de associação) exige o estabelecimento de

Três Ingredientes: $f \equiv \{A, B, \to\}$

em que A e B são conjuntos não vazios e a seta $\rightarrow$ representa uma maneira (não necessariamente especificada) que a **cada** elemento $a \in A$ se faz corresponder um **único** elemento de B que será denotado por $b = f(a)$.

O conjunto $\boldsymbol{A}$ é denominado **Domínio** da função e $\boldsymbol{B}$ é denominado seu **Contradomínio** (ou conjunto de chegada).

Freqüentemente o próprio símbolo que representa a função f é utilizado para designar a "regra de associação" entre os elementos dos dois conjuntos. E, vice-versa, freqüentemente uma regra de associação é utilizada para representar uma função deixando apenas implícito os seus domínio e contradomínio. (Por exemplo, quem nunca ouviu referencia à "função x^2" , ou `função $\sqrt{x}$?)

A notação matemática para uma função f expõe os seus ingredientes na seguinte forma esquemática visualmente sugestiva:

$$f: A \xrightarrow[a \ \mapsto \ b]{} B$$

-Imagem de um conjunto:

Se $A_0 \subset A$ então, define-se imagem de A_0 pela função o conjunto $f(a_0) = \{f(a); a \in A_0\}$.

Imagem inversa de Elemento ou conjunto-Índice

Se $B_0 \subset B$ então, define-se imagem inversa de B_0 pela função $f: A \rightarrow B$ o conjunto denotado e definido por: $f^{-1}(B_0) = \{a \in A;\ f(a) \in B_0\}$.

Se $b \in B$ então, define-se imagem inversa de b pela função $f: A \rightarrow B$ o conjunto denotado e definido por: $f^{-1}(b) = \{a \in A;\ f(a) = b\}$.

Se o conjunto A for finito, define-se e denota-se índice de um elemento $b \in B$ pela função $f: A \rightarrow B$ ao número : $Ind_f\{b\} = \#\{f^{-1}(b)\} = \#\{a \in A;\ f(a) = b\}$.

Observações:

1-A **Existencia** de uma correspondência sem ambigüidade que associa cada elemento $a \in A$ ao seu respectivo valor $b \in B$ deve ser ressaltada como essencial ao conceito de função. Os detalhes da sua "implementação prática" não são parte deste ingrediente, apenas a sua existência.

Obviamente esta correspondência constitui o núcleo da idéia de função, mas sozinha ela não caracteriza o objeto matemático "função"; para isto são necessários os três ingredientes.

2-Portanto, como uma função é constituída de **três ingredientes**, a modificação de qualquer um deles, implica na modificação do objeto matemático. Assim, por exemplo, as **funções** abaixo **são distintas**:

a- $f: \mathbb{R} \to \mathbb{R},\ x \to f(x) = x^2$
b- $f: \mathbb{R} \to \mathbb{C},\ x \to f(x) = x^2$
c- $f: \mathbb{R}^{+} \to \mathbb{R},\ x \to f(x) = x^2$

3-A regra "prática" de associação entre elementos de domínios e contradomínios numéricos pode ser determinada por **1**) Um algoritmo finito que utiliza uma seqüência bem determinada de operações aritméticas (Isto é, uma Fórmula elementar algébrica),ou **2**) Um algoritmo infinito ($f(x) = cosx = \sum_{k=0}^{\infty} \frac{(-1)^k}{(2k)!} x^k$), ou **3**) A solução de uma equação (por exemplo, $f(x) = \sqrt{x}$) , que é, eventualmente, descrita também por um algoritmo infinito (por exemplo, o Método de Newton), e **4**) Também por diversas outras formas "exóticas" que não admitem ser representadas por algoritmos enumeráveis em que cada passo é resultado de uma operação aritmética. (Por exemplo, $f(x) = 1$ se x for racional e $f(x) = 0$ se x for irracional).

4-O conceito de **algoritmo** é estreitamente ligado ao conceito de função, pois na maioria das vezes é por meio de um algoritmo (em um sentido lato) que se representa o procedimento sistemático que relaciona elementos de A a elementos de B. Os algoritmos podem ser finitos (caso em que é descrito por "Fórmulas" elementares) ou infinito enumerável, caso em que o processo de construção é infinito e definido por convergência. O que caracteriza a classe de Algoritmos são as operações admissíveis em cada passo elementar. (Ref. Donald E. Knuth).

Operações com Funções:

Uma vez definida uma classe de objetos (no presente caso, as *funções*), o próximo passo natural na construção de uma estrutura Matemática nesta classe é determinar operações que possam ser efetuadas entre e sobre estes objetos que permitam construir novos elementos da mesma classe.

Uma das finalidades deste procedimento matemático geral é possibilitar a representação/construção de todos os objetos da classe como resultado da aplicação de seqüências sistemáticas destas operações a algum subconjunto restrito de elementos "básicos" que são apropriadamente escolhidos pela sua simplicidade.

Esta estratégia construtiva é a essência do Método Matemático, que foi introduzido com a invenção dos Números inteiros $\mathbb{N}$ em que cada elemento pode ser descrito sistematicamente por intermédio de uma seqüência finita e bem determinada de **somas** e **produtos**, de apenas dois elementos $\{0,1\}$ na representação binária, ou, como é mais usual, na representação decimal que utiliza os dez dígitos sugeridos pela anatomia digital humana: {0,1,2 ....9}. Este mesmo procedimento foi mais tarde estendido para a construção-representação do conjunto de números reais, caso em que são admitidas seqüências infinitas de somas.

-Operação de SOMA em $\mathcal{F}(A,\mathbb{R}) = \{f: A \to \mathbb{R}\}$.

Se $f, g \in \mathcal{F}(A,\mathbb{R})$, então define-se a **função soma** $h \in \mathcal{F}(A,\mathbb{R})$ de $f\ e\ g$, denotada por $h = f + g$ à função $h: A \to \mathbb{R}$, $tal\ que\ \ h(a) = f(a) + g(a)$.

Exercicio: Mostre que esta operação é bem definida , isto é, produz o que promete: é comutativa, associativa,e tem elemento neutro (a função nula)-.

-Operação PRODUTO em $\mathcal{F}(A,\mathbb{R}) = \{f: A \to \mathbb{R}\}$.

Se $f, g \in \mathcal{F}(A,\mathbb{R})$, então define-se a **função produto** $k \in \mathcal{F}(A,\mathbb{R})$ de duas funções $f\ e\ g$ denotada por $k = fg$ à função , $k: A \to \mathbb{R}$, $k(a) = f(a)g(a)$.

Exercicio: Mostre que esta operação é bem definida (isto é, produz o que promete), é comutativa, associativa, tem elemento neutro –a função constante com valor unitário- e é distributiva com relação à soma.

As duas operações definidas acima (soma e produto) são naturais e "*herdadas*" das operações correspondentes dos elementos do contradomínio (real) do conjunto de funções.

A próxima operação a ser definida, denominada **composição** entre funções, é **intrínseca** ao caráter específico destes objetos, e não depende de propriedades algébricas do domínio ou do contradomínio das funções. A operação de composição é fundamental para o estudo de funções, pois com ela é possível formular e analisar a classe mais importante de problemas da Matemática: ***As equações***.

Operação de COMPOSIÇÃO

Sejam $\mathcal{F}(A, B_0)$ e $\mathcal{F}(B, C)$ dois conjuntos de funções e suponha que $B_0 \subset B$. Assim, se $f \in \mathcal{F}(A, B_0)$,a imagem do domínio de f está contido no domínio de qualquer $g \in \mathcal{F}(B, C)$, isto é, $f(A) \subset B$ e, portanto é possível calcular $g(f(a))$ para qualquer $a \in A$.

Neste cenário, para todo par de funções $f \in \mathcal{F}(A, B_0)$ e $g \in \mathcal{F}(B, C)$ é possível definir entre elas uma operação denominada **Composição** que produz uma nova função $h \in \mathcal{F}(A, C)$, denotada por $h = g \circ f$, tal que $h(a) = g(f(a))$ para todo $a \in A$.

O esquema abaixo ilustra visualmente este cenário:

$$h: A \xrightarrow[A \xrightarrow{f} B_0 \subset B \xrightarrow{g} C]{} C$$

Observe-se que a composição $g \circ f$ entre duas funções somente é possível se a função à esquerda tem domínio que engloba o contradomínio da função à esquerda e, portanto, há uma ordem bem determinada para esta operação.

No conjunto de funções $\mathcal{F}(A, A)$, dadas duas funções quaisquer $f, g \in \mathcal{F}(A, A)$ é sempre possível definir as composições $f \circ g$ e $g \circ f$, mas, mesmo assim *em geral*, a operação de composição não é comutativa, ou seja pode produzir resultados distintos nas duas ordens de aplicação.

1-Função Injetiva (injetora): Uma função $f \in \mathcal{F}(A, B)$ é dita injetora se cada valor de f é atingido única vez, ou seja, se $f(a_1) = f(a_2)$ implica que $a_1 = a_2$.

2-Função Sobrejetiva(Sobrejetora): Uma função $f \in \mathcal{F}(A, B)$ é dita Sobrejetora todos os valores $b \in B$ são atingidos pela menos uma vez, ou seja, se para qualquer $b \in B$ existe algum $a \in A$ tal que $f(a) = b$. Em outros termos, se $f(A) = B$.

3-Função Inversa à Direita: Se $f \in \mathcal{F}(A, B)$ então diz-se que uma função $g \in \mathcal{F}(B, A)$ é sua inversa à direita se $f \circ g \in \mathcal{F}(B, B)$ é tal que $f \circ g = i_d$, ou seja, se $f\big(g(b)\big) = b$ para todo $b \in B$.

4-Função Inversa à Esquerda: Se $f \in \mathcal{F}(A, B)$ então diz-se que uma função $h \in \mathcal{F}(B, A)$ é sua inversa à Esquerda se $h \circ f \in \mathcal{F}(A, A)$ é tal que $g \circ f = i_d$, ou seja, se $h\big(f(a)\big) = a$ para todo $a \in A$.

5-Função Inversa: Se $f \in \mathcal{F}(A, B)$ então diz-se que uma função $h \in \mathcal{F}(B, A)$ é sua Inversa se for sua inversa à Esquerda **e** à Direita. Neste caso, denomina-se esta única função inversa pela notação $h = f^{-1} \in \mathcal{F}(B, A)$.

Exercicios:

-Mostre que uma função tem inversa à Direita *se e somente se* for Sobrejetiva e que, em geral, tem várias inversas à direita.Analise esta situação.

-Mostre que uma função tem inversa à Esquerda se e somente se for injetiva e que, em geral, tem várias inversas à esquerda. Analise esta situação.

-Mostre que uma Função tem inversa se e somente se for Bijetiva, isto é, injetiva e sobrejetiva e, neste caso, ela é única.

-Mostre que uma Equação $f(x) = b$ admite alguma solução x para todo $b \in B$ se e somente se a função f for sobrejetiva. Mostre que e a solução é sempre única (caso exista) se e somente se a função f for injetiva.

-Mostre que se existir uma função bijetora $f: \{1, \dots, n\} \to \{1, \dots, m\}$, então $m = n$.

Isomorfismos, Mudança de Variáveis e Regularização

Funções bijetoras φ entre dois conjuntos $\varphi: Y \to X$ são tão importantes que merecem várias outras formas de designação, cada uma delas enfatizando um aspecto.

Diz-se que uma função bijetora φ é um ***Isomorfismo*** entre os conjuntos $X\ e\ Y$ (também denotada por uma seta dupla $\varphi: Y \leftrightarrow X$), pois identifica completamente e sem ambigüidade os elementos de um conjunto em termos dos elementos de outro.

Por este motivo também denominamos estas funções de ***Mapeamento.***

Também, podemos interpretar estes isomorfismos como "**Mudança de Variáveis**" pois qualquer função $f: X \to Z, x \longmapsto f(x) = z$ pode ser representada inequivocamente pela função $F: Y \longrightarrow Z, y \mapsto F(y) = z$ em que $F(y) = f \circ \varphi(y) = f(\varphi(y))$, que, por abuso de notação escrevemos $f(y)$.

Uma função Bijetora pode ser considerada uma "função perfeita", pois apresentam uma perfeita associação entre elementos de dois conjuntos. Por este motivo, é importante analisar meios de "regularizar" uma função de forma a torná-la "perfeita".

Funções Injetivas também podem ser consideradas perfeitas no sentido de não "confundirem" os elementos de seu domínio. Basta restringir o seu contradomínio à imagem do domínio e teremos uma bijeção perfeita.

O método mais imediato para regularizar uma função $f: A \to B$ não injetiva é a definição de uma relação de equivalência no seu domínio, fazendo $a_1 \sim a_2$ se $f(a_1) = f(a_2)$. Com isto, definimos uma nova função $\tilde{f}: A/\sim \to B, \tilde{f}([a]) = f(a)$ que a torna injetora.

Exercicio:

Determine uma forma para "regularizar" a função argumento: $Arg: \mathbb{C} - \{0\} \to \mathbb{R}, Arg(re^{i\theta}) = \theta$ tomando o domínio $S = \frac{\mathbb{C}-\{0\}}{\sim}$ e identificando-o com um objeto geométrico no espaço tridimensional.

Resolução de Equações: Funções *Inversa, Inversa à Direita e Inversa à Esquerda*

Problemas da forma: "*Dada* $F: X \longrightarrow Y$*, então para cada* $y \in Y$ *obter os elementos* $x \in X$ *tais que* $F(x) = y$ " , onde X é um conjunto de objetos matemáticos (números, vetores, matrizes, funções numéricas e etc), são as questões mais fundamentais da Matemática e de suas diversas Aplicações.

Obviamente, um problema desta natureza depende muito especificamente do conjunto de ***incógnita*** X , da ***operação*** F e do ***contradomínio*** Y , ou seja da função que o define.

Apesar da generalidade desta formulação, é possível estabelecer alguns conceitos e cenários gerais que são úteis na sistematização de seu tratamento matemático.

Se a função for sobrejetora a equação sempre terá ***pelo menos uma*** solução e se for injetora terá ***no máximo*** uma solução.

Exercício:

Mostre que a equação *que* $F(x) = y$ tem alguma solução $x \in X$ qualquer que seja o elemento $y \in Y$ se e somente se a função $F: X \longrightarrow Y$ for sobrejetora e, neste caso, mostre que uma função inversa à direita $G: Y \longrightarrow X$ produz uma solução $x = G(y)$ para qualquer equação $F(x) = y$, mas não necessariamente tôdas as soluções.

As funções bijetivas são importantes na solução de equações, pois garantem sempre a *existencia* e *unicidade* de soluções para estas equações.

A inversão de funções é uma questão intimamente ligada à obtenção de soluções de equações.

Exercício:

1-Mostre que a função $\tilde{f}$ definida acima é bem definida, ou seja, o seu valor associado a cada classe de equivalência $\tilde{f}(s)$ independe do elemento representante $a \in s$ escolhido nesta classe para calcular $\tilde{f}(s) = f(a)$.

2-Mostre que se f for injetiva então a sua regularizada $\tilde{f}$é, essencialmente, ela mesma pois A e $\tilde{A}$ são, essencialmente, os mesmos.

3-Mostre que vale a composição $\tilde{f} \circ c = f$, onde : $c: A \to \frac{A}{\sim}, c(a) = [a]$, ou seja, o procedimento é simplesmente uma "mudança de variável".

Índice de um elemento do contradomínio- Se $f \in \mathcal{F}(A, B)$, então $\#f^{-1}\{b\} = \#\{conjunto\ de\ soluções\ x \in A\ da\ equação\ f(x) = b\} \in \mathbb{N}$ é denominado índice de b com respeito à função f.

IV-CÁLCULO

Obviamente as funções mais importantes da Matemática são aquelas que tem domínio e contradominio definidos por ***conjuntos numéricos. Nesta classe*** estão incluídas os seguintes exemplos:

-Funções de variável inteira e valores complexos $\mathcal{F}(\mathbb{N}, \mathbb{C})$ que são interpretáveis como seqüências de números complexos.

-Funções de uma variável e um valor real, $f: \mathbb{R} \to \mathbb{R}$, e admitindo k derivadas contínuas, $f \in C^k(\mathbb{R}, \mathbb{R})$ do Cálculo Elementar interpretáveis Geometricamente por uma curva na forma de um gráfico cartesiano.

Exercício:

Mostre como uma função $f: \mathbb{R} \to \mathbb{R}$ pode ser "regularizada" como injetiva utilizando para isto um novo domínio real "fatiado" ou um domínio real com dobras".
Exemplifique este procedimento com a função definida pela relação $f(x) = x^2$.
(Sugestão: Utilize o gráfico cartesiano 2D desta função e identifique os ramos da parábola como a reta real)

- Funções de uma variável e vários valores reais, $f: \mathbb{R} \to \mathbb{R}^m$, $f(t) = (f_1(t), \dots, f_m(t))$ do Cálculo Elementar e Geometria Analítica, especialmente aquelas que admitem k derivadas contínuas, $f_j \in C^k(\mathbb{R}, \mathbb{R})$. Para o caso $n = 2{,}3$ estas funções são Geometricamente interpretáveis como uma curva parametrizada ou como a reta real deformada. Cinematicamente é possível interpretá-las também como trajetórias no espaço que admitem uma tangente (velocidade instantânea) bem definida em cada ponto.

-Funções de $\boldsymbol{n}$ variáveis e $\boldsymbol{n}$ valores reais, $F: \mathbb{R}^n \to \mathbb{R}^n$, $F(x_1, \dots., x_n) = \left(f_1(x_1, \dots., x_n), \dots., f_n(x_1, \dots., x_n)\right)$, especialmente aquelas que admitem *k* derivadas parciais contínuas, isto é, $f_j \in C^k(\mathbb{R}^n, \mathbb{R})$.

No caso $n = 2{,}3$ estas funções são interpretáveis como um **Mapeamento** de um domínio "regularizado" como sendo o plano, em geral, com *dobras*.

Geometricamente, ou **Elasticamente**, estas funções podem ser interpretadas como uma deformação em que o ponto x do espaço é ***deslocado*** para a posição $y = x + f(x)$ no mesmo espaço.

Dinamicamente a função f pode ser interpretada como um Campo Vetorial em um Meio Contínuo em que x é interpretado como um ponto do espaço e $f(x)$ um vetor ***velocidade*** deste ponto que define suas linhas de fluxo.

-Funções de $\boldsymbol{n}$ variáveis e de valores reais e valor real $f: \mathbb{R}^n \to \mathbb{R}$, $f(x_1, \dots., x_n)$. Para $n = 2{,}3$ a função pode ser interpretada como um campo escalar (temperatura, altura topográfica do terreno e etc.) em que x representa um ponto do espaço. No caso particular em que $n = 2$, a função pode ser geometricamente interpretada como uma superfície no espaço tridimensional representada pelo gráfico $x_3 = f(x_1, x_2)$.

-Funções gerais de $\boldsymbol{n}$ variáveis e $\boldsymbol{m}$ valores reais,
$F: \mathbb{R}^n \to \mathbb{R}^m$, $F(x_1, \dots., x_n) = \left(f_1(x_1, \dots., x_n), \dots., f_m(x_1, \dots., x_n)\right)$ são utilizadas para representar a dependência de várias medidas f_k em termos de vários parâmetros x_k. A interpretação geométrica e sua representação espacial é, em geral impossível no caso de dimensões superiores ($n, m > 3$), pois extrapolam a nossa cognição espacial. Entretanto, a familiaridade adquirida com espaços ambientes plano e tridimensional são de grande ajuda e mesmo indispensáveis no desenvolvimento da intuição para situações gerais em que o "*vôo deve ser completamente realizado com instrumentos"matemáticos*)".

FUNÇÕES LINEARES: ***Algébricas de Primeiro grau Homogêneas***

A Álgebra Linear trata da classe mais simples de funções de múltiplas variáveis e valores numéricos, $L: \mathbb{R}^n \longrightarrow \mathbb{R}$ que são determinados explicitamente por uma ***Fórmula homogênea*** de ***primeiro grau*** nas variáveis, ou seja,

$$f(x_1, \ldots., x_n) = a_1 x_1 + \cdots. + a_n x_n$$

onde a_k são números reais (ou complexos) fixos.

O termo "***homogênea***" significa que a Fórmula aritmética para o seu cálculo contem apenas termos de primeiro grau de potencia das variáveis x_k na expressão e não comparecem produtos ou potencias menores(constantes) ou maiores do que a unidade.

Excetuando as triviais funções constantes, esta é a classe de funções mais simples sob ponto de vista computacional.

Não se deve iludir com sua simplicidade, todavia. pois o seu emprego como aproximação local de funções gerais é suficiente para fundamentar o desenvolvimento de nada mais do que o Cálculo Diferencial e Integral.

O Teorema de Leibniz citado abaixo se constitui na base conceitual do Cálculo Diferencial de funções de várias variáveis:

Teorema de Leibniz-Jacobi:

Se a função real de várias variáveis, isto é, $F: \mathbb{R}^n \to \mathbb{R}, F(x)$, possui derivadas parciais continuas $\frac{\partial F}{\partial x_k}(x)$ nas vizinhanças do ponto x^0,

Então ***existe*** *uma* ***única*** Aproximação **Linear** com erro menor do que **Primeira Ordem** local em torno de x^0 de seu domínio, isto é, existe uma função linear $Ah = a_1 h_1 + \cdots + a_n h_n$ de tal forma que :

$$F(x + h) = Ah + \|h\| \, \varepsilon(h)$$

Em que a função $\varepsilon(h)$ tem limite nulo para $h \to 0$.

A função linear A é **única** e pode ser calculada em termos de derivadas *unidimensionais* (parciais) na forma $A_k = \frac{\partial F}{\partial x_k}(x^0)$. Na literatura clássica esta Função linear é denotada das seguintes maneiras: Gradiente de $f = GradF(x^0) = \nabla F(x^0) = \frac{\partial F}{\partial x}(x^0) = F^{/}(x^0)$).

xxxxxxxx

Observações:

1-O Teorema acima é uma generalização *possível* do conceito de derivada Newtoniana que é definida para funções de variável real , $f: \mathbb{R} \to \mathbb{R}$ como o *limite da razão* $\lim_{h\to 0} \frac{f(x^0+h)-f(x^0)}{h} = A$. Esta afirmação limite, é equivalente à uma expressão funcional da forma : $f(x^0 + h) = f(x^0) + Ah + o(h)$ que é exatamente a formulação de derivada linear para dimensão 1. Esta última era a formulação de derivada preferida por G.Leibniz (que foi o outro inventor do Cálculo), que enfatiza o conceito de ***aproximação local*** (isto é, nas vizinhanças $x = x^0 + h$ de um ponto base x^0) em lugar de limites. Ou seja, o foco é na *reta tangente* em lugar do ângulo de inclinação da curva que foi a preferida por Newton.

Assim, como a razão Newtoniana $\frac{f(x^0+h)-f(x^0)}{h}$ ***não tem sentido*** para

$h \in \mathbb{R}^n, n > 1$, (e, portanto, não pode ser estendida para variáveis múltiplas*) a generalização da poderosa idéia de derivada*, e de todo o Cálculo Diferencial, somente é possível por intermédio da formulação Leibniziana em que $Ah = A(x - x^0)$ passa a ser interpretada como uma função de *primeiro grau* (polinômio de primeiro grau em h_k), isto é, uma função linear.

Exercicio:

1-Vefique a equivalência entre a formulação de Newton e Leibniz para funções reais de variável real. (À propósito, houve uma disputa ideológica pouco elegante em torno desta e de questões correlatas entre partidários de um e de outro lado do canal da Mancha. Ref. A.Ruppert-Hall-*Philosophers at War*, Cambridge UPress).

2-Mostre que, existindo, a derivada de Jacobi-Leibniz é única.

2-A Demonstração deste Teorema (e muitos outros da área) pode ser encontrada na referencia P.Lax-Caculus, vol II).

3-Um *erro funcional de primeira ordem em* h é alguma função limitada por um multiplo fixo de $\|h\|$.

Um *erro funcional de ordem menor do que* $\|h\|$ (genericamente denotado pelo símbolo $o(h)$) é da forma

$$o(h) = \|h\| \, \varepsilon(h)$$

onde $\varepsilon(h) \to 0$ se aproxima de zero. Portanto, a idéia é de que uma função $o(h)$ se aproxima mais rápido de zero do que a perturbação h.

3-O mesmo conceito de derivada vale para funções de várias variáveis e valores múltiplos (que são simplesmente uma coluna de m funções do tipo acima) $F: \mathbb{R}^n \to \mathbb{R}^m$;basta repetir o enunciado acima para cada coordenada do contradomínio e coleciona-las apropriadamente em uma coluna.

Assim, no caso de uma função com n variáveis e m valores reais, $F: \mathbb{R}^n \to \mathbb{R}^m$, a aproximação linear é da forma $A: \mathbb{R}^n \to \mathbb{R}^m, Ax = (A_1x, \dots, A_mx)$, ou seja, $A_kx = \sum_{j=1}^{n} a_{kj}x_j$ em que , $a_{kj} = \frac{\partial F_k}{\partial x_j}(x^0)$, é representada por uma Matriz. (Denominada ***Jacobiana*** em alguns textos).

Referencias:

P.D.Lax-M.Terrell-*Caluclus, vol II*, Springer

W.Castro Ferreira Jr.- *Notas de Cálculo, pp*

VI-GEOMETRIA EUCLIDEANA- *Deslocamentos & Rotação e sua Álgebra*

Referência:

W. Castro Ferreira Jr.-*Fundamentos Geométricos("Omográficos")da Álgebra Linear, pp*

VII-MÉTODO DE GAUSS :*Algoritmo Aritmético Finito para a Resolução de Sistemas de Equações Lineares*

Este é um Tema abordado em Cálculo Numérico.

Referencias:

J.M.Martínez –*Geometria Analítica* -IMECC-Arquivo Escolar online

G.Strang-*Introduction to Linear Algebra*, Wellesley, 5th edition

L.Trefethen-D.Bau-*Numerical Linear Algebra*, SIAM

VIII-NÚMEROS

"Os Números naturais são uma dádiva divina original, perfeita; as outras estruturas construídas a partir deles são meras ilusões humanas".)parafraseando Leopold Kronecker-sec.XIX)

O conceito de Número natural {1,2,..n..} é considerado um dos mais antigos e universais tendo sua origem em procedimentos de contagem e ordenação tão comuns e necessários que até mesmo alguns animais os utilizam. Todavia, o conceito abstrato de conjunto ***infinito*** dos Números naturais $\mathbb{N} = \{0,1,2, \ldots.\}$e sua estrutura algébrica dotada da operação de ***soma*** se constitui em um enorme salto posterior que somente se incorporou ao conhecimento humano há poucos séculos. As estruturas mais importantes da Matemática contemporânea estão fundamentadas na estrutura de Números Naturais, inclusive as estruturas de números inteiros, racionais, reais e complexos que somente foram elucidadas ao final do século XIX. (H.Thurston-The Number Systems, Dover).

A introdução do conceito de número zero e a representação decimal dos números naturais originada na Índia e propagada pelos árabes por volta do século 7 foi o marco inicial do desenvolvimento da Matemática contemporânea. O conceito de algoritmo atribuído ao matemático Al-Kwarizmi (Bagdad, sec. VIII) está completamente baseado no conceito de conjunto (ordenado) de Números Naturais e mais tarde deu origem ao conceito de limite e de números reais.

A representação decimal foi um marco revolucionário na Matemática pois facilita a manipulação aritmética com os números naturais e propiciou a sua extensão para o conceito de número real.

O aspecto mais importante da representação decimal é a sistematização de um algoritmo que produz uma nomeação de todos os números a partir de um conjunto finito de números {0,1,..,9} e das próprias operações aritméticas. Para quem sempre foi acostumado ao uso dos números nesta forma é difícil imaginar o enorme alcance desta idéia. Naturalmente a base decimal tem origem anatômica e não tem qualquer importância intrínseca. Neste caso, a representação mais fundamental para os números é a binária que faz uso dos dígitos {0,1} e, analogamente, com a utilização das operações aritméticas nomeia (longamente) todos os números reais. Esta é a base utilizada em computadores e tem várias vantagens em outros contextos.

Exercicio:

Descreva a representação binária para os números cujas representações decimais são: $a = 17$, $b = 3{,}14$ e descreva o algoritmo de soma e multiplicação para a obtenção dos números $a + b$ e ab também na representação binária (sem passar pela representação decimal). Faça o mesmo utilizando a base vigesimal dos Maias utilizando as letras do alfabeto para designar os números da base.

Os astrônomos Maias utilizavam a representação vigesimal com base de 20 números e os Assírios utilizavam a bas sexagesimal, com 60 números. Imaginem a "tabuada" que teriam de aprender!

A idéia de representação dos elementos de todo um grande conjunto (infinito) fazendo uso de um pequeno subconjunto dele (chamado de ***base***, ***geradores*** e etc) e as suas operações algébricas intrínsecas é uma estratégia universal da Matemática e especialmente relevante para a estrutura de Espaço Vetorial.

Para o estudo do conceito e história dos Números naturais e reais consulte a bibliografia:

G.Birkhoff-S.MacLane-*Álgebra Moderna,*

H.Thurston-*The Number Systems*, Dover

H.Ebbinbghaus&al.-*Numbers*, Springer Verlag

S.Dehaene-*The Number Sense,*1996

A.Nieder-*A Brain for Numbers-The Biology of Number Instinct*, MIT Press 2020

J.C.Stillwell-*The Mathematics from Euclid to Goedel*, Princeton UP 2016

VIIIB-NÚMEROS COMPLEXOS:

Representações Geométrica, Cartesiana e Matricial

Referências:

G.Birkhoff-S.MacLane-*Álgebra Moderna,*

F.Remmert-*Functions of a Complex Variable*, Springer Verlag

W.Castro Ferreira Jr.-*A Desmistificação dos Números Complexos, PP-*

IX-POLINÔMIOS

Referências:

G.Birkhoff-S.MacLane-*Álgebra Moderna,*

W.Castro Ferreira Jr.- *Notas de Análise Complexa*

X-GRUPOS

A estrutura de Grupo é uma simples estrutura matemática que diz respeito a uma operação binária entre elementos de um conjunto e comparece em inúmeras situações tanto na Matemática quanto em suas aplicações. A quantidade de resultados que é possível obter para esta pequena estrutura é uma das razões de sua importância.

Um Grupo é uma Estrutura Matemática descrita por ***três ingredientes*** $\{G,*,e\}$, *sendo*

1) Um Conjunto G,

2)Uma operação binária definida entre quaisquer pares $(a,b) \in G \times G$ de seus elementos, denominada **produto,** $a * b = c \in G$ (comumente exclui-se o símbolo " $*$ " na operação produto) e

3)Um elemento denominado unidade e denotado por ***e*** **,** *satisfazendo as seguinte propriedades:*

Para todos os elementos $a, b, c \in G$

1-Associatividade: $a(bc) = (ab)c$

2-Elemento neutro: $ae = ea = a$

3-Existencia de elemento inverso*: para todo elemento $a \in G$ existe um elemento $h \in G$ tal que $ah = ha = e$*

Se a comutatividade *do produto também for verificada, isto é,*

4*-$ab = ba$*

Então o Grupo é denominado **Comutativo** *(ou Abeliano)*

Observações:

1-O elemento inverso é único e, portanto, é razoável denotá-lo por a^{-1}.

Exercicios:

1-Demonstre que o elemento inverso é único e que a função $R: G \to G, R(a) = a^{-1}$ é bem definida e bijetiva.

2-Mostre que $(ab)^{-1} = (b^{-1})(a^{-1})$ e que $(a \cdot b \cdots c)^{-1} = (c^{-1}) \cdots (b^{-1})(a^{-1}) \cdot$

3-Mostre que o $\mathbb{R}^2 - (0,0)$ com o produto $.(a,b)(x,y) = (ax - by, ay + bx)$... é um grupo.

4-Mostre que $\{\mathbb{R}, +, 0\}$ e $\{\mathbb{R}^{++}, \cdot, 0\}$ são Grupos.

Isomorfismo

Dados dois Grupos $\{G, \circ, e\}$ e $\{H, *, \varepsilon\}$, se existir uma função *bijetiva* $\varphi: G \to H$, que é "consistente" com as duas operações de produto, isto é,

$$\varphi(ab) = \varphi(a)\varphi(b)$$

então diz-se que φ é um ***isomorfismo entre os dois Grupos***. Podemos interpreta-la com um "espelho" que descreve biunivocamente não apenas os elementos dos dois conjuntos, mas também suas Estruturas de grupo.

As duas estruturas são consideradas *algebricamente indistinguíveis*. Uma das estratégias matemáticas para entender um grupo é identificá-lo isomorficamente com outro grupo mais conhecido, em geral constituído de de matrizes numéricas quadradas.

Indução

Se $\{G,*,e\}$ for um Grupo e $\varphi: G \to C$ uma função bijetiva entre os dois conjuntos, **então** podemos definir uma estrutura de Grupo $\{C,°,E\}$ denominada **induzida** da seguinte maneira natural:

1-$E = \varphi(e)$

2-Para quaisquer $\alpha, \beta \in H$, então $\alpha°\beta = \varphi(\varphi^{-1}(\alpha) * \varphi^{-1}(\beta))$)

Subgrupos

Se $\{G,*,e\}$ for um grupo e $H \subset G, e \in H$ e a operação produto * for fechada em H (isto é, para $h, g \in H \Longrightarrow hg \in H$) **então** $\{H,*,e\}$ é um grupo e diz-se que é subgrupo de $\{G,*,e\}$.

Exercícios:

0-Mostre que se $\varphi: G \leftrightarrow H$ for um isomorfismo entre dois Grupos $\{G,°,e\}$ e $\{H,*,\varepsilon\}$, então, necessariamente, $\varphi(e) = \varepsilon$.

1-Demonstre as afirmações constantes das duas definições acima.

2-Mostre que $\{\mathbb{R},+,0\}$ e $\{\mathbb{R}^{++}, \cdot, 0\}$ são Grupos Isomorfos segundo a bijeção definida pela função exponencial (logaritmo).

3-Mostre que se *A* for um conjunto não vazio, então o conjunto de funções invertíveis $\varphi A \leftrightarrow A$, $\wp(A)$a operação composição "°" e a função identidade $i: A \leftrightarrow A, i(a) = a$ constituem um Grupo $\{\wp(A),°,i\}$denominado Grupo de Permutações de *A*.

4-Mostre que o subconjunto $\mathcal{M}$ das matrizes reais 2×2 da forma $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ tais que $a^2 + b^2 \neq 0$, a operação produto matricial e a matriz identidade constituem um Grupo $\{\mathcal{M},\cdot,I\}$.

5-Mostre que o Grupo $\{\mathcal{M},\cdot,I\}$ definido acima é isomorfo ao Grupo $\{\mathbb{C} - \{0\}, \cdot ,1\}$ constituido dos números complexos não nulos, a operação produto e a unidade natural.

6-Mostre que o Grupo $\{\mathcal{M},\cdot,I\}$ é um subgeupo do Grupo constituído das Matrizes reais 2×2 da forma $\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$ inversíveis com o produto matricial e a Identidade *I*.*(Na verdade as matrizes* $n \times n$ *inversiveis , o produto e a identidade formam um Grupo).*

7-Mostre que o subconjunto das matrizes 2×2 da forma $\begin{pmatrix} cos\theta & sen\theta \\ -sen\theta & cos\theta \end{pmatrix}$ constituem um subgrupo de $\{\mathcal{M},\cdot,I\}$ que é isomorfo ao subgrupo dos complexos unitários de $\{\mathbb{C} - \{0\}, \cdot ,1\}$ que são isomorfos ao subgrupo de $\{\wp(\mathbb{C} - \{0\}),°,i\}$ formada pelas Rotações em torno da origem.

8-Mostre que o conjunto $C^0([0,1])$ das funções reais de variável real continuas $f: [0,1] \leftrightarrow [0,1]$ formam um subgrupo de $\wp([0,1])$.

9- Mostre que o conjunto $C^0([0,1]) \cap \wp([0,1])$ (Funções reais continuas $f: [0,1] \leftrightarrow [0,1]$, invertíveis) constituem um subgrupo de $\{\wp([0,1], \circ, i\})$.

10- Mostre que o conjunto das funções reais $f: [0,1] \leftrightarrow [0,1]$ continuamente diferenciáveis $C^1([0,1]) \cap \wp([0,1])$ **não** constituem um subgrupo de $\{\wp([0,1], \circ, i\})$, mas se nos restringirmos ao subconjunto das funções continuamente diferenciáveis cuja derivada é sempre não-nula em $(0,1)$ então teremos um subgrupo de $\{\wp([0,1], \circ, i\})$. (Sugestão: Analise a função $f(x) = x^3$).

Definição: ***Grupo de Permutações - Transposições***

O Grupo de Permutações $\{\wp(A), \circ, i\}$).em um conjunto finito $A, \#A = n$ pode ser representado pelo Grupo de permutações do conjunto $I_n = \{1, \dots \dots, n\}$ que será denominado P_n. Um elemento deste grupo é freqüentemente representado pela sugestiva notação: $\pi = \begin{pmatrix} 1 & k & n \\ p_1 & p_k & p_n \end{pmatrix}$ em que $\pi: k \to \pi(k) = \pi_k$.

Uma classe especial de permutações de P_n é constituída das transformações denominadas **transposiçõ**es e significam que se restringem a uma simples **troca** τ_k ,$1 \leq k < n$ de posição entre dois índices **adjacentes** $\pi_k \leftrightarrow \pi_{k+1}$ enquanto que as outras posições são mantidas.

Exercício

Mostre que $\tau_k \circ \tau_k = i$.

Mostre que qualquer permutação $\pi \in P_n$ pode ser representada como resultado de uma seqüência de transposições aplicada à identidade, isto é, existe $\{\tau_k\}_{1 \leq k < m}$ tal que, sucessivamente, efetuam a mesma transformação, isto é, $p = \tau_m{}^{\circ\circ\circ\circ\circ\circ}\tau_1$.

Mostre que existe um número mínimo de transposições que efetuam esta fatoração e determine este número.

O importante teorema abaixo mostra que qualquer seqüencia de transposições que *fatora* uma determinada permutação $\pi \in P_n$ tem sempre uma mesma paridade (ímpar ou par) que é, portanto, uma característica de π descrita por $\sigma: P_n \to \{+1, -1\}$, onde $\sigma(\pi) = \sigma_\pi = 1$ se a paridade de π for par e $\sigma_\pi = -1$ se a paridade for ímpar.

Teorema: ***Existencia do sinal de Permutação***

Existe uma ***função*** $\sigma: P_n \to \{+1,-1\}$, denominada sinal de permutação, de tal forma que se $\pi \in P_n$ e $\pi = \tau_m \circ \circ \circ \; \tau_1$ então $\sigma_\pi = (-1)^{\,m}$.

Demonstração:

Considere o polinômio $p(x_1, \dots, x_n) = \prod_{j<k}(x_k - x_j)$, constituído do produto de todas as possíveis diferenças na ordem dos índices das suas variáveis.

Defina agora a ação de uma permutação $\pi \in P_n$ sobre um polinômio $Q(x_1, \dots, x_n)$ de *n* variáveis ao seguinte polinômio denotado por πQ também de *n* variáveis definido por: $\pi Q(x_1, \dots, x_n) = Q\left(x_{\pi(1)}, \dots, x_{\pi(n)}\right)$. Observe que $\pi p = \pm p$ e, particularmente, para uma transposição qualquer, τ , temos o seguinte efeito $\tau p = -p$.

Assim, se $\pi = \tau_m \circ \circ \circ \; \tau_1$ for uma fatoração da permutação π por uma particular sequencia $\{\tau_k\}$ de transposições, conclui-se que $\pi p = \tau_m \circ \circ \circ \; \tau_1 p = (-1)^m p$. Como o termo da direita terá sempre o mesmo resultado πp , independente da fatoração, conclui-se o desejado.

Referências:

G.Birkhoff-S.MacLane-*Álgebra Moderna,*