Verbetes do dicionário de Matemática
A

Praciano-Pereira, Tarcisio [1]

12 de fevereiro de 2022
preprints da Sobral Matemática
no. 2022.01
Editor Tarcisio Praciano-Pereira
tarcisio@sobralmatematica.org

[1]tarcisio@sobralmatematica.org

Resumo

Estou começando a publicação do *dicionario de Matemática* que é trabalho que comecei em 2007, despretensiosamente, apenas preparando material para usar em minhas aulas. Ao me aposentar se transformou no *meu objetivo de vida* uma motivação para seguir aprendendo Matemática. Se despertar interesse agradeço críticas e colaborações. Deixo claro que consultei muito mais textos do que estes citados na bibliografia, *e que os erros são todos meus*, um estudante de Matemática.

- **Abel, Lema de** Considere a série de potências

$$S_n(z) = \sum_{k=0}^{n} c_n z^n \tag{1}$$

por comparação com séries geométricas se pode deduzir que se

$$\overline{\lim} \sqrt[n]{|c_n|} = \frac{1}{r} \tag{2}$$

então S_n converge absoluta e uniformemente no disco $B(0,\rho); \rho < r$. Nada se pode dizer sobre o que acontece na fronteira deste disco. O número r é o raio de convergência da série de potências. As séries de potências definem funções de classe $\mathcal{C}^\infty$ no interior do disco de convergência e tais funções satisfazem às equações de Cauchy-Riemann são as funções analíticas, ou holomorfas.

Usando-se a fórmula de *Euler-De Moivre* se pode escrever sucessivamente

$$c_n z^n = \rho_n e^{in\theta} r e^{in\alpha} = \rho_n r e^{in(\theta+\alpha)}; \tag{3}$$

$$|c_n z^n| = \rho_n r < 1 \iff \rho_n < \tfrac{1}{r}; |c_n| = \rho_n < \tfrac{1}{r}; \tag{4}$$

$$S_n(z) = \sum_{k=0}^{n} c_n z^n \tag{5}$$

donde se conclui que uma condição necessária para que a série na equação (eq.5) seja absoluta e uniformemente convergente é que o domínio da série seja o disco de raio r tal que

$$\overline{\lim_n} \rho_n = \frac{1}{r}; \tag{6}$$

O recurso ao *limite superior* se deve porque os coeficientes da série nem mesmo precisam ter um limite mas devem estar confinados no disco de raio r para que se possa usar o *critério de convergência* das séries geométricas.

A recíproca é também verdadeira, se os coeficientes da série se encontrarem confinados no disco de centro r a série é absoluta e uniformemente convergente. Este é o conteúdo do *Lema de Abel*.

Substituindo na equação (eq.5) a expressão do desenvolvimento de Taylor no ponto z_0 se tem

$$\sum_{k=0}^{n} c_n (z - z_0)^n \tag{7}$$

para qual expressão valem as mesmas contas que eu fiz acima conduzindo ao resultado genérico do *Lema de Abel* para uma série de potências qualquer que é convergente uniformemente no disco de raio r centrado no ponto z_0.

O resultado na equação (eq.2) é equivalente a forma como eu expressei o *Lema de Abel* se eu fizer a comparação com a série de potências como uma série geométrica de razão ρ o que leva a expressão conhecida como *critério da razão* que é a equação (eq.2).

- **absolutamente somável**

Uma série $S_n = (\sum_{k=0}^{n} a_k)_n$ se diz **absolutamente somável** ou **absolutamente convergente** se a série obtida com a substituição $a_k := |a_k|$ for convergente.

Theorem **1 (comutatividade)** *Séries e comutatividade Se S_n for* **absolutamente convergente** *e se α for uma bijeção de* $\mathbf{N}$ *então, [5, página 39]*

$$(\sum_{k=0}^{n} a_k)_n = (\sum_{k=0}^{n} a_{\alpha(k)})_n$$

Observe que usar uma bijeção α é apenas uma *forma generalizada* de expressar a comutatividade.

A série harmônica, $S_n = (\sum_{k=1}^{n} (-1)^{k+1}/k)_n$ converge mas a permutação

$$\left(\sum_{j=1}^{2^{n-1}} \frac{1}{2^n + (2j+1)} - \sum_{j=1}^{2^{n-1}} \frac{1}{2^n - 2j} \right)_n$$

não converge.

- **ação** de um grupo. Da teoria dos grupos.

Definição 1 (ação do grupo G) *sobre o conjunto S*

Considere um grupo $(G, \cdot)$, um conjunto S arbitrário, "e" indicando a unidade *de G. A transformação*

$$G \times S \to S; (g, s) \mapsto g(s) \in S; \begin{cases} (e, s) \mapsto e(s) = s; \text{ identidade}; \\ (g, (h, s)) = (gh, s); \text{ associatividade}; \end{cases} \tag{8}$$

é uma ação de G sobre S.

Exemplo 1 (permutações) *de G Intuitivamente,* ação *dum grupo sobre um conjunto S significa que os elementos do grupo agem como funções sobre este conjunto S. Um exemplo é que um grupo G age sobre si mesmo porque os elementos do grupo representam permutações de G ao serem multiplicados (operados) sobre os outros elementos inclusive a si próprio. A tabela dum grupo finito é composta de todas as permutações que os elementos do grupo produzem e assim em cada linha ou coluna se encontram cópias de G.*

Exemplo 2 (Matrizes) *representação de G*

Como um exemplo, considere $S = \mathcal{M}_{n\times n}$ o grupo das matrizes inversíveis de ordem n e $G = Sim(n)$ o grupo das permutações de n elementos. Defina para

$$g \in G, s \in S \mapsto (g, s) = g - \text{permutação das colunas de } s; \tag{9}$$

Se $g = e$ resulta na própria matriz s e a segunda condição também é satisfeita porque g, h permutações, gh é a composição das outras permutações de sorte que (gh, s) é uma permutação das colunas de s.

Uma especialização interessante dos segundo exemplo é obtida quando S for exatamente o conjunto das permutações das colunas da identidade quando se diz que S é uma representação do grupo G como transformações lineares do espaço $\mathbf{K}^n$ em que o corpo $\mathbf{K}$ é de onde se tomam as entradas dos elementos de S. .

G não precisa ser um *grupo de permutações* porque na verdade todos os grupos finitos são grupo de permutações ou contém um grupo de permutações, e até mesmo os grupos não finitos mas em geral não se

pensa nestes como grupo de permutações... Este exemplo descreve o que significa *representar um grupo G com um grupo de transformações lineares dum certo espaço vetorial*.

Como um outro exemplo derivado do anterior, tome agora um conjunto arbitrário com n elementos $S = \{1, 2, \ldots, n\}$ ao qual está associado o grupo das permutações $G = Sim(n)$ de formas que

$$\sigma \in G, i \in S; (\sigma, i) = j \in S; \tag{10}$$

$$\begin{cases} e(i) = i; \\ \sigma(\tau(i)) = ((\sigma o \tau), i); \end{cases} \tag{11}$$

Este exemplo, que na verdade deveria ter sido o primeiro porque justifica o anterior, mostra que existe uma ação canônica dum grupo qualquer num conjunto que tenha, pelo menos como cardinalidade a ordem do grupo.

O próximo exemplo mostra que a condição de igualdade entre cardinalidade e ordem não é essencial. Considere o grupo cíclico $Z_2 = \{0, 1\}$ e S o conjunto das simetrias dum triângulo equilátero, de vértices $\{a, b, c\}$. Então é o diedral D_3 que tem 2×3 elementos e posso definir

$$0 \mapsto I; 1 \mapsto (ab); \tag{12}$$

em que I é permutação identidade e (ab) deixa c fixo, permutando a, b. As duas condições são satisfeitas.

O próximo exemplo mostra uma forma canônica que implementar uma *ação* dum grupo qualquer sobre um conjunto S também arbitrário. Para não aderir a uma notação muito complicada vou manter o espírito de *exemplo*.

Dado um grupo G e um conjunto S o conjunto G^S é

$$f \in G^S; \tag{13}$$

$$f : S \longrightarrow G; S \ni s \xrightarrow{f} y = f(s) \in G \tag{14}$$

é o conjunto de todas as funções definidas em S e tomando valores em G. Se $S = \{1, 3, 3\}$ e $G = \mathbf{R}$ então $G^S = \mathbf{R}^3$.

S tem uma imagem canônica em G^S que é $(1, r), (2, r), (3, r)$ a função constante de valor $r \in G$, os conjuntos

$$S, \{(1, r), (2, r), (3, r)\} = \tilde{S}$$

são equipotentes, têm mesma cardinalidade[1]

Dado um par $(r, s) \in G \times S$ posso identificar de forma única o ponto $(s, r) \in \tilde{S}$ que posso *identificar* com s e dizer que tenho:

$$r(s) = s \equiv (r, s);$$

definindo assim uma ação de G em S.

Esta identificação de S com a imagem duma função constante de de G^S é muito frutífera e aparece em vários contextos.

- **aceleração da gravidade** é considerada uma constante e vale $g = -9m/s^2$. Os cálculos seguintes mostram que é razoável admitir que Galileu *estava correto* ao tentar mostrar que Arquimedes *estava errado* em supor que corpos com massas distintas cairiam com velocidades diferentes contra o solo.

[1] Na verdade seria uma $r-$imagem canônica... uma imagem para cada valor de r.

$$F = ma; \text{ segunda lei de Newton;} \tag{15}$$

$$\begin{cases} F_1 = \frac{m_1 M}{r^2} = m_1 A; A = \frac{M}{r^2}; \\ F_2 = \frac{m_2 M}{r^2} = m_2 A; A = \frac{M}{r^2}; \\ m_1 \leq m_2 \quad \Rightarrow \quad F_1 \leq F_2; \end{cases} \tag{16}$$

$$v_1(t) = \frac{F_1 t}{m_1} = At; A = g; \tag{17}$$

$$v_2(t) = \frac{F_2 t}{m_2}; = At; A = g; \tag{18}$$

$$g = -9m/s^2; v(t) = gt; s(t) = \frac{g}{2}t^2 + v_0 t + s_0; \tag{19}$$

Newton tirou conclusões e escreveu a sua *obra magna* compilando tudo de Física que se conhecia à sua época, mas certamente Galileu e Arquimedes desconfiavam que que $f = ma$. Aqui se encontra embutido um postulado da matéria, pelo qual a *massa* é uma propriedade da matéria, é o coeficiente de resistência da matéria a alterar um seu *estado* chamado *velocidade*.

Então as equações (eq.16) medem a força de atração de dois corpos de massas m_1, m_2 pela Terra o que levou Arquimedes a concluir que as velocidades em queda livre seriam diferentes para dois corpos com massas distintas. Aqui entrou Galileu, que não me parece que tenha expressado o postulado sobre massa como uma propriedade da matéria que resiste à alteração do seu estado de velocidade, mas certamente ele tinha esta percepção.

A solução para corrigir Arquimedes consiste em colocar a massa do corpo como coeficiente de razão inversa o que fiz na equação (eq.17) e na equação (eq.18) encontrando a equação da velocidade em que $A = g$.

Os experimentos todos confirmam que esta é equação dando à como expressão da distância percorrida a equação duma parábola

$$s(t) = -\frac{g}{2}t^2 + v_0 t + s_0; \tag{20}$$

em que s_0 é a distância inicial, v_0 a velocidade inicial.

A conclusão que tiro destes cálculos, na equação (eq.17) e na equação (eq.18) se baseiam no postulado que define *massa* como sendo a propriedade que tem os corpos para resistirem à mudança do seu *estado de velocidade*. A *velocidade* é uma *ilusão relativista*, somente podemos falar de velocidade por comparação com um referencial, portanto a velocidade, como tal, em forma absoluta, não existe. Idealmente, se aplicarmos uma força a um corpo, estaremos alterando o seu *estado de velocidade*, e esta alteração será tanto mais forte quanto menor massa o corpo tiver. É por isto que existe uma velocidade máxima no Universo, da luz, porque também ela, como corpo, é formada da *menor das massas* que se podem encontrar no Universo, mas tem massa e portanto tem uma *velocidade máxima*, a velocidade da luz, simbolizada pela letra c, é, por definição, igual a 299.792.458 metros por segundo no vácuo.

Uma forma de verificar se Galileu estava correto é a experimental e aqui entra a história da torre inclinada de Pisa que alguns historiadores afirmam que se trata duma lenda. Gilberto Cunha, em artigo escrito em 30 de Agosto de 2019 no jornal O Nacional de Passo Fundo, "Galileu e a fake news de Pisa" menciona o historiador Alexander Koyré que concluiu em seus estudos que a famosa experiência seria uma *notícia falsa* produzida por Viviani que é o autor de uma das primeiras biografias de *Galileu Galilei*.

- **acumulação, ponto de**, confira *ponto de acumulação*.

- **álgebra de grupo** é uma álgebra de convolução sobre um espaço vetorial indexado no grupo G, $\mathbf{C}^G$.

O conjunto $\mathbf{C}^G$ é o espaço vetorial das funções definidas em G com valores complexos. Se G for um grupo finito, com n elementos, $\mathbf{C}^G = C^n$ é o espaço dos vetores complexos com n coordenadas indexados sobre G, é uma *forma complicada de descrever* C^n mas que vale a pena para considerar uma nova estrutura a ser definida em C^n usando a indexação sobre um grupo que tenha n elementos. Logo vou mostrar *onde* posso ganhar com esta *complicação*.

Observe que

$$C^n = C^{\{1,2,\ldots,n\}} \approx C^G; |G| = n; \tag{21}$$

é o conjunto das funções definidas no conjunto $\{1, 2, \ldots, n\}$ com valores em $\mathbf{C}$, da mesma forma como C^G é o conjunto das funções complexas definidas em G.

Deixe-me supor inicialmente seja o caso, $|G| = n$, um grupo finito, e vou definir algumas das operações mais importantes de $\mathbf{C}^G = C^n$ estabelecendo também a *representação linear* de G em $\mathcal{GL}(\mathbf{C}^G)$, o grupo das transformações lineares com determinante diferente de zero do espaço vetorial C^G.

Vou apresentar uma lista de equações que quase se auto explicam, mas você pode descer um pouco no texto e ler os comentários que vou tecer sobre cada uma destas equações. Nelas estou também introduzindo a notação que vou usar no resto do artigo.

$$u \in \mathbf{C}^G; (u_g)_{g\in G}; M(u) = \tfrac{1}{|G|} \sum_{g\in G} u_g \in \mathbf{C}; \text{ um valor médio;} \tag{22}$$

$$h \in G \mapsto M(u)_h = \tfrac{1}{|G|} \sum_{g\in G} u_{gh^{-1}} = M(u) \in \mathbf{C}; \text{ permutação dos termos da soma;} \tag{23}$$

$$(u_g), (v_g) \in \mathbf{C}^G; u * v = (x_h)_{h\in G}; x_h = \tfrac{1}{|G|} \sum_{g\in G} u_g v_{gh^{-1}}; x = u * v \in \mathbf{C}^G; \tag{24}$$

$$(\mathbf{C}^G, +, *) \text{ é uma álgebra ;} \tag{25}$$

$$A : \mathbf{C}^G \to \mathbf{C}^G; A = \begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ & & \vdots & \\ a_{n1} & a_{n2} & \ldots & a_{nn} \end{pmatrix} \in \mathcal{GL}(\mathbf{C}^G); \tag{26}$$

$$G = \{e = g_1, \ldots, g_n\}; g_i \equiv \sigma_i \in Sim(n); \tag{27}$$

$$I = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ 0 & 0 & \cdots & 1 \end{pmatrix} \ni \mathcal{GL}(\mathbf{C}^G) \equiv e \in G; G \ni e \mapsto I; \tag{28}$$

$$I_{\sigma_i} \equiv g_i \in G; G \ni g_i \mapsto I_{\sigma_i} \tag{29}$$

Vou comentar as equações listadas acima, elas descrevem os principais fatos *duma representação linear* do grupo G dentro do *grupo linear* $\mathcal{GL}(\mathbf{C}^G)$ e deixe-me relembrar estes tópicos.

Eu vou usar, na continuação, a notação já apresentada nas equações, as letras u, v são elementos do espaço vetorial $\mathbf{C}^G$, eventualmente também x, w. As letras g, h representam elementos do grupo G. Letras maiúsculas, A, B representam funções lineares definidas em $\mathbf{C}^G$.

Observe que eu *escolhi implicitamente* uma base para $\mathbf{C}^G$, é isto que está revelado nas matrizes $I_{\sigma_i} = I_{g_i}$, só existe a *matriz* duma *transformação linear* se houver uma base escolhida.

1. A equação (eq.22) descreve um elemento genérico de $\mathbf{C}^G$, um vetor com $|G| = n$ coordenadas se G for um grupo finito. Se G for enumerável é uma sucessão de números complexos e então tenho que discutir a convergência para que eu possa me referir a este espaço. Vou adiar esta discussão. Neste momento isto é apenas uma forma complicada de fazer referência a $\mathbf{C}^n = \mathbf{C}^G$, um espaço de sucessões finitas, todas com n elementos, se $|G| = n$. Associado a cada ênupla, eu posso definir uma

média, $M(u) \in \mathbf{C}$. Para ficar mais claro, observe que as três expressões seguintes significam a mesma coisa, embora a terceira seja uma *transformação* da anterior,

$$u = (u_1, \ldots, u_n), (u_g)_{g\in G}, (u_{gh^{-1}})_{g\in G}; h \in G \text{ fixo} ; \tag{30}$$

ou seja G é também um conjunto de índices, apenas é *um conjunto de índices inteligentes*, são elementos dum grupo. A terceira expressão na equação (eq. 30) é diferente da segunda expressão uma vez que eu fiz uma permutação dos elementos quando eu multipliquei por $h^{-1}; h \in G$. É neste ponto que o *conjunto de índices é inteligente*. Eu posso rapidamente permutar as ênuplas num espaço vetorial se ele estiver indexado sobre um grupo.

2. Na equação (eq.23), dada uma ênupla $u = (u_{g\in G})$ estou mostrando que a média definida na equação anterior tem uma propriedade de invariância relativamente à permutação provocado pelo elemento h, na última igualdade. Observe que embora eu tenha usado a notação $M(u)_h$, o valor da média não depende de h, é um invariante relativamente ao elemento h usado. Mas vou precisar deste índice logo em seguida.

   A *invariância* é apenas consequência de duas coisas, uma, que h permuta os elementos da soma, dois, que a soma não muda porque estou aplicando a propriedade comutativa. Esta média é invariante sob permutações dos elementos do grupo. Simples consequência da propriedade comutativa, mas é uma primeira razão que justifica o *método complicado*: as somas são invariantes por permutação dos índices dos elementos e fazer esta permutação é tão simples quando multiplicar por qualquer elemento do grupo, outro que a identidade. Isto no caso $|G| = n$ é pura aplicação da propriedade comutativa, estou calculando a mesma soma permutando as parcelas uma vez que h^{-1} permuta os elementos da ênupla. Dado um grupo G tenho em $\mathbf{C}^G$ uma média invariante sob a permutação dos elementos de G.

   também a propriedade associativa se $n > 2$.

3. a convolução Na equação (eq.24) tenho um nova *ênupla* associada as ênuplas u, v, tenho uma soma em que aparecem os produtos $u_g v_{gh^{-1}}$ mas a soma "*consome*" apenas a variável g portanto o resultado define o número complexo x_h. É a média do produto ponto a ponto das ênuplas u, v com a segunda permutada, ou ainda, é o produto escalar

$$x_h = \tfrac{1}{|G|} < u, v^h >; (v^h) = (v_{gh^{-1}})_{g\in G}; h \text{ é constante}; \tag{31}$$

$$x = u * v; \tag{32}$$

   em que segundo fator, v^h teve suas coordenadas permutadas por $h \in G$. A nova ênupla é o produto por convolução de $u, v \mapsto u * v$. O fator $\frac{1}{|G|}$ pode ser eliminado para definir a *convolução habitual*. Mas vou logo mostrar que ele pode ser interessante. *Qualquer produto* pode ser transformado em outro *produto* por um fator multiplicativo. Observe que isto altera a escala, a unidade tem que ser também alterada, se houver unidade.

   notação péssima $v^h = (v_{gh^{-1}})_{g\in G}$ $v^h \in \mathbf{C}^G$ com coordenadas permutadas por $h \in G$

   Na equação (eq.24) eu defini um novo elemento de $\mathbf{C}^G$, a partir dos dois elementos $u, v \in \mathbf{C}^G$ que estou chamando $x = u*v$. Esta é a segunda razão para o uso da *forma complicada* de apresentar $\mathbf{C}^G = C^n$. Seria mais trabalhoso definir o produto de convolução de duas ênuplas de números complexos se elas não estivessem indexada sobre um grupo G. Este ponto é mais um dos que tornam a *complicação* $C^n = \mathbf{C}^G$ interessante. Num artigo de 1967, [25], eu encontrei esta forma de definir a convolução numa *Álgebra de Grupos*, e vale a pena repetir o método porque ela oferece uma alternativa a notação que apresentei acima usando v^h para representar uma $h-$permutação de v. Acompanhe na sequência de equações que entendo que são autoexplicativas. A notação permanece a mesma das equações

anteriores.

$$u, v \in \mathbf{C}^G; (u_g)_{g\in G}; (v_h)_{h\in G}; \tag{33}$$

$$(gh)_{g,h\in G} \text{ descreve a tabela do grupo } G; \tag{34}$$

$$x_h = \frac{1}{|G|}\sum_{g\in G} u_g v_h; \text{ ao longo da linha } h \text{ da tabela do grupo } G = \tag{35}$$

$$= \frac{1}{|G|}\sum_{g\in G} u_g v_{h^{-1}}; \text{ ao longo da linha } h \text{ da tabela do grupo } G; \tag{36}$$

$$x_h = \frac{1}{|G|}\sum_{g\in G} v_g u_h \text{ ao longo da linha } h \text{ da tabela do grupo } G; \tag{37}$$

$$x = u * v \neq v * u; \tag{38}$$

O autor citado alterou a notação ao longo do artigo algumas vezes usando a média para definir a convolução, outras vezes sem a média como foi o caso desta expressão que é a equação (9) do artigo citado.

(a) Na equação (eq.33) estou descrevendo duas ênuplas de $\mathbf{C}^G$, uma indexada com o símbolo g e a outra com o símbolo h o que não representa absolutamente nenhuma diferença, é uma lista de elementos indexados no conjunto de índices G, que agora também é um grupo.

(b) Na equação (eq.34) estou descrevendo a tabela do grupo G. Você pode admitir que estou usando o método *LICO*, portanto estou descrevendo ao longo de cada linha determinada por g e depois variando g.

(c) Na equação (eq.35) estou fazendo o produto ponto-a-ponto das ênuplas com a segunda permutada pelo índice $h \in G$ e calculando a média deste produto ponto-a-ponto;

(d) Na equação (eq.36) eu reescrevi a média usando agora o fator h^{-1} porque algumas vezes é interessante usar esta expressão.

(e) Na equação (eq.37), para calcular $v*u$, eu vou multiplicar todos os números complexos $(v_g)_{g\in G}$ pelo número complexo u_h o que torna o produto de convolução não comutativo, independentemente de que G seja ou não comutativo.

(f) Na equação (eq.38) o novo elemento $x = u*v$ tem em cada coordenada esta média com $u*v \neq v*u$.

Uma das dificuldades para compreender Álgebra de Grupos reside na notação, algumas vezes confusa de certos autores, e é bem o caso no artigo de Löwdin, [25] em que ele usa dois símbolos para representar a mesma coisa. Junte-se a importância que esta álgebra é importante para os físicos que usam uma notação algumas vezes diferentes daquela que nós os matemáticos usamos, e é bem o caso da equação (9) de [25], mas também de outras equações à volta desta quando o somatório representa um vetor e não uma soma, observe que na parte esquerda de (9) não tem sentido somar

$$\sum_k a_k g_k$$

que na verdade significa

$$(a_g)_{g\in G} \text{ o vetor } a \in \mathbf{C}^G;$$

Na equação (10) ele deixa isto claro quando escreve

$$\alpha(g_k) = a_k;$$

Onde acima eu estou usando u_g para representar um número complexo da ênupla $u \in \mathbf{C}^G$, Löwdin faz uso de dois símbolos um dos quais ele chama de função α que é uma função $\alpha : G \to \mathbf{C}$, nada mais nada menos do que uma ênupla de números complexos. Os dois símbolos, α, u representam a mesma coisa o que eu simplifiquei acima usando apenas u, v e em [25] aparecem α, β, u, v.

4. Na equação (eq.25) eu tenho a *álgebra de grupo*. Usando a soma usual das ênuplas de números complexos e a nova operação, produto por convolução, tenho uma álgebra não comutativa porque $u * v \neq v * u$. É um espaço vetorial no qual está definida um produto com as propriedades dum anel não comutativo.

5. funções lineares do espaço $\mathbf{C}^G$ Na equação (eq.26) eu escrevi uma matriz $n \times n$. Um tipo de função definida na *álgebra de grupo* são as matrizes. Elas são as funções lineares da *álgebra de grupo*. Eu vou representar as matrizes usando as letras maiúsculas $A, B, \ldots, I$. Entre estas matrizes tem duas classes que vão ser muito importantes na representação de grupos que são (1) as matrizes com determinante diferente de zero elas formam o que se chama de *grupo linear*, e (2) as matrizes com determinante exatamente 1 que é um grupo fechado das matrizes com determinante diferente de zero. Este segundo grupo é o SL_n, em que n é a dimensão do espaço, ou dentro da terminologia deste artigo é $|G|$. $SL_1 = \mathbf{S}^1$ o círculo trigonométrico o que mostra que a cardinalidade deste segundo grupo é a mesma de $\mathbf{C}$. Na verdade a cardinalidade deixa de ser um catálogo importante porque o que vai interessar são os isomorfismos que pudermos estabelecer entre os diferentes tipos de grupos.

6. G é um conjunto de permutações Na equação (eq.27) eu repeti o que já havia dito acima que G funciona como um conjunto de índices, ao mesmo tempo que cada elemento de G representa uma permutação de G. Observe que $G \subset Sim(n)$, a menos dum isomorfismo: $|G| = n < n! = |Sim(n)|$.

7. A matriz identidade de $GL(\mathbf{C}^G)$ aparece na equação (eq.28) é a matriz identidade de $GL(C^G)$. Esta matriz tem um papel importante na teoria de representação de grupos, ela tem n colunas que podem ser permutadas, é o que aparece na equação (eq.29).

8. Um elemento qualquer de G é uma permutação dos seus n elementos, exatamente dos n elementos de G. Para isto eu tenho que identificar σ_g que represente g como permutação dos elementos de G. Para ver como se faz isto, confira *representação linear de grupos* mas a ideia básica eu descrevi no item anterior, permute as colunas de da matriz identidade I obtendo as matrizes I_g, claro, indexadas em G.

Deixe-me fazer um rápido sumário do foi discutido acima, repetindo a notação uma vez que há muita informação já acumulada. Também vou chamar atenção dum aspecto fino que ficou pouco comentado.

Começando pelas duas últimas equações porque elas são a *chave* para *representar* G como um conjunto de matrizes de ordem n.

$\mathbf{C}^G = \mathbf{C}^n$, como estou ainda mantendo como hipótese, é um espaço vetorial de dimensão n e os morfismos de espaço vetorial deste espaço, as funções lineares, formam dois importantes grupos, de todas as matrizes $n \times n$, um grupo aditivo, comutativo, e um subconjunto que é um grupo multiplicativo, não comutativo: as matrizes $n \times n$ cujo determinante é diferente de zero, $\mathcal{GL}(\mathbf{C}^G)$

$$(\mathcal{L}(\mathbf{C}^G, \mathbf{C}^G), +); (\mathcal{GL}(\mathbf{C}^G, *); \tag{39}$$

o primeiro, o grupo aditivo, é todas as matrizes que algumas vezes é referenciado como $\mathcal{M}_{n\times n}$. O segundo, o grupo multiplicativo e usualmente chamado de *grupo linear*, é formado por todas as matrizes que tenham determinante diferente de zero. A importância deste grupo está ligada ao fato de que ele é um conjunto

aberto duma topologia "*habitual*". Qualquer matriz *singular* pertence à fronteira deste grupo. Eu estarei aqui centrado neste grupo multiplicativo, no *grupo linear*.

O *grupo linear* ainda tem um subgrupo importante, o das matrizes cujo determinante seja 1, porque o

- *determinante do produto* é o *produto dos determinantes*, e
- o *determinante da inversa* é o *inverso do determinante*.

estas duas condições com um teorema fundamental da teoria dos grupos garante que as matrizes com determinante 1 é um grupo multiplicativo. Este é um subgrupo fechado do anterior. Compare com $\mathbf{C}$ onde este grupo é o círculo trigonométrico, $\mathbf{S}^1$ é um grupo fechado do grupo dos números complexos diferentes de zero. Aqui a única matriz singular é o $0 + 0i$;

Um *subgrupo das matrizes cujo determinante seja* 1 é formado pela matriz identidade,I, junto com as permutações de suas colunas, este grupo é uma imagem perfeita de $Sim(n)$ que é um grupo muito especial pois ele contém todos os grupos de ordem menor ou igual a n, em particular contem G. A imagem de G é obtida quando se aplicam as colunas de I as permutações σ_g que os elementos $g \in G$ representam como permutações sobre G.

Exemplo 3 ($G = \mathbf{Z}_3$) *a álgebra de grupo* $\mathbf{R}^{\mathbf{Z}_3}$

O que eu disse anteriormente para $\mathbf{C}^{\mathbf{Z}_3}$ *vale para* $\mathbf{R}^{\mathbf{Z}_3}$*, é o espaço vetorial* $(x_0, x_1, x_2) = (x_g)_{g \in \mathbf{Z}_3}$ *é uma* forma complicada *de descrever o* $\mathbf{R}^3$.

Vou usar a base usual do $\mathbf{R}^3$ *indexada em* $\mathbf{Z}_3$

$$\mathbf{Z}_3 = \{0, 1, 2\} = \{g_0, g_1, g_2\} \tag{40}$$

$$e_0 = (1, 0, 0); e_1 = (0, 1, 0); e_2 = (0, 0, 1); \tag{41}$$

$$I_0 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}; I_1 = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}; I_2 = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}; \tag{42}$$

Eu obtive estas matrizes aplicando g_1, g_2 *às colunas da matriz identidade* I_0*. Experimente com um programa de álgebra linear computacional, por exemplo* `octave` *que é de* domínio público *e é uma* réplica dum famoso programa comercial *que é vendido por uma nota preta.* `octave` *foi iniciado e mantido por um professor americano, John W. Eaton, hoje acompanhado por muitos outros. Num sistema do tipo Debian/Gnu/Linux você instala* `octave` *com o comando:*

```
sudo apt-get install octave
```

Melhor é usar o sistema instalador de programas *para uma versão completa do* `octave`

As equações acima ficam em `octave` *assim*

```
I_0 = [ 1, 0, 0; 0, 1, 0; 0, 0, 1 ];
I_1=  [ 0, 1, 0; 0, 0, 1; 1, 0, 0 ];
I_2=  [ 0, 0, 1; 1, 0, 0; 0, 1, 0 ];
```

e agora você pode executar $I_1 * I_2$ *para obter* $I_0 = I$.

```
I_{1}*I_{2};
function y = pow(x,n) x**n endfunction;
function z = F(x,y) pow(x,2) - 3*x*y + pow(y,2) endfunction;
```

Eu tenho aqui a condição de demonstrar este teorema importante da teoria dos grupos: $Sim(n)$ contém todos os grupos de ordem menor ou igual a n, porque eu representei um grupo de ordem n,G, como permutações das colunas da matriz identidade de ordem n usando a permutação que $g \in G$ representa para G mas se eu escrever todas as permutações da colunas de I eu vou ter uma representação de $Sim(n); G \subset Sim(n)$. O argumento é mesmo para $k < n$.

Observe o detalhe, $G \subset Sim(n)$ e o grupo das matrizes I_g obtidas aplicando às colunas da matriz identidade as permutação σ_g que os elementos $g \in G$ representam como permutações sobre G é um subconjunto de todas as matrizes obtidas permutando as colunas da identidade que é um grupo isomorfo a $Sim(n)$. As matrizes $\hat{G} = (I_g)_{g \in G}$ formam um grupo isomorfo a G com n elementos.

$$\hat{G} \approx G \tag{43}$$

É o que estou indicando na última equação da lista acima, com a notação I_{σ_i} em que σ_i equivale g_i como permutação de G. Repetindo, o conjunto de matrizes obtidas a partir da matriz identidade ao lhe aplicar as permutações σ que cada elemento de $g_i \in G$ representa sobre os elementos de G são a imagem de G no grupo das matrizes de ordem n com determinante 1.

A partir do grupo G eu construí o espaço vetorial $\mathbf{C}^G$ no qual defini um produto, $*$ de modo que $(\mathbf{C}^G, +, *)$ é uma álgebra. G é um conjunto de índices para descrever $u \in \mathbf{C}^G$ e G aparece como um subconjunto do grupo linear de $\mathbf{C}^G$,

$$\hat{G} = (I_g)_{g \in G} \approx G; \hat{G} \subset \mathcal{GL}(\mathbf{C}^G); \tag{44}$$

os elementos de G são representados por matrizes que são elementos do grupo linear de $\mathbf{C}^G$.

Vou agora obter um resultado bem especial que vai inclusive testar a notação que construí acima. Quem representa em $\hat{G}$ o produto $gh \in G$?

Obviamente, pela notação produzida, é I_{gh}. Ocorre que no grupo G gh representa a composição das permutações $\sigma_g o \sigma_g$. Ou seja o produto de G é a composição das permutações que os elementos de G representam sobre G. Então $I_{gh} = I_g I_h$ é o produto de matrizes. Isto fecha a afirmação de que $\hat{G}$ é uma imagem isomorfa de G.

A leitora atenta pode observar que o espaço $\mathbf{C}^G$ é inteiramente inútil na construção acima. Em particular eu fiz nenhum uso da convolução a não ser para definir a álgebra $(\mathbf{C}^G, +, *)$. Eu poderia diretamente construir $\hat{G}$ produzindo $(I_g)_{g \in G}$ que é a *representação* de G como transformação linear. Inclusive a *convolução* não está sendo utilizada nesta passagem. Este parágrafo sintetiza a *teoria da representação linear de grupos* e sugere que houve uma *complicação inútil* introduzida para atingir um objetivo relativamente simples. Existe um único ponto que parece válido que é a própria convolução que permitiu a criação da álgebra $(\mathbf{C}^G, +, *)$.

Vou agora mostrar que há alguns resultados que se perderam no caminho. Por exemplo $\hat{G}$ representa apenas n transformações lineares, ou matrizes, porque sempre podemos fixar uma base no espaço e assim identificar matrizes e transformações lineares. É apenas o grupo da matrizes com determinante 1 do espaço vetorial $\mathbf{C}^{Sim(2)} = \mathbf{C}^2$ tem uma infinidade não enumerável de elementos compare com $\mathbf{S}^1$, o círculo trigonométrico. Então tem muita coisa que se está perdendo dentro da *simplificação útil*...

Deixe-me retomar $\mathbf{C}^G$ e também a propriedade que esta indexação dos vetores deste espaço me oferece pelo fato de que seja um grupo. Um subgrupo de $H \subset G$ produz um subespaço vetorial de $\mathbf{C}^G$ que é $\mathbf{C}^H$. Se $H \lhd G$ for um *subgrupo normal* de G então H particiona G em classes de equivalência de tal modo que G/H é um grupo, $\mathbf{C}^H$ é um subespaço de $\mathbf{C}^G$ e é interessante questionar o que acontece com representação linear de H em relação à representação linear de G.

H particiona G, mesmo que não seja *normal*, entretanto as classes Hg são diferentes das classes gH consequentemente particiona de duas maneiras diferentes tornando estas classes inconsistentes com o produto, por que tem dois

produtos, um produto à direita e outro à esquerda. Vou considerar apenas quando $H \triangleleft G$, um subgrupo normal. Mas é provável que seja interessante o caso complementar porque, mesmo que H não seja normal, as classes laterais formam uma partição de G.

- $|H|$ é menor do que $|G|$ e é um divisor da ordem de G,
- $\mathbf{C}^H$ é um subespaço de $\mathbf{C}^G$,
- $\mathbf{C}^{gH}$ é um subespaço de $\mathbf{C}^G$, para todo elemento de $g \in G$ e desta forma eu tenho $|H|$ subespaços de $\mathbf{C}^G$, um para cada uma das classes. A lista $(gH)_{g\in G}$ contém repetições, mas basta selecionar o conjunto $(gH)_{g\in G}$. Como as classes formam uma partição de G, e como a base do espaço $\mathbf{C}^G$ está indexada pelos elementos de G estes subespaços produzem uma soma direta que recompõe $\mathbf{C}^G$

$$\oplus_{g\in G}\, \mathbf{C}^{gH} = \mathbf{C}^G \tag{45}$$

A primeira observação mais evidente é que como H particiona G então eu tenho um *método automático* para selecionar os vetores da base do espaço, coisa que eu não teria com formatação $\mathbf{C}^n$. Óbvio que é uma seleção associada ao subgrupo H, esta partição é formada de H das translações de H dentro de G que são em número $\frac{|G|}{|H|}$, quando G for finito que eu ainda continuo com esta hipótese.

Então aqui vem a primeira grande vantagem da *útil complicação*, eu posso decompor a imagem de qualquer transformação linear, mais exatamente eu posso decompor a matriz de qualquer transformação linear em blocos relativamente à partição que H produz nos vetores básicos que estão indexados nos elementos de G. A escolha do grupo G é também uma *escolha automática duma base de vetores para o espaço* $\mathbf{C}^G$.

No próximo exemplo eu estou acrescentando uma estrutura ao grupo G, uma topologia de grupo, uma topologia relativamente à qual a operação do grupo seja contínua, o que faz de G um *grupo topológico*.

A leitora é convidada a observar que estou repetindo alguns dos fatos já mencionados anteriormente dentro do próximo exemplo, afinal um exemplo, mas agora incluindo uma *nova operação de conjugação* que define um automorfismo de grupos dentro do *grupo geral linear*.

Exemplo 4 (grupo topológico) *endomorfismo complexo*

Seja G um grupo topológico de Hausdorff, $|G| = n$, e suponha definido um morfismo de grupo topológico, um morfismo contínuo

$$\phi : G \to \mathcal{GL}(\mathbf{C}^G); \phi : g \ni G \mapsto \phi(g) = A_g \in \mathcal{GL}(\mathbf{C}^G); \tag{46}$$

Como $|G| = n$, então $phi(g) = A_g$ é uma matriz $n \times n$ e deixe-me abusar da notação por motivo de simplificação e chamar a imagem deste morfismo, a matriz A_g, usando a mesma letra para indicar as entradas da matriz, onde se usaria normalmente $A = (a_{ij})$ eu vou evitar a inclusão da letra "a".

$$g \ni G \mapsto \phi(g) = A_g = A_g(ij)_{i=1,\dots,n;j=1,\dots,n}; |G| = n; \tag{47}$$

$$i \mapsto A_{t,i,j=1,\dots,n}; A_{t,ij} : G \to \mathbf{C}^G; \tag{48}$$

Fixando i, uma linha da matriz $A(ij)$, na equação (eq.48) eu estarei identificando uma função

$$i \mapsto A_{t,ij=1,\dots,n} : G \to \mathbf{C}^G; \tag{49}$$

Cada linha da matriz A_g é uma ênupla de números complexos portanto uma função de G em $\mathbf{C}$, lembrando que $|G| = n$. Fica claro que A é contínua se e somente se cada linha da matriz for uma função contínua *de G em $\mathbf{C}^G \approx \mathbf{C}^n$.*

Posso relembrar algumas notações importantes da álgebra dos números complexos

$$A = (A_{ij}); {}^{t}A = (A_{ji}) \textit{ é a transposta da matriz } A; \tag{50}$$

$$\overline{A} = (\overline{A_{ij}}) \textit{ é a conjugada } A; \tag{51}$$

$${}^{t}(AB) = {}^{t}(\sum_{j=1}^{n} A_{ij}B_{jk}) = \sum_{j=1}^{n} B_{kj}A_{ji} = ({}^{t}B)({}^{t}A); \tag{52}$$

$$({}^{t}({}^{t}A)) = A; \tag{53}$$

$$\overline{AB} = \overline{AB}; \overline{\overline{A}} = A; \tag{54}$$

e a transposição e a conjugação definem dois morfismos topológicos de ordem 2. A conjugação é um automorfismo *do* grupo geral linear.

A matriz A_t é regular*, ou* não singular *se ela tiver um inverso e no presente exemplo isto corresponde a*

$$\det(A_t) \neq 0; (AB)^{-1} = B^{-1}A^{-1}; \det(A^{-1}) = \det(A)^{-1}; \tag{55}$$

$${}^{t}(A^{-1}) \neq ({}^{t}(A))^{-1}; \tag{56}$$

A demonstração da equação (eq.56) é consequência direta da definição da matriz inversa que depende do cálculo da matriz dos cofatores de A que são diferentes dos cofatores de $({}^{t}A)$ assim a equação (eq.56) mostra que a transposição não é um automorfismo *do* grupo geral linear *como é o caso da conjugação. Entretanto é possível definir uma outra expressão, a* transposta conjugada*, que produz um* automorfismo *do* grupo geral linear*,*

$$A^{*} = ({}^{t}A^{-1}); \tag{57}$$

$$(A^{-1})^{*} = ({}^{t}A) \tag{58}$$

$$(A^{*})^{-1} = ({}^{t}(A)^{-1})^{-1}; \tag{59}$$

$$(AB)^{*} = {}^{t}((AB)^{-1}) = {}^{t}(B^{-1}A^{-1}) = {}^{t}(A^{-1})^{t}(B^{-1}) = A^{*}B^{*}; \tag{60}$$

fazendo da transposta conjugada *um* automorfismo *do* grupo geral linear.

Há dois conjuntos significativos que são das matrizes unitárias em que o determinante vale 1 e como o produto dos determinantes é o determinante do produto, o conjunto destas matrizes forma um subgrupo do grupo das matrizes regulares *que também é um grupo pela mesma propriedade do produto dos determinantes, este um grupo aberto da topologia de do* grupo geral linear*, porque o determinante é uma função multilinear contínua do conjunto das matrizes do* grupo geral linear *e o anterior, das matrizes unitárias, um* grupo fechado *consequência imediata de estar definido por uma igualdade. Este exemplo repassa alguns dos fatos já expostos acima com a inclusão da* transposta conjugada*.*

- **álgebra vetorial** é o conjunto de regras da Álgebra que se aplicam aos vetores. Este conjunto de regras é também conhecido como *análise vetorial*.

Esta "*análise vetorial*" foi produzida ao longo de muito tempo e aos poucos foi sendo recompilada para ser usada no Cálculo Avançado, o Cálculo a três variáveis então grande parte das fórmulas se referem a três vetores dados. Ela vale no espaço de dimensão n como uma generalização em que se considera um espaço tridimensional contido no $\mathbf{R}^n$ vou seguir aqui esta formulação.

Considere três vetores $u, v, w \in \mathbf{R}^n$

$$< u, v >= u \cdot v = \sum_{k=1}^{n} u_k v_k \text{ produto escalar;} \tag{61}$$

$$\|u\| = \sqrt{< u, u >} \text{ módulo de } u; \tag{62}$$

$$< u, v >= \|u\|\|v\| \cos(\alpha); \alpha = arg(u, v); \tag{63}$$

$$u \times v = \begin{vmatrix} \vec{i} & \vec{j} & \vec{k} \\ u_1 & u_2 & u_3 \\ v_1 & v_2 & v_3 \end{vmatrix} \tag{64}$$

$$\|u \times v\| = \|u\|\|v\| \sin(\alpha); \alpha = arg(u, v); \tag{65}$$

$$< u, v \times w >= u \cdot (v \times w); \text{ produto misto ;} \tag{66}$$

- O *produto escalar* chamado assim quando foi posteriormente inventado, em oposição ao *produto vetorial*, este último produz um vetor enquanto que o *produto escalar* produz um número e é comutativo. A definição na equação (eq. 61) é independente da dimensão do espaço.

- O produto escalar define o módulo dum vetor, está associado a uma das possíveis normas do $\mathbf{R}^n$ a chamada norma euclidiana.

- A propriedade expressa na equação (eq. 63) redefine o produto escalar geometricamente usando o ângulo , (argumento), entre os dois vetores. Pode-se demonstrar a equivalência entre as duas definições, (eq. 61) e (eq. 63), e isto é facilmente feito usando números complexos e a fórmula do cosseno da diferença entre dois ângulos. A propriedade vale em qualquer dimensão por que dois vetores determinam um plano então é uma propriedade bidimensional, mesmo com $u, v \in \mathbf{R}^n$. Confira mais abaixo o caso do produto vetorial em que também posso usar a trigonometria e números complexos para estabelecer a identidade entre as definições geométrica e algébrica.

- A equação (eq. 64) está redigida para $n = 3$ mas ela vale para $u, v \in \mathbf{R}^n$ uma vez que dois vetores determinam um plano. Ela descreve o *produto vetorial* de dois vetores e o seu significado e origem são geométricos embora com o tempo se tenha descoberto a forma algébrica, expressa no "*falso determinante* que aparece na equação (eq. 64). É um "falso determinante" que algumas vezes é chamado de "*determinante formal*" pela sua aparência com o determinante da álgebra. O produto vetorial é anticomutativo o que justifica o uso do determinante em sua definição:

$$u \times v = -v \times u; \tag{67}$$

O uso dos vetores $\vec{i}, \vec{j}, \vec{k}$, da Física, é parte integrante da definição original uma vez que a troca de linhas implica na alteração da ordem como os *vetores da Física* são utilizados e em particular se tem

$$\begin{cases} \vec{i} \times \vec{j} = \\ \begin{vmatrix} \vec{i} & \vec{j} & \vec{k} \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{vmatrix} = \vec{k}; \\ \vec{j} \times \vec{i} = -\vec{k}; \\ \vec{j} \times \vec{k} = \vec{i}; \vec{k} \times \vec{j} = -\vec{i}; \\ \vec{k} \times \vec{i} = \vec{j}; \vec{i} \times \vec{k} = -\vec{j}; \end{cases} \tag{68}$$

quando os *vetores da Física* forem substituídos, dentro do determinante, nas linhas dois e três, por suas coordenadas relativamente à base do $\mathbf{R}^3$ que estes três vetores formam:

$$\vec{i} = (1,0,0)\,;\ \vec{j} = (0,1,0)\,;\ \vec{k} = (0,0,1)\,; \tag{69}$$

No $\mathbf{R}^n$ esta fórmula segue valendo pela escolha de três vetores que formam um *triedro positivo* e que são, nesta ordem, paralelos aos vetores $\vec{i}, \vec{j}, \vec{k}$ da Física.

- A equação (eq. 65) redefine o produto vetorial geometricamente o que facilita a expressão deste produto para qualquer dimensão uma vez que dois vetores determinam um plano então fica bem definido o ângulo , (argumento), entre eles. Como no caso do produto escalar, podemos usar a trigonometria para demonstrar a equivalência entre as definições, a algébrica e a geométrica:

$$u = (\cos(\alpha), \sin(\alpha)); v = (\cos(\beta), \sin(\beta)); \tag{70}$$

$$u \times v = \begin{vmatrix} \vec{i} & \vec{j} & \vec{k} \\ \cos(\alpha) & \sin(\alpha) & 0 \\ \cos(\beta) & \sin(\beta) & 0 \end{vmatrix} = \tag{71}$$

$$= \vec{k}\,(\cos(\alpha)\sin(\beta) - \cos(\beta)\sin(\alpha)) = \tag{72}$$

$$= \vec{k}\sin(\alpha - \beta); \tag{73}$$

de onde posso deduzir alguns fatos:

  - se $\vec{u}, \vec{v}$ forem ortogonais então $\alpha - \beta = \frac{\pi}{2}$;
  - se $\vec{u}, \vec{v}$ forem unitários e ortogonais, então $\vec{u} \times \vec{v}$ é unitário, esta é a metodologia para obter um triedro positivo no $\mathbf{R}^n$ pela escolha de dois vetores unitários ortogonais, então $\vec{u} \times \vec{v} = \vec{k}$
  - $u = \vec{i}, v = \vec{j}$ então $u \times v = \vec{k}$, $v \times u = -\vec{k}$.
  - $(u \times v) \perp [u, v]$, o produto vetorial pertence ao espaço perpendicular àquele gerado por u, v porque:
    - sempre posso identificar o espaço gerado por u, v como gerado por $\vec{i}, \vec{j}$ se eles forem l.i. é simplesmente um espaço de dimensão dois.
    - $u \times v$ se encontra na direção de $\vec{k}$.

  então $\|u \times v\| = \sin(\alpha - \beta)$ o *seno* do ângulo entre os dois vetores u, v se eles forem unitários.

- O *produto misto* é fácil de ser entendido geometricamente: $u \cdot (v \times w)$

  1. Primeiro observe que $u \times u$ é nulo porque o ângulo entre eles é zero.
  2. Agora, $u \times v \times w$ precisa ser definida então se impõe a *associatividade* como regra:

     $$u \times v \times w = u \times (v \times w) = (u \times v) \times w;$$

     e agora se tem

     $$u \times (u \times v) = (u \times u) \times w = 0$$

     de onde se conclui que $u \perp (u \times v)$, ou ainda que $u \times v$ é um vetor perpendicular ao plano determinado pelos vetores u, v.

3. pela definição geométrica do produto vetorial, $v \times w$ é área do paralelogramo que estes vetores determinam.
4. como $u \cdot (v \times w)$ é o produto escalar por vetor que é perpendicular ao plano determinado pelos vetores u, w então $u \cdot (v \times w)$ é projeção de u na direção perpendicular ao plano determinado pelos vetores v, w e consequentemente o *produto misto* corresponde, em módulo, ao volume do paralelepípedo determinado pelos três vetores u, v, w.

- **algébrico, número** são os números definidos por uma equação algébrica, por exemplo, como $\sqrt{2}$ é uma solução da equação polinomial $P(x) = 0$ com

$$P(x) = x^2 - 2 \tag{74}$$

então o número irracional $\sqrt{2}$ é um número algébrico o que mostra que existem números algébricos que são irracionais e então o conjunto dos números algébricos tem interseção não vazia com o conjunto dos números irracionais. Mas como há números irracionais que não são algébricos, π, então estes dois conjuntos são distintos.

O conceito de *número algébrico* é *relativo* a um certo corpo. De partida, todos os elementos de corpo K são algébricos sobre K uma vez que eles são soluções de equações polinomiais do primeiro grau com coeficientes em K, o que tornaria a definição inútil. Então o conceito de número algébrico diz respeito a "números" que se encontram num corpo que é estensão de K. Um número é *algébrico sobre um corpo* K se ele for solução duma equação polinomial cujos coeficientes se encontram em K. A definição anterior de *numero algébrico* deve ser lido "*número algébrico sobre o corpo* $\mathbf{Q}$. Por exemplo i é algébrico sobre $\mathbf{Q}$ e também é algébrico sobre $\mathbf{R}$ e i é uma elemento duma estensão de $\mathbf{Q}$ ou de $\mathbf{R}$.

Conceitos relacionados:

- Estensão de um corpo, ou um corpo F estende o corpo K dado.
- Anel dos polinômios sobre um corpo K.

- **algoritmo** é um método descrevendo a execução de uma tarefa. Um programa, escrito em uma linguagem de computação, é um algoritmo. Algumas equações podem representar um algoritmo, como

$$p = dq + r; p, d, q, r \in \mathbf{N}; r < d; q > 0 \tag{75}$$

é o algoritmo da divisão euclidiana de p por d, porque, dados p, d podemos encontrar dois únicos números q, r de modo a definir a divisão de p por d. Embora este "algoritmo" seja passivo, ele é um antigo exemplo de expressão algorítmica em Matemática.

Como exemplo de algoritmo, fere um pouco a concepção atual desta palavra uma vez que ele não produz os números q, r, apenas serve para testar uma quantidade finita de de pares (q, r) com objetivo de encontrar um que sirva. Mas, como esta expressão podemos construir um *método*, com divisões sucessivas, e expressar esta sucessão de divisões com uma linguagem de programação que seria um algoritmo na concepção atual. O próprio método de divisão sucessivas é um *algoritmo* uma vez que ele pode ser traduzido numa linguagem de programação.

- **ampere** é uma unidade do sistema de medidas, "*Sistema Internacional de Unidades*" para a quantidade de corrente elétrica pelo tempo. É também uma homenagem ao físico francês André-Marie Ampère.

Um *ampere* equivale à média de 1 coulomb de carga elétrica por segundo sendo portanto uma medida de velocidade.

- **análise não padronizada** é uma teoria encabeçada pelo matemático holandês Abraham Robinson e por vários dos seus seguidores, que tentam recuperar o conceito *infinitesimal* que se encontra na fundação do *Cálculo Diferencial e Infinitesimal*. É um belo exercícios de construção lógica! Eu suspeito que usando o conjunto das sucessões dos números racionais se possa criar um exemplo concreto para a *análise não padronizada*, ou ainda que os infinitesimais são as as sucessões dos números racionais, possivelmente o anel das que convergem para zero.

Sem dúvida é um belo exercícios de construção lógica que merece ser enfrentado mas sem esperar atingir o objetivo de livros cujo título é *Nonstandard Analysis in Practice*, ou *análise não padronizada na prática*...

- **analise vetorial** é estensão ao $\mathbf{R}^n$ das operações vetoriais para serem usadas pelo Cálculo Vetorial multivariado. Confira **operadores diferenciais**.

As operações significativas, sendo $A, B, C \in \mathbf{R}^n$ são

1. *produto vetorial*, $A \times B \in \mathbf{R}^{n+1}$,
2. *produto escalar*, $< A, B >= A \cdot B \in \mathbf{R}$, é um número que corresponde ao tamanho da projeção de A na direção de B expandido com módulo de B

$$< A, B >= |A||B| \cos(\alpha); \alpha \text{ o ângulo entre } A, B;$$

3. *produto misto*, $< A \times B, C > \in \mathbf{R}$ é a projeção de $A \times B$ na direção de C expandido com módulo de C.

Estas operações também são feitas com os *vetores formais* que representam operadores diferenciais criando novos operadores diferenciais. Confira **operadores diferenciais**.

- **analítica, função** é uma função complexa de variável complexa que é diferenciável no sentido complexo.

As funções complexas de variável complexa tem integral e derivada exatamente como estas operações foram definidas no Cálculo para funções reais de variável real, entretanto, a derivação complexa cria um tipo novo de função, as *funções analíticas*.

O *plano complexo*, ou o *conjunto dos números complexos*, pode ser visto como $\mathbf{R}^2$,

- um espaço vetorial sobre o corpo dos reais, ou
- um espaço vetorial sobre o corpo dos números complexos.
- as funções $\mathbf{R}^2 \to \mathbf{R}^2$;
- as funções $\mathbf{C} \to \mathbf{C}$ que sejam diferenciáveis com derivada complexa.

são aspectos que é preciso separar.

Vou mostrar aqui que o conjunto das *funções complexas de variável complexa diferenciáveis* é um subconjunto próprio das *funções vetoriais reais de variável vetorial real diferenciáveis* com propriedades muito diferentes do "grande conjunto". Na verdade o estudo das *funções complexas de variável complexa* se chamou durante muito tempo *teoria das funções* embora não se pensasse que o assunto se restringisse a subclasse das *funções complexas*.

Definição 2 (analítica) *função*

F é uma função analítica se tiver derivada complexa*, e isto quer dizer que $F'(z) \in \mathbf{C}$ ou ainda que vale*

$$dF(z) = F'(z)dz \in \mathbf{C}$$

é o modelo da função linear complexa *tangente ao gráfico de F num ponto a em que ela seja derivável.*

Uma função definida pela *integral de Cauchy* é uma função analítica.

Teorema 1 (integral) *de Cauchy*

Seja Ω um domínio do plano complexo, e $\gamma = \partial\Omega$ a fronteira de Ω. Sobre a curva γ considere definida uma função ou uma medida, F. A integral de Cauchy

$$F(a)Ind_\gamma(a) = \frac{1}{2\pi i}\int_\gamma \frac{F(t)dt}{t-a}; a \in \Omega \tag{76}$$

estende F como uma função analítica ao domínio Ω. **Dem**:

Observação 1 (considerações) *sobre a fórmula integral de Cauchy*

Como Ω é aberto e γ é a sua fronteira, então $a \notin \gamma$.

O número $Ind_\gamma(a)$ é o índice de $\underline{a}$ relativamente à curva γ. Se $\underline{a}$ estiver no exterior da curva então ele será zero. Se a curva γ der mais de uma volta em torno de $\underline{a}$, o número $Ind_\gamma(a)$ irá assumir isto com um número inteiro do número de voltas. Se γ for uma curva simples e fechada, então $Ind_\gamma(a) = 1$ e pode ser omitido da fórmula, eu farei isto nas próximas vezes que usar a fórmula a não ser que seja preciso usar uma curva que não seja simples e que portanto tenha índice superior a 1 para algum ponto interior à curva.

A forma mais "geral" para a integral de Cauchy que elimina esta discussão é

$$F(a) = \frac{1}{2\pi i Ind_\gamma(a)}\int_\gamma \frac{F(t)dt}{t-a}; a \in \Omega$$

o problema é que $Ind_\gamma(a)$ pode ser zero... sendo esta a razão de que prefiro a forma "menos elegante" da equação (eq. 76).

Na equação (eq. 76) posso identificar um produto por convolução *de F pelo núcleo de Cauchy.*

Por ser uma convolução, a regularidade de uma das funções, no caso o chamado núcleo de Cauchy*, é herdado pela nova função que é assim derivável indefinidamente. A propriedade da derivada dum produto de convoluções, $(f * g)' = f' * g = f * g'$ nos leva à conclusão de que F é derivável e que $F'(a) \in \mathbf{C}$ portanto, F tem uma* derivada complexa *sendo então analítica.*

Este raciocínio se itera, a conclusão é se F for uma função analítica é então indefinidamente diferenciável e todas suas derivadas são também analíticas e todas definidas no mesmo domínio *pela fórmula integral de Cauchy.*

q.e.d .

Teorema 2 (série de potências) *e função analítica*

Seja Ω um domínio do plano complexo, e $\gamma = \partial\Omega$ a fronteira de Ω. Sobre a curva γ considere definida uma função ou uma medida, F. A integral de Cauchy

$$F(a) = \frac{1}{2\pi i}\int_\gamma \frac{F(t)dt}{t-a}; a \in \Omega \tag{77}$$

então F tem uma série de potências convergente em cada um dos pontos do domínio Ω. **Dem**:

γ é a fronteira dum domínio então $Ind_\gamma(a) = 1$ e assim eu omiti esta expressão.

A integral de Cauchy define F como infinitamente diferenciável em qualquer ponto $a \in \Omega$ então tem uma série de Taylor em cada ponto $a \in \Omega$. Resta-me calcular o raio de convergência e verificar que é diferente de zero.

Partindo da equação (eq. 77) o coeficiente de Taylor a_k de F no ponto $a \in \Omega$ é

$$a_k = \frac{F^{(k)}(a)}{k!} = \frac{1}{k!} F * \frac{d^k C(t)}{dt}(a) = 2\pi i \int\limits_{\gamma} \frac{(-1)^k k! F(t) dt}{k!(t-a)^{2k-1}}; \tag{78}$$

$$a_k = 2\pi i \int\limits_{\gamma} \frac{(-1)^k F(t) dt}{(t-a)^{2k-1}}; \tag{79}$$

em que $C(t) = \frac{1}{t}$ é o núcleo de Cauchy.

Majorando e minorando a última integral, tenho

$$Km(a)^{2k-1} \leq \|a_k\| \leq KM(a)^{2k-1};\ K = 2\pi \|F\|_{\infty} \mu(\gamma);$$

em que $\mu(\gamma)$ é a medida de γ, $m(a), M(a)$ são, respectivamente, o mínimo e o máximo da translação $C(t)$ para o ponto $\underline{a}$, calculados sobre γ. $M(a)$ pode não ter limite quando $\underline{a}$ se aproximar da fronteira sendo este um item que vou comentar ao final da demonstração.

Aplicando o teste da raiz *para o cálculo do* raio de convergência *tem-se*

$$\frac{1}{\rho} = \limsup_k \sqrt[k]{|a_k|} \leq \tag{80}$$

$$\leq \lim_k \sqrt[k]{KM(a)^{2k-1}} = \lim_k \sqrt[k]{K} \sqrt[k]{M(a)^{2k-1}}; \tag{81}$$

$$\frac{1}{\rho} \leq M(a); \rho = \frac{1}{M(a)} \tag{82}$$

q.e.d .

Observação 2 (Raio) *de convergência*

Observe que $M(a)$ cresce muito à medida que $\underline{a}$ se aproximar da fronteira, e, respectivamente, ρ decresce para zero. A figura (fig 1), página 18 mostra dois valores de ρ para dois pontos, $\underline{a}$, $\underline{b}$ dentro do domínio Ω, é o raio do disco máximo *que seja possível obter,*

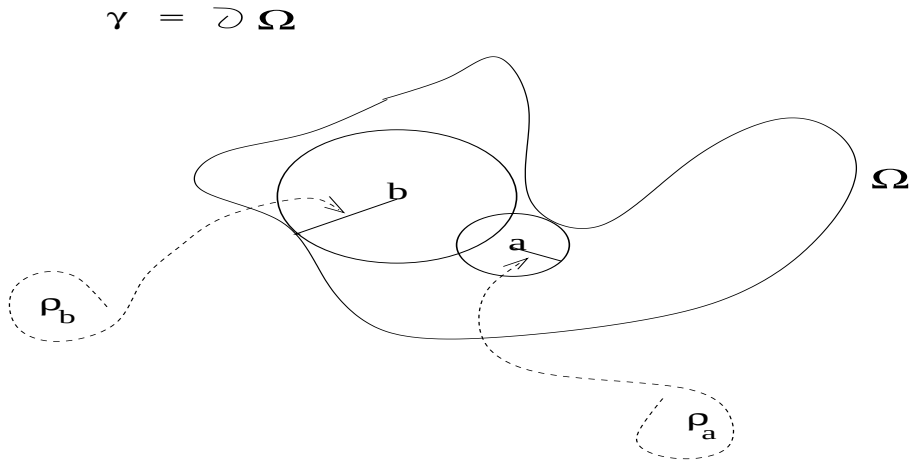

Figura 1: Raio de convergência na série de potências

centrado no ponto $\underline{a}$ ou $\underline{b}$ tangenciando a fronteira γ. O inverso de ρ_a é o máximo atingido pela translação do núcleo de Cauchy ao ser transladado para o ponto $\underline{a}$.

Se $\underline{a}$ for escolhido sobre γ então $M(a) = \infty$ e consequentemente $\rho = 0$ entretanto isto não é tudo porque na demonstração os valores na fronteira, F foram eliminados com a majoração de a_k e se F for considerada com mais cuidado é possível que este limite exista e seja diferente de zero o que abre a expansão do domínio de analiticidade de F para além do domínio Ω. Esta é uma situação a ser considerada em cada caso particular e caí no contexto de extensão do domínio de analiticidade que não vou considerar aqui, mas posso voltar a este ponto em outra versão deste trabalho. Observe que "levar F em consideração apenas altera as contas da demonstração do teorema 2 no caso do calculo do disco de convergência no ponto $a \in \gamma$. Esta consideração mostra a riqueza de detalhes que se pode atingir com esta teoria.

A figura (fig 2), página 19 ilustra esta nova situação, quando $\rho \neq 0$ e $a \in \gamma$. Neste caso o domínio de analiticidade contém o antigo Ω e mais a bola $W = B(a, \rho)$.

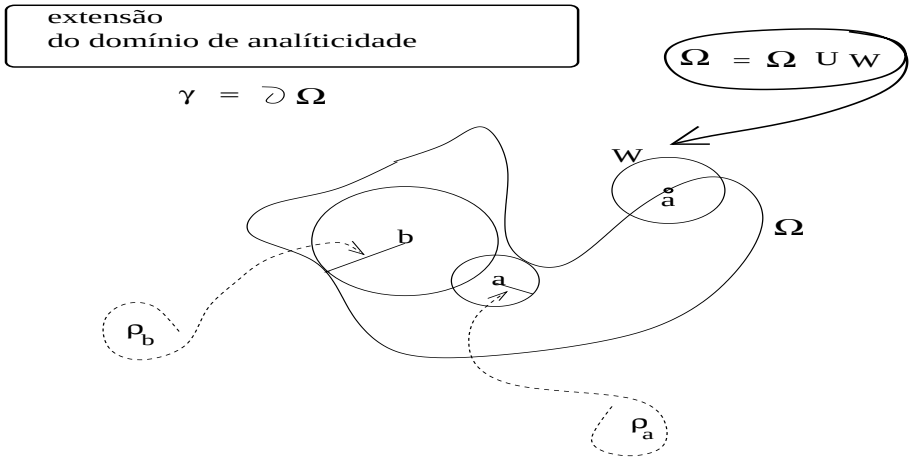

Figura 2: extensão do domínio de analiticidade

Considere agora uma função analítica como uma função $\mathbf{R}^2 \longrightarrow \mathbf{R}^2$ a consequência da hipótese, "*ter uma derivada complexa*", sobre a jacobiana $J(f)$ será que a jacobiana de F é uma *função linear complexa*.

As funções lineares complexas formam um subconjunto próprio das funções lineares do $\mathbf{R}^2$, $\mathcal{L}(\mathbf{R}^2)$, elas são representadas pelas matrizes da forma

$$\mathcal{L}(\mathbf{R}^2) \ni \begin{bmatrix} \alpha & \beta \\ -\beta & \alpha \end{bmatrix} \approx (\alpha - i\beta) \in \mathbf{C} \tag{83}$$

$$\begin{bmatrix} \alpha & \beta \\ -\beta & \alpha \end{bmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} \alpha x + \beta y \\ -\beta x + \alpha y \end{pmatrix}; \tag{84}$$

$$\begin{bmatrix} \alpha & \beta \\ -\beta & \alpha \end{bmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \equiv (\alpha - i\beta)(x + iy); \tag{85}$$

são as funções lineares do $\mathbf{R}^2$ que se identificam com a multiplicação por um número complexo, quando vistas como funções lineares complexas, como está indicado na equação (eq. 84). Observe que a equação (eq. 84) é a hipótese para obter a equação (eq. 83). Obviamente também é possível reverter esta implicação e na verdade (eq. 83) é equivalente a (eq. 84).

Equações de Cauchy-Riemann

Considere agora uma função analítica F que também pode ser vista como uma função vetorial real de variável vetorial,

$$\mathbf{R}^2 \xrightarrow{F} \mathbf{R}^2 \tag{86}$$

e como é uma função vetorial então ela tem duas funções coordenadas sendo comum escrever $F = u + iv \equiv (u, v)$ em que as funções coordenadas u, v são funções reais de variável vetorial real

$$F = u + iv;\ u : \mathbf{R}^2 \longrightarrow \mathbf{R};\ v : \mathbf{R}^2 \longrightarrow \mathbf{R}; \tag{87}$$

Usando as equações (eq. 87) posso obter a jacobiana de F

$$J(F) = \begin{bmatrix} u_x & u_y \\ v_x & v_y \end{bmatrix} = \begin{bmatrix} u_x & u_y \\ -u_y & u_x \end{bmatrix} = \begin{bmatrix} v_y & -v_x \\ v_x & v_y \end{bmatrix}; \tag{88}$$

$$u_x = v_y; u_y = -v_x; \tag{89}$$

$$F'(a) = u_x(a) - iu_y(a) = v_y(a) + iv_x(a); \tag{90}$$

A igualdade na equação (eq.88) vem da hipótese de que F seja uma função analítica, quer dizer, tenha *derivada complexa*. A identificação da derivada de F, calculada no ponto $\underline{a}$, na equação (eq.90) é consequência da equação (eq.85).

Um dos objetivos deste texto é mostrar que a equação (eq. 77) pode ser tomada como definição para função analítica. Até agora tenho um teorema estabelecendo que a equação (eq. 77) define uma função analítica e quero chegar à recíproca, com alguma restrição: toda função analítica num domínio Ω pode ser obtida pela (eq. 77) a partir de valores na fronteira de Ω, ou seja um *problema de valor na fronteira*.

O sistema de equações parciais de primeira ordem que aparece na equação (eq.89) se chama *equações de Cauchy-Riemann* e também pode ser usado como definição para uma função analítica porque, valendo, implica em que a derivada de F, é uma derivada complexa. Vale a recíproca.

Teorema 3 (funções harmônicas) *Equação de Laplace*
As funções coordenadas de $F = u + iv$ satisfazem à equação de Laplace,

$$u_{xx} + u_{yy} = 0 = v_{xx} + v_{yy}$$

Dem.

$$\begin{cases} u_{xx} + u_{yy} = v_{yx} - v_{xy} = v_{yx} - v_{yy} = 0 \\ v_{xx} + v_{yy} = -u_{yx} + u_{xy} = -u_{xy} + u_{xy} = 0 \end{cases}$$

aplicando primeiro as equações de Cauchy-Riemann e depois a identidade de Clairot-Schwarz para as derivadas mistas.
q.e.d .

As soluções da equação de Laplace são chamadas funções harmônicas e um biproduto da construção da teoria das funções analíticas é a solução da equação de Laplace no caso bivariado porque se a cada função harmônica u existe um *conjugado harmônico* v que é uma solução das equações de Cauchy-Riemann.

Pelo teorema de Clairaut-Schwarz podemos concluir que as partes real e imaginária da função analítica F satisfazem a formula trivial do teorema de Green:

Teorema 4 (Os conjugados harmônicos) *e o teorema de Green*
Dem.

$$\partial\Omega = \gamma; \tag{91}$$

$$\iint_{\Omega}(v_{yx} - v_{xy})dxdy = 0 = \oint_{\gamma} v_x dx + v_y dy; \tag{92}$$

$$\iint_{\Omega}(u_{yx} - u_{xy})dxdy = 0 = \oint_{\gamma} u_x dx + u_y dy; \tag{93}$$

q.e.d .

Observação 3 (Séries de potências) *outra definição de função analítica*

A definição 77 não era a usual até os anos 50 do século 20, quando se definiam as funções analíticas como aquelas que tinham um desenvolvimento em série de potências.

Na literatura clássica, para citar dois exemplos que fizeram mais sucesso, o livro de Titchmarsh, Theory of Functions, ou livro de Hobson, se define função analítica usando uma série de potências:

$$(a_k)_{k\in N}; F(z) = \sum_{k=0}^{\infty} a_k z^k; \tag{94}$$

que pode ser livremente baixado da página https://archive.org

Henri Cartan também escreveu um livro sobre funções analíticas *que infelizmente não teve o sucesso que merecia até mesmo porque foi escrito numa época em que já se iniciava o abandono da definição de funções analíticas via séries de potências convergente em seu domínio de analiticidade, e Cartan partiu para este método desenvolvendo no primeiro capítulo uma complicada teoria das séries, suficiente para assustar qualquer leitor iniciante. O método usado aqui é o que será utilizado nas extensões da teoria para várias variáveis ou para o caso de dimensão infinita.*

Théorie élémentaire des fonctions analytiques d'une ou plusieurs variables complexes.

O uso das séries como definição para as funções analíticas está baseado no Lema de Abel pelo qual existe um número ρ que pode ser calculado a partir dos coeficientes $(a_k)_{k\in N}$ da série, chamado raio de convergência*, definindo um disco onde a série converge absolutamente, e consequentemente também uniformemente. A partir dos discos de convergência é possível construir por um processo artesanal o domínio Ω de analiticidade de uma função. A figura (fig 3), página 21, mostra uma curva passando pelo centro de discos*

construir por um processo artesanal
o domínio de analiticidade de uma função

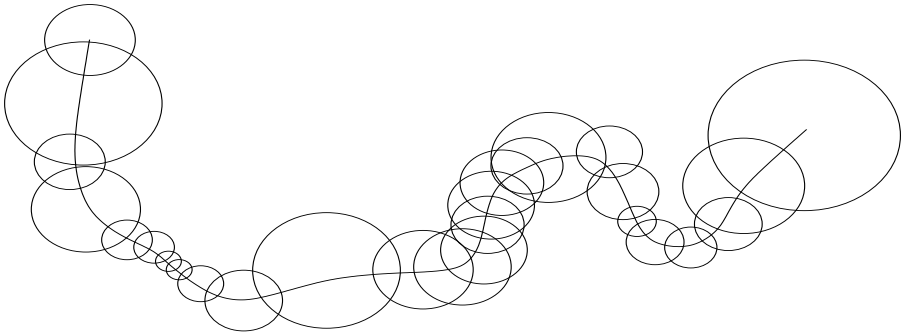

Figura 3:

que estão contidos no domínio de analiticidade da função analítica F, cada disco foi obtido calculando o raio de convergência da série.

Este método, apesar de extremamente ingenioso, conduz a uma teoria muito longa e difícil que foi, afinal, a história das funções analíticas, ou teoria das funções*. A figura (fig 3) mostra uma das construções típicas da teoria das funções a* expansão por analiticidade *do domínio duma função analítica F: sabendo que nalgum ponto da fronteira do disco de convergência a série de potência convergia, então era possível naquele ponto construir um disco de modo a obter mais um disco para expandir o domínio de analiticidade da função.*

A figura (fig. 2, página 19, dá um exemplo concreto *de que isto pode ocorrer, basta, por exemplo que F, no exemplo, tenha $\underline{a}$, como raiz.*

O lema de Abel garante a convergência no interior do disco de convergência sendo evasivo sobre o que acontece na fronteira.

A equação (eq. 77) passou a predominar a partir da década de 50, do século 20, como definição de função analítica e a equação (eq. 77) já traz uma proposta de domínio de analiticidade, que é o domínio Ω sobre cuja fronteira γ se vai usar a integral de Cauchy para definir uma função no interior de Ω que agora não precisa mais ser um disco. Na verdade a integral de Cauchy define as funções analíticas usando o fim da história *quando se percebeu que a* teoria das funções *nada mais era que a solução das equações de Cauchy-Riemann. Aliás, resolvendo e já explicitando um* problema de valor inicial *que é a função F definida na fronteira de Ω. Corrigindo: a medida que representa o valor na fronteira que em muitos dos casos particulares é uma função.*

Alguns exemplos

- a $exp(z) = e^z$ se define usando a *fórmula de Euler*,

$$e^z = e^{x+iy} = e^x e^{iy} = e^x(\cos(y) + i\sin(y))$$

e a derivada de e^z é $e^x(\cos(y) + i\sin(y)) = e^z$ usando as equações de Cauchy-Riemann. Exatamente como no caso real. Apenas a função exponencial é periódica na parte imaginária, o período é uma faixa do plano complexo com largura 2π.

- se $w = exp(z)$ então $z = log(w)$ fazendo do logaritmo uma função multivaluada cuja imagem deve ser restrita a uma faixa de largura 2π. A derivada do logaritmo pode ser obtida da mesma maneira como se faz no caso real:

$$z = e^w; w = log(z); h(z) = exp(log(z)) = z; \tag{95}$$
$$Dh(z) = 1 = e^w Dlog(z); Dlog(z) = \frac{1}{e^w} = \frac{1}{z}; \tag{96}$$

Exatamente como no caso real.

Mas como log é inverso de uma função periódica então se torna uma função multivaluada e uma solução para este "problema" é uma superfície de Riemann, ou alternadamente, para ficar dentro do contexto das variáveis complexas, considere o plano complexo com uma semirreta removida, na figura (fig 4), página 22, você vê a semirreta real negativa removida. Nesta semirreta removida é onde se

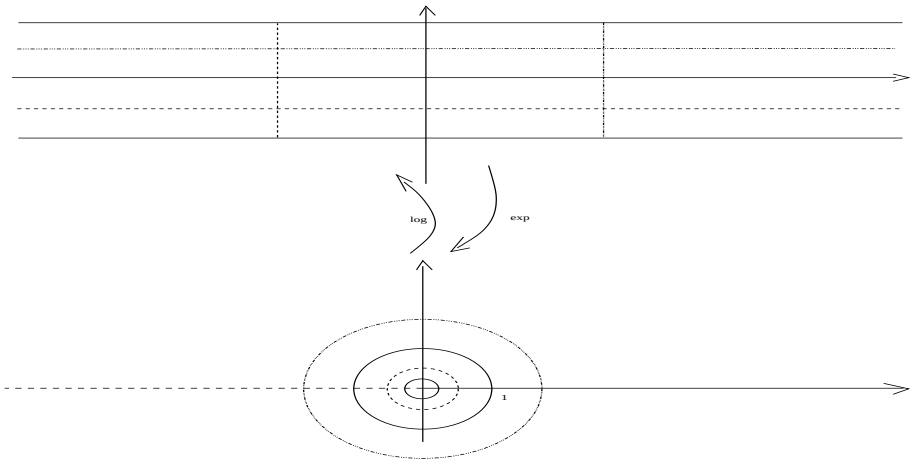

Figura 4: Definindo o logaritmo complexo

"colaria" uma folha da superfície de Riemann. Então o logaritmo complexo está definido no plano exceto em cima desta semirreta. O círculo trigonométrico tem como imagem o segmento $[-\pi, \pi)$ do eixo OY. Cada círculo com centro na origem corresponde a um segmento de reta "vertical" com medida unidimensional 2π na imagem. A cada semirreta partindo da origem, corresponde uma reta "horizontal" cuja altura é argumento que esta semirreta determina. Na figura (fig 5), página 23, você pode ver a imagem do círculo $\mathbf{S}^1 + \vec{a}; \|\vec{a}\| < 1$. Este círculo tangencia um pequeno círculo de centro zero (raio menor do que 1) e outro maior, de raio $1+\|\vec{a}\|$, consequentemente sua imagem irá tangenciar dois segmentos de reta verticais. Agora retiramos, por conveniência, a semirreta que se opõe ao vetor $\vec{a}$ cujo argumento é α. A reta vertical de altura α será o centro de simetria na imagem que pode ser

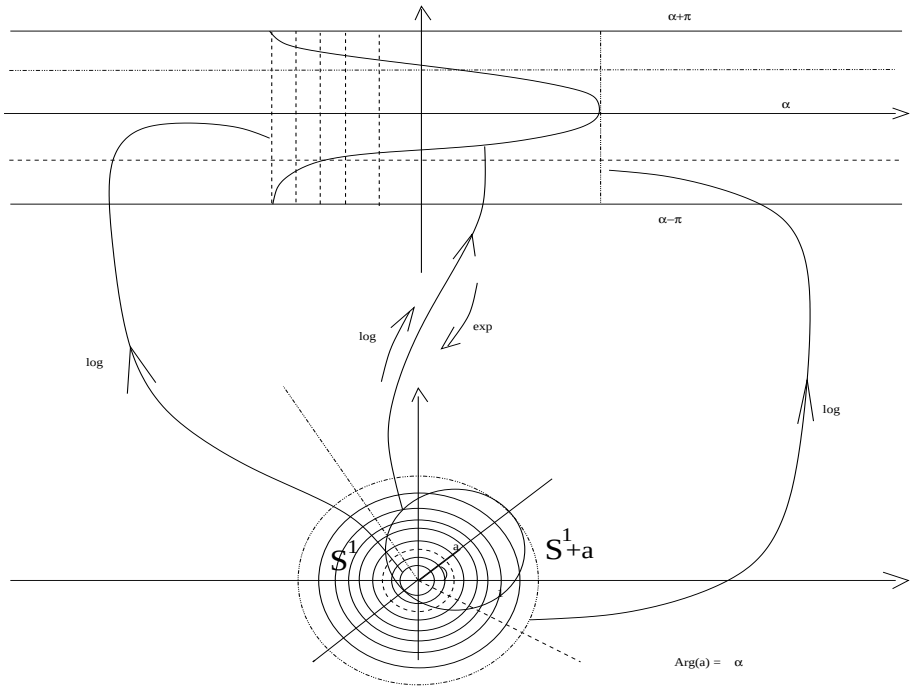

Figura 5: imagem de um círculo pelo logaritmo

vista na figura (fig 5), feita à mão usando `xfig`. O desenho está feito sem cuidados com escala, apenas mostra o comportamento da imagem de um círculo deslocado da origem.

A tangência com a imagem do círculo menor é particularmente interessante, ela se dá sobre a semirreta que foi retirada e seu efeito na imagem corresponde às tangências laterais em cada um dos extremos do segmento que é a imagem do círculo de menor raio.

A curva-imagem do círculo menor, prossegue para fora da faixa tangenciando a semirreta vertical que é imagem do círculo menor.

Esta é a metodologia para obter imagens via logaritmo tomando por base as imagens que posso obter com grande precisão, dos círculos centrados na origem e das semirretas partindo da origem. Com um programa de computador é possível obter imagens mais perfeitas.

Notação: $Arg(z) = Arg(e^z) = y$ e algumas vezes se identifica a *fórmula de Euler* com a *forma polar de um número complexo*.

- como $\mathbf{C}$ é um corpo os polinômios definem funções da mesma forma como no caso caso real. A derivada de z^n é nz^{n-1} como habitual e é a derivada complexa de z^n. Da mesma forma uma primitiva de z^n é $\frac{z^{n+1}}{n+1}$. Calcular a derivada passa pelas equações de Cauchy-Riemann com apoio do binômio de Newton, apenas um pouco trabalhoso.

- se $F|_\gamma$ for zero, na equação (eq. 77), concluímos que a função identicamente nula é analítica.

- suponha que γ seja o círculo trigonométrico, então Ω é o disco de raio 1 centrado na origem. Considere

$F|_{\mathbf{S}^1} = k \in \mathbf{R}$, quer dizer os valores na fronteira são constantes e iguais a k. O resultado devolvido pela (eq. 77) é k portanto qualquer função constante é analítica.

- Usando a linearidade da derivada se conclui que as expressões das derivadas e das integrais complexas para polinômios tem a mesma expressão formal para funções reais ou complexas.

- suponha que F, na fronteira de γ seja o polinômio $F(z) = z$. Vou mostrar que $g(a)$ definida pela equação (eq. 77) é $g(a) = a$ e portanto o polinômio do primeiro grau se estende a todo o domínio Ω. Vou fazer isto num caso particular e depois mostro como generalizar: $\Omega = U$ o disco unitário e $\gamma = \mathbf{S}^1$. O método que vou usar é um exemplo de como resolver problemas em casos particulares que permitam uma generalização.

  Quero calcular o valor de

$$g(a) = \frac{1}{2\pi i} \oint\limits_{\mathbf{S}^1} \frac{tdt}{t-a}$$

  Confira as contas, vou fazer os comentários depois.

$$a = \rho e^{i\alpha}; 0 < \rho < 1; \alpha = Arg(a); \tag{97}$$
$$\theta_1 = \alpha - \pi; \theta_2 = \alpha + \pi; \tag{98}$$
$$g(a) = \frac{1}{2\pi i} \oint\limits_{\mathbf{S}^1} \frac{tdt}{t-a} = \frac{1}{2\pi i}\left(S_1 - S_2\right); \tag{99}$$
$$S_1 = tlog(t-a)|_{\mathbf{S}^1} \tag{100}$$
$$S_2 = \oint\limits_{\mathbf{S}^1} log(t-a)dt \tag{101}$$
$$S_1 = e^{2\pi i} log(e^{2\pi i} - a) - e^{0i} log(e^{0i} - a) \tag{102}$$
$$S_1 = log(e^{2\pi i} - a) - log(e^{0i} - a) = 2\pi i; \tag{103}$$
$$S_2 = \left((t-a)log(t-a) - (t-a)\right)|_{\mathbf{S}^1} = \tag{104}$$
$$= \left((e^{2\pi i} - a)log(e^{2\pi i} - a) - (e^{2\pi i} - a) - (e^{0i} - a)log(e^{0i} - a) + (e^{0i} - a)\right) = \tag{105}$$
$$= (1-a)\left(log(e^{2\pi i} - a) - log(e^{0i} - a)\right) - 1 + 1 = \tag{106}$$
$$= (1-a)2\pi i + 0 = 2\pi i(1-a); \tag{107}$$
$$\frac{1}{2\pi i}\left(S_1 - S_2\right) = \frac{1}{2\pi i}\left(2\pi i + 2\pi i(1-a)\right) = \tag{108}$$
$$1 + (1-a) = a = g(a) \tag{109}$$

  Desta forma mostrei num caso particular que a integral de Cauchy reproduz a expressão que se espera para as funções analíticas polinomiais para todos os monômios z^n, e confira porque! $g(z) = z$ é a derivada de $G(z) = \frac{z^2}{2}$ e já verifiquei que a *integral de Cauchy* serve para calcular as derivadas... por indução tenho o caso para qualquer $n : g(z) = z^n$.

  Resta apenas um detalhe que não é imediato, a fórmula de Cauchy somente funciona dentro dum domínio Ω e os polinômios estão definidos no plano inteiro, são as funções *inteiras*, e vou deixar que a leitora encontre uma saída para este problema.

O índice dum ponto relativamente a uma curva

A fórmula, na equação (eq. 77), se chama *integral de Cauchy* e ela tem uma formulação pouco habitual para uma fórmula trazendo no primeiro membro $F(a)$ multiplicado por uma outra fórmula, $Ind_\gamma(a)$, o

índice do ponto $\underline{a}$ relativamente à curva γ. Isto se encontra ligado a um fenômeno muito particular das funções complexas, tirando as funções complexas complexas da forma $z \mapsto ax + b$ em que a, b são números complexos, todas as outras funções complexas transformam o plano complexo em *várias cópias dele mesmo*. Por exemplo, $z \mapsto z^2$ transforma $\mathbf{C}$ em duas cópias de $\mathbf{C}$, $z \mapsto z^3$ em três. E este número de vezes é a potência usada. Isto se encontra ligada ao número de soluções de uma equação polinomial. E o número $Ind_\gamma(a)$ entra, neste contexto, de forma bem significativa. Para entender isto deixe-me mostrar-lhe alguns exemplos.

1. Considere na *integral de Cauchy* F identicamente 1, a função constante 1, $a = 2$ e $\gamma = \mathbf{S}^1$, o círculo unitário. Acompanhe os cálculos:

$$\oint_\gamma \frac{dt}{t-a} = log(t-a)|_{\mathbf{S}^1} \tag{110}$$

   não dá para fazer isto aqui! na equação (eq. 110)

2.

Teorema de Cauchy-Goursat

Teorema 5 (Teorema de) *Cauchy-Goursat*
Seja F uma função analítica no domínio Ω e γ uma curva fechada de Ω então

$$\oint_\gamma F(z)dz = 0$$

Dem:
Expandindo $F(z)dz$ tem-se

$$\partial\Omega = \gamma; \tag{111}$$

$$F(z)dz = (u(z) + iv(z))(dx + idy) = u(z)dx - v(z)dy + i(u(z)dy + v(z)dx); \tag{112}$$

$$\int\int_\Omega (v_x + u_y)dxdy = 0 \text{ Cauchy-Riemann}; \tag{113}$$

$$\int\int_\Omega (v_y - u_x)dxdy = 0 \text{ Cauchy-Riemann}; \tag{114}$$

$$\oint_\gamma F(z)dz = \oint_\gamma u(z)dx - v(z)dy + i(u(z)dy + v(z)dx) = \tag{115}$$

$$= \int\int_\Omega (v_x + u_y)dxdy + i\int\int_\Omega (v_y - u_x)dxdy = 0 \tag{116}$$

a última igualdade é uma aplicação Teorema de Green.

q.e.d .

Teorema 6 (teorema de) *Morera*
Seja f uma função complexa contínua num domínio Ω tal que $\oint_\gamma f(z)dz = 0$ para qualquer curva fechada contida em Ω então f é analítica.

Dem:
A hipótese de continuidade é um detalhe sútil, se omitida, será possível produzir um salto em um ponto sobre alguma curva sobre a qual a integral ainda seria zero, mas f não seria analítica, uma descontinuidade restaurável que mostra ser necessário a hipótese de continuidade para completar o teorema de Morera para que ele seja o recíproco do teorema de Cauchy. Observação feita por C. O. Kiselman.

Também é uma aplicação do teorema de Green, a hipótese conduz à conclusão de que $f(z)dz$ é um diferencial exato logo a integral de f é independente de caminhos portanto tem uma primitiva F que tem uma derivada complexa que é f, portanto F é analítica e consequentemente também f.

q.e.d .

O teorema de Cauchy-Goursat não é exatamente a recíproca do teorema de Morera. Para obter o teorema de Morera é preciso a continuidade de f e como consequência f é analítica.

É interessante elaborar em cima da hipótese de continuidade do teorema de Morera pensando na equação (eq. 77). A função f que representa o *problema de valor na fronteira* pode ser descontínua ou mesmo ser uma medida, mas a extensão de f ao domínio Ω é obtida por convolução com uma função analítica. A razão da condição de *continuidade* no teorema de Morera é que ele simplesmente deixaria de ser verdadeiro porque posso ter duas funções *quase iguais*, uma analítica e a outra descontínua se eu retirar a condição de continuidade do teorema 6.

Esta observação generaliza o comentário dentro da demonstração do teorema de Morera: se duas funções diferirem num conjunto de *medida de Lebesgue* zero sobre uma curva fechada γ elas definem a mesma função analítica. Ou seja, a menos dum conjunto de medida zero, o teorema de Morera é a recíproca do teorema de Cauchy.

- **analítica, geometria** confira *geometria analítica*.

- **anel** é uma das *categorias da Álgebra* em que um conjunto A está associado a duas operações chamadas de *adição* e *multiplicação* tal que

- $(A, +)$ é um grupo comutativo.
- $(A, *)$ é um monoide, a multiplicação é uma operação binária associativa, que possui um elemento neutro, e se a multiplicação for comutativa se diz que o anel $(A, +, *)$ é comutativo.
- A multiplicação é distributiva relativamente à adição e o elemento neutro da adição anula todos os elementos do anel. Se houver um elemento neutro para multiplicação ele é usualmente designado pela letra e.

Notação: é cômodo se referir a um anel $(A, +, *)$ simplesmente usando o símbolo do conjunto A e vou usar este método sempre que não houver dúvida a respeito do que eu estiver descrevendo. As seguintes regras operatórias precisariam ser demonstradas, o que não vou fazer para não tornar a exposição pesada.

$$n \in \mathbf{Z}, a \in A; na \in A; na = a + a \cdots + a \text{n vezes}; \tag{117}$$

$$n, m \in \mathbf{Z}; a, b \in A; nmab = (na)(mb); \qquad z, y, z \in Ax - (y - z) = (x - y) + x; \tag{118}$$

Na verdade a *subtração* não está nem mesmo definida, mas é útil trabalhar com ela. Praticamente todas as expressões que valem para o anel $(\mathbf{Z}, +, \cdot)$ se aplicam para um anel qualquer com a restrição da comutatividade na multiplicação. Por exemplo a notação

$$\frac{a}{b}; a, b \in A; \tag{119}$$

em geral não tem sentido porque ela depende tanto da comutatividade como da existência dum inverso. A notação mista na dum elemento de A com um inteiro pode ser facilmente explicada considerando que $\mathbf{Z} \subset A$ em que via morfismo de anel

$$n \mapsto n * 1; 1 \in A; \tag{120}$$

a equação (eq.120) mostra que qualquer anel pode ser visto como um subanel de outro.

Dados dois anéis R, S é sempre possível estabelecer entre ele um morfismo de anel que é um método da categoria de anéis, confira a figura (fig 6). Os morfismos de anel preservam as operações de adição e multiplicação entre os dois anéis R, S.

Nesta exposição eu vou supor que você tem um conhecimento operatório da categoria dos grupos. Se não for o caso, não se assuste e procure adquirir este conhecimento, em paralelo, enquanto lê sobre a categoria de anel.

Exemplos

Exemplo 5 (o anel dos) *inteiros* $(\mathbf{Z}, +, *)$ $*$ *significa a multiplicação usual dos números inteiros, é formado do grupo aditivo dos inteiros com a adição, acrescentando-lhe a operação de multiplicar dos inteiros.*

Uma subestrutura importante nos anéis é um ideal. *Um ideal é um subconjunto dum anel que é subgrupo aditivo fechado para a multiplicação. Em geral se exige que seja um subconjunto próprio que não tenha a unidade, ou o elemento neutro da multiplicação porque o próprio anel é um ideal. Os ideais de* $\mathbf{Z}$ *são todos da forma* $n\mathbf{Z}$ *em que* $n \in Z$. *O caso trivial, quando* $n = 0$ *cria o ideal formado apenas pelo elemento zero.*

Como um ideal é um subgrupo do grupo aditivo do anel, então eu lhe posso aplicar os métodos da teoria do grupos *calculando, por exemplo o grupo quociente do anel por um ideal, aqui está a importância dos ideais para a estrutura de anel. Este processo permite descrever de forma muito bonita a aritmética contornando a divisão que é uma operação defectiva do conjunto dos números inteiros: ela não é comutativa, nem sempre está definida, tem elemento neutro mas não permite a definição do inverso relativamente à divisão.*

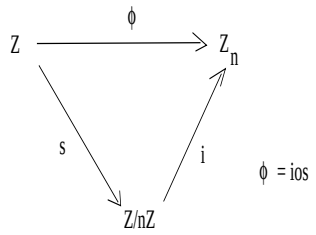

Figura 6:

Na figura (fig 6), página 27, você tem o grupo quociente $\mathbf{Z}/n\mathbf{Z}$ *e o morfismo canônico da estrutura quociente que é também um morfismos de grupos. Tem um morfismo de conjuntos entre o grupo quociente e o "*conjunto das etiquetas*" que marcam as classes quocientes que é o conjunto* $\mathbf{Z}_n$ *ao qual eu lhe posso atribuir, de forma natural, uma estrutura de grupo a partir da estrutura de grupo de* $\mathbf{Z}/n\mathbf{Z}$*, porque a seta* i *no gráfico da figura (fig 6) é uma bijeção, então o diagrama na figura (fig 6) é um* diagrama *da categoria de grupo, quer dizer que os "*lados*" do diagrama são morfismo da categoria de grupos, que eu agora vou mostrar que é um* diagrama *da categoria de anel.*

- *Primeiro vou expandir o morfismo de grupo para que se torne um morfismo de anel verificando que* $s(a * b) = s(a) * s(b)$.

- *Há* n *classes quocientes que são as possíveis translações de* $n\mathbf{Z}$ *que são*

$$n\mathbf{Z}, n\mathbf{Z} + 1, \ldots, n\mathbf{Z} + (n-1) \text{ porque } n\mathbf{Z} + n = n\mathbf{Z} \tag{121}$$

  ou seja existem tantas classes quocientes quantos sejam os restos na divisão por n *e* $n\mathbf{Z}$ *é o elemento neutro do grupo quociente. Os restos na divisão por* n *são as etiquetas que servem para dar nome às classes quocientes. Então*

$$\overline{0} = n\mathbf{Z}, \ldots, \overline{n-1} = n\mathbf{Z} + (n-1); \tag{122}$$

- *A imagem do elemento neutro da multiplicação por* s *é a classe* $n\mathbf{Z} + 1$ *porque*

$$(n\mathbf{Z} + 1) * (n\mathbf{Z} + a) = n\mathbf{Z} * n\mathbf{Z} + a * n\mathbf{Z} + n\mathbf{Z} + a = n\mathbf{Z} + a; \tag{123}$$

$$\mathbf{Z}_n = \mathbf{Z}/n\mathbf{Z} = \{n\mathbf{Z} + 0, \ldots, n\mathbf{Z} + (n-1)\}; \tag{124}$$

os conjuntos $n\mathbf{Z}*n\mathbf{Z}, a*n\mathbf{Z}$ são subconjuntos de $n\mathbf{Z}$, as três primeiras parcelas na equação (eq.123) são somas de subconjuntos e última parcela "a" é este elemento sendo somado aos três anteriores. Como as classes são disjuntas ao identificarmos um subconjunto de uma classe damos a classe como resposta da operação e assim $n\mathbf{Z}n\mathbf{Z} = n\mathbf{Z}$ que por sinal é o elemento neutro do grupo quociente, o zero, então $0 * 0 = 0$.

Uma outra maneira de fazer é uma demonstração direta de que

$$(\mathbf{Z}_n, +, *) \tag{125}$$

é um anel provando que a soma e o produto de restos é o resto do resultado destas operações na divisão por n. Mas acho que é uma forma mais límpida e elegante fazer uso do resultado da teoria dos grupos ou categoria de grupos e transportar o resultado para a categoria de anel como eu fiz.

Assim s é um morfismo de anel! E como i é uma identidade*, um* isomorfismo de conjuntos*, entre o conjunto das classes quocientes e as etiquetas que as identificam, fica definida de forma natural uma estrutura de anel no conjunto das etiquetas $\mathbf{Z}_n$ que é o conjunto dos restos na divisão por n fazendo também de i um isomorfismo de anel.*

O diagrama na (fig 6) é um diagrama *da categoria de anel, os três objetos ligados pelas setas são três objetos da categoria de anel e os lados do diagrama são morfismos de anel.*

A decomposição canônica *do morfismo de grupos de $\mathbf{Z}$ sobre o grupo dos quocientes na divisão por n, é ios a composição da sobrejeção canônica de $\mathbf{Z}$ no conjunto das classes quocientes obtidas quando se translada o ideal $n\mathbf{Z}$ e i com a injeção canônica que neste caso também é uma bijeção canônica do conjunto das classes quocientes no conjunto das etiquetas que marcam estas classes que são os restos na divisão por n. Tanto s como i são morfismos de grupo e agora, também, morfismos de anel.*

Ainda que defectiva, divisão em $\mathbf{Z}$ produz as estruturas de anéis finitos $(\mathbf{Z}_n; n \in \mathbf{Z}^+)$ formado dos restos na divisão pelo inteiro $n \geq 2$. Apenas é mais trabalhosa a demonstração de que as operações com restos produzem um resto da mesma classe de restos, ou ainda que $\mathbf{Z}_n$ é fechado para soma e produto, o que eu obtive diretamente da decomposição canônica do da estrutura de grupo e com a definição de $\mathbf{Z}_n$ como etiquetas das classes quocientes $\mathbf{Z}/n\mathbf{Z}$. Dizendo isto em outras palavras, adição de restos *é um* resto*, e, da mesma forma,* produto de restos *é um* resto*. Confira* anel finito*. São muito importantes estes anéis finitos quando n for um número primo porque eles são* corpos *e têm um importante papel em criptografia.*

Exemplo 6 (o caso dos restos) *Anel $\mathbf{Z}_n$*

Vou considerar dois casos: $n \in \{4, 5\}$.

- *O caso $n = 4$. As tabelas de das operações de adição e multiplicação do anel $\mathbf{Z}_4$ são*

+	0	1	2	3	*	0	1	2	3
0	0	1	2	3	0	0	0	0	0
1	1	2	3	0	1	0	1	2	3
2	2	3	0	1	2	0	2	0	2
3	3	0	1	2	3	0	3	2	1

Na tabela de multiplicação aparece um fenômeno típico da categoria de anel, os divisores de zero*, que é um dos nomes impróprios dentro do vocabulário matemático. É o caso quando $x * y = 0$ sem que nenhum dos dois fatores seja zero. Isto acontece porque $n = 4$ não é primo e os fatores de 4 são* "divisores de zero".

E o que eu construí, usando o anel quociente, significa que posso, primeiro calcular a adição, ou a multiplicação, e depois o resto, para obter o mesmo resultado que aparece nas tabelas de adição e multiplicação.

- *O caso $n = 5$. As tabelas de das operações de adição e multiplicação do anel $\mathbf{Z}_5$ são*

+	0	1	2	3	4	*	0	1	2	3	4			1	2	3	4
0	0	1	2	3	4	0	0	0	0	0	0		*				
1	1	2	3	4	0	1	0	1	2	3	4	1		1	2	3	4
2	2	3	4	0	1	2	0	2	4	1	3	2		2	4	1	3
3	3	4	0	1	2	3	0	3	1	4	2	3		3	1	4	2
4	4	0	1	2	3	4	0	4	3	2	1	4		4	3	2	1

Eu coloquei em destaque a tabela de multiplicação eliminando o zero, e você pode comparar as duas tabelas, de $\mathbf{Z}_4$ e $\mathbf{Z}_5$ para observar uma característica dos casos em que n for primo, tanto a tabela de adição quanto a de multiplicação, sem o zero, são tabelas de grupo. Isto faz de $\mathbf{Z}_5$ um corpo finito*. Como um número primo não tem divisores então quando n for primo se tem um anel sem* divisores de zero*, são corpos finitos.*

Exemplo 7 (anel) *de polinômios* *Se R for um anel posso construir o anel $R[x]$ formado dos polinômios com coeficientes em R. R é um subanel de $R[x]$ formado dos polinômios de grau zero. E você pode usar os anéis discutidos no exemplo anterior para produzir diversos exemplos do anel $R[x]$, com $R \in \{\mathbf{Z}, \mathbf{Z}_n\}$.*

Se R, S forem dois anéis e se for possível estabelecer entre eles um morfismo de anel

$$\phi : R \to S; \qquad \phi_* : R[x] \to S[x]; \tag{126}$$

$$(r_0, \ldots, r_n) \mapsto (\phi(r_0), \ldots, \phi(r_n)) \tag{127}$$

Confira a figura (fig. 7), página 43,

Estes anéis de polinômios são extremamente ricos. Eu vou dar um exemplo dos mais simples que serve para construir o *conjunto dos números complexos* usando o que fiz acima com na construção dos corpos finitos. O quociente dum anel por um ideal é um novo anel e agora aparecem dois conceitos de *ideal principal, ideal maximal*. É o caso dos corpos finitos na divisão por n quando o divisor for um número primo. Estes conceitos se confundem entre os ideais de $\mathbf{Z}$.

Dado um anel A e um seu subconjunto S o conjunto SA é um ideal de A e se um ideal for do tipo $I = SA$ com S unitário então I é um *ideal principal*. O conjunto dos ideais de A é parcialmente ordenado pela inclusão. Os *maximais* desta relação se chamam *ideais maximais*.

Se um ideal I for maximal então A/I é um corpo. Esta é uma forma bonita de construir $\mathbf{R}$ a partir das sucessões convergentes de números racionais que é um anel com c_0 das sucessões que convergem para zero sendo um *ideal maximal*. Se S for o anel das sucessões convergentes de números racionais, $S/c_0 = \mathbf{R}$. As sucessões convergentes são as sucessões de Cauchy.

Exemplo 8 (ideal principal) *Conjunto dos números complexos*

Outro exemplo interessante são os ideais do anel $\mathbf{R}[x]$ *dos polinômios com coeficientes reais. Dado* $P \in \mathbf{R}[x]$*,* $P\mathbf{R}[x]$ *é um ideal e se* P *não puder ser fatorado em* $\mathbf{R}[x]$ *então* $P\mathbf{R}[x]$ *é um ideal maximal, logo* $\mathbf{R}[x]/P\mathbf{R}[x]$ *é um corpo. O caso* $P(x) = x^2 + 1$ *gera* $\mathbf{C}$*.*

O polinômio $1 + x^2$ *não tem fatores no anel* $\mathbf{R}[x]$ *quer dizer que é um polinômio primo, neste anel. Qualquer polinômio de* $\mathbf{R}[x]$*, deixa um resto do primeiro grau na divisão por* $q(x) = 1 + x^2$*. Deixe-me escrever a expressão do* algoritmo da divisão euclidiana *para um polinômio* $P \in \mathbf{R}[x]$*:*

$$P(x) = q(x)Q(x) + a + bx; a, b \in \mathbf{R} \tag{128}$$

Se o grau de P *for menor do que 2, então* Q *é identicamente nulo e* P *é igual ao resto* $a + bx$*. Se o grau de* P *for maior do que 2, eu posso decompô-lo num múltiplo de* q *mais o resto na divisão por* q *portanto basta que eu discuta o que acontece com os polinômios do primeiro grau, os possíveis restos na divisão por* q*. Comparando com o que fiz com os anéis* $\mathbf{Z}_n$*, haverá "*tantas*" classes quantos forem os possíveis restos, quer dizer que as classes quocientes de*

$$\mathbf{R}[x]/(1 + x^2) \equiv \{(a, b) \in \mathbf{R}^2\}; \tag{129}$$

qualquer par $(a, b) \in \mathbf{R}^2$ *determina junto com um polinômio qualquer* $Q(x)$ *o dividendo a partir do* algoritmo da divisão euclidiana*. A equação (eq.129) é um isomorfismo de conjuntos que vou mostrar que é um isomorfismo entre o anel das classes quocientes e o o anel dos números complexos.*

E como fica a tabela de adição e multiplicação de restos. É fácil de calculá-la, neste caso, diretamente, acompanhe os cálculos na sequência de equações

$$p_1(x) = a_1 + b_1x, p_2(x) = a_2 + b_2x \in \mathbf{R}[x]; \tag{130}$$

$$p_1(x)p_2(x) = (a_1 + b_1x)(a_2 + b_2x) = a_1a_2 + (a_2b_1 + a_1b_2)x + b_1b_2x^2 = \tag{131}$$

$$= b_1b_2(1 + x^2) + (a_2b_1 + a_1b_2)x + a_1a_2 - b_1b_2x^2; \tag{132}$$

$$p_1(x)p_2(x) = b_1b_2(1 + x^2) + (a_2b_1 + a_1b_2)x + a_1a_2 - b_1b_2; \tag{133}$$

$$(a_1 + b_1i)(a_2 + b_2i) = (a_2b_1 + a_1b_2)i + a_1a_2 + b_1b_2i^2 = \tag{134}$$

$$a_1a_2 - b_1b_2 + (a_2b_1 + a_1b_2)i; \tag{135}$$

Da equação (eq.131) para a equação (eq.132) eu criei uma identidade algébrica para que aparecesse o algoritmo da divisão euclidiana em que o divisor é $q(x) = 1 + x^2$ *evidenciando o resto na divisão como aparece na equação (eq.133). Na equação (eq.134) eu substitui a variável* x *pelo número complexo* i *comparando a expressão do resto na equação anterior com a expressão do produto dos dois números complexos que aparece na equação (eq.135).*

Dividindo $p_1(x)p_2(x)$ *por* $1 + x^2$ *fica o resto*

$$a_1a_2 - b_1b_2 + (a_2b_1 + a_1b_2)x; \tag{136}$$

e compare com o produto de números complexos

$$(a_1 + b_1i)(a_2 + b_2i) = a_1a_2 - b_1b_2 + (a_2b_1 + a_1b_2)i; \tag{137}$$

Provei que o conjunto dos restos na divisão por $1 + x^2$ *se comporta na multiplicação como um produto de números complexos. Limitei-me ao caso em que estiver multiplicando dois polinômios do primeiro para simplificar as contas.*

O polinômio 1 *é a identidade no anel quociente e como* $1+x^2$ *não tem divisores no anel* $\mathbf{R}[x]$*, é um polinômio primo, não há divisores de zero neste anel. Basta-me mostrar que todo "*resto*" $a+bx$ tem um inverso para concluir que*

$$\mathbf{R}[x]/(1+x^2) \tag{138}$$

é um corpo porque é um anel sem divisores de zero em que todo elemento diferente de zero, tem inverso. Para calcular o inverso de $a+bx$*, eu vou resolver um sistema de equações, cujo determinante é diferente de zero, portanto tem solução e ela é única. Considere um par de inversos* $a+bx, c+dx$ *ao qual eu vou aplicar a multiplicação de restos.*

$$(a+bx)(c+dx) \equiv 1; \tag{139}$$

$$(ad+bc)x + ac - bd \equiv 1 = 0x + 1; \tag{140}$$

$$\begin{cases} ad+bc = 0 \\ ac-bd = 1 \end{cases} \tag{141}$$

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \begin{pmatrix} d \\ c \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \tag{142}$$

$$\det(\begin{pmatrix} a & b \\ -b & a \end{pmatrix}) = a^2+b^2; \tag{143}$$

$$d = \frac{-b}{a^2+b^2}; c = \frac{a}{a^2+b^2}; (c,d) = (\frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2}); \tag{144}$$

$$(c,d) = \frac{(a,-b)}{|(a,b)|^2} = \frac{\overline{(a,b)}}{|(a,b)|^2}; \tag{145}$$

O inverso do resto $c+dx$ *é o resto* $a+bx$ *que tem que ser diferente de zero, como também* $c+dx$*. O determinante igual a zero corresponderia ao resto* $a+bx = 0+0x$ *portanto a condição de que o determinante seja diferente de zero equivale a que* $a+bx \neq 0+0x$*, o resto nulo que é o único que não tem inverso multiplicativo.*

Corresponde com a álgebra dos números complexos em que o número complexo $a+bi$ *tem como inverso o número complexo* $c+di$

$$c+di; d = \frac{-b}{a^2+b^2}; c = \frac{a}{a^2+b^2}; \tag{146}$$

$$c+di = \frac{a-bi}{a^2+b^2} = \frac{\overline{a+bi}}{|a+bi|^2}; \tag{147}$$

$$z = c+di; w = a+bi; zw = 1; z = \frac{\overline{w}}{|w|^2}; \tag{148}$$

Conceitos relacionados:

- anel dos polinômios com coeficientes no anel A
- O anel $A[x]$

- **anel dos polinômios.** Se A for um anel, ou um corpo, as sucessões finitas dos seus elementos são os coeficientes dos polinômios com coeficientes em A. Eu gosto de pensar em polinômios como sucessões finitas de elementos dum anel porque a multiplicação de polinômios é exatamente o produto por convolução de duas tais sucessões. E a unidade no produto por convolução é a sucessão que tem um único termo no índice zero, a *delta de Dirac*. Esta forma de descrever $A[x]$ *aparentemente* entra em contradição com a habitual formulação dum polinômio como uma função da variável $x \in A$ portanto como uma função

definida em A e tomando valores em A. Do ponto de vista das operações o produto por convolução é o produto de polinômios e valem todas as propriedades da estrutura de anel com a unidade *delta de Dirac* e a soma de sucessões finitas sincronizadas a partir do índice zero:

$$P = (a_0, \ldots, a_n); Q = (b_0, \ldots, b_m); \tag{149}$$

$$P * Q_j = \sum_{j=0}^{k} a_{k-j} b_j; \tag{150}$$

$$H(x) = P * Q(x); H(x) = \sum_{k=0}^{n+m} c_k x^k; \tag{151}$$

$$c_k = \sum_{j=0}^{k} a_{k-j} b_j; \tag{152}$$

Ao multiplicar dois polinômios, P, Q tal que $H = P * Q$ o *algoritmo da multiplicação* consiste em arrumar os coeficientes, apenas os coeficientes, em duas linhas fazendo coincidir a_0, b_0 e produzindo m linhas, em que $m \leq n$ de modo que em cada coluna da matriz com formato dum losango com os lados de tamanho n fiquem paralelos à horizontal e tenham, em cada coluna os termos da soma

$$c_k = \sum_{j=0}^{k} a_{k-j} b_j; \tag{153}$$

que é o coeficiente de x^k.

Multiplique

$$\begin{cases} 1 + 3x + 5x^3 + 7x^5 \\ 2 + 5x + 8x^2 \end{cases} \tag{154}$$

e não se esqueça dos coeficientes nulos.

A equação (eq.152) ou (eq.153) define o termo de índice k da sucessão e se você acrescentar a *variável muda* x^k você tem a expressão usual do produto de polinômios como expressões na variável x. A variável x serve apenas para transformar a (eq.153) num produto de expressões algébricas. A equação (eq.153) lhe mostra o coeficiente do monômio x^k.

É um exercício no estudo da estrutura algébrica de anel o exemplo que $A[x]$ é um anel com unidade. A unidade é a `Delta de Dirac`, um nome pomposo para o polinômio constante $\delta_0(x) = 1$, e neste caso o *losango* se reduz a uma única linha na qual se encontram os coeficientes do outro polinômio.

O papel da variável x é apenas de transformar sucessão finita numa expressão algébrica de modo que o produto de tais expressões corresponda a convolução de sucessões finitas e historicamente foi assim que se definiram os polinômios. Mas também a expressão algébrica define uma função em A e tomando valores em A e há diversos aspectos da teoria em que esta versão é importante. Dependendo do momento, eu vou usar a formulação que for mais adequada.

Vou me especializar no caso em que A é um corpo caindo assim numa estrutura em que algumas propriedades vão se perder mas vou ganhar algumas e atingir um objetivo. Desta forma vou estudar o anel dos polinômios sobre um corpo K, o anel $K[x]$.

Uma primeira vantagem vem quando se pensa que $K \subset F$ em que F é um corpo que estende K. Nem toda equação polinomial com coeficientes em K, tem solução em K, como é o caso de $\sqrt{2} \notin \mathbf{Q}$ que é raiz do polinômio $x^2 - 2 \in \mathbf{Q}[x]$ ou $i \notin \mathbf{R}$, que é raiz do polinômio $x^2 + 1 \in \mathbf{R}[x]$. As equações polinomiais produzem estensões do corpo onde se encontram os coeficientes e este é o meu interesse neste texto.

Estes dois casos citados no parágrafo anterior são bem conhecidos e estudados e eu vou me aventurar para um caso menos comum. Deixe-me pensar em $K = Z_p$ quando p for um número primo, um corpo finito. Logo de partida tenho um "problema interessante", $Z_5 \not\subset Z_7$ e é fácil ver porque,

$$\text{em } Z_5,\ 2+3=0; 2+3 \neq 0 \text{ em } Z_7; \tag{155}$$

o que mostra que a adição de Z_5 não é compatível com a adição de Z_7. Este "problema" produz a pergunta *que corpo seria um super corpo de* Z_5? porque não pode ser nenhum dos Z_p. A saída é estudar $Z_5[x]$.

Deixe-me estudar no anel $Z_5[x]$ como uma equação polinomial poderia definir um *número algébrico* dum corpo estenda Z_5. Confira a definição de *número algébrico*, é a solução duma equação polinomial e todo elemento de Z_5 é um *número algébrico*, é solução duma equação do primeiro grau. Interessam-me os outros como $\sqrt{2}$ que é um número algébrico obtido como solução duma equação cujos coeficientes se encontram em $\mathbf{Q}$ mas que pertence a um corpo que estende $\mathbf{Q}$ que é $\mathbf{R}$.

Uma generalização bem interessante da *Aritmética*, que é uma teoria antiga, ainda da época da chamada matemática grega, que sob muitos aspectos foi copiada pelos gregos dos árabes ou dos chineses, feita em cima do anel $(\mathbf{Z}, +, \cdot)$. Conceitos como "primo" podem ser definidos no anel $K[x]$.

No anel $(\mathbf{Z}, +, \cdot)$ o conjunto $n\mathbf{Z}$ é um subgrupo, cujo quociente define um subgrupo finito $\mathbf{Z}_n$. No contexto de *anel* $n\mathbf{Z}$ se chama um *ideal*.

Definição 3 (ideal) *dum anel*
Um subgrupo I dum anel A é um ideal se $AI \subset I$. O próprio anel é um ideal não próprio, os ideais próprios são subconjuntos próprios de A.

Aproveitando da teoria dos grupos, A/I é um grupo e um anel, porque A é um grupo abeliano então I é grupo normal. O caso $\mathbf{Z}_p$ quando p é primo é interessante. $p\mathbf{Z}$ é *ideal maximal*, a relação de ordem definida pela inclusão não é total, há elementos que não são comparáveis, como $5\mathbf{Z}, 7\mathbf{Z}$, *ninguém está contido em ninguém*, mas nenhum ideal próprio contém estes ideais, eles são *maximais*, e quando isto acontece o quociente é um corpo: $\mathbf{Z}_5, \mathbf{Z}_7$. Para medir a importância deste resultado, deixe-me dar-lhe um exemplo bem conhecido, $(x^2+1)\mathbf{R}[x]$ é um ideal de $\mathbf{R}[x]$ e como não posso fatorar x^2+1 em $\mathbf{R}[x]$ então este ideal é maximal e produz o corpo $\mathbf{R}[x]/(x^2+1)$ das classes bilaterais deste ideal. A forma de obter as classes laterais é considerando os restos na divisão por x^2+1 que são os polinômios do primeiro grau $a+bx$. Se você escrever i em lugar de x vai obter os restos $a+bi$ que é a forma usual de escrever os números complexos, este corpo é $\mathbf{C}$.

Quero estudar os ideais de $\mathbf{Z}_5[x]$. Observe que $\mathbf{Z}_5[x]$ é o conjunto de todas as sucessões finitas de elementos de $\mathbf{Z}_5$, é o conjunto de todos os arranjos *com repetição* dos elementos de $\mathbf{Z}_5$. Esta caracterização vale para qualquer anel $K[x]$ em que K é o corpo de onde se tiram os coeficientes. Uma outra forma de falar é que são todas as sucessões finitas de elementos do corpo. Pensar em um polinômio "sem as variáveis" permite um linguagem mais simples... Outra forma de ver é que $\mathbf{Z}_5[x]$ é o anel dos polinômios com coeficientes em $\mathbf{Z}_5$ e com valores em $\mathbf{Z}_5$ e agora eu vou considerar que polinômios são funções da variável x.

Os grupos aditivos e multiplicativos do corpo $\mathbf{Z}_5$ são cíclicos, quer dizer um dado elemento gera o grupo, completamente, relativamente a operação do grupo. 2 e 3 geram $(\mathbf{Z}_5, +)$, as sucessivas somas destes elementos reproduzem todos os elementos de $\mathbf{Z}_5$. Eles também geram $(\mathbf{Z}_5, \cdot)$, sem o zero, como é habitual fazer-se com os reais na multiplicação porque 0 não tem inverso, porque, como números inteiros, eles são primos com 5.

Um elemento de $P(x) \in \mathbf{Z}_5[x]$ é dado por

$$x \equiv x^5, x^1 \ldots, x^9 \equiv x^5 \equiv x; \tag{156}$$

$$P(x) = a_0 + a_1 x + a_2 x^2 + a_3 x^2 + a_4 x^4 + \cdots + a_n x^n; \tag{157}$$

$$a_0, a_1, a_2, a_3, a_4, \ldots, a_n \in \mathbf{Z}_5; \tag{158}$$

$$x \in \{0,1,2,3,4\}; x^2 \in \{0,1\}; x^3 \in \{0,1,2,3,4\}; x^4 \in \{0,1\}; x^5 \in \{0,1,2,3,4\}; \tag{159}$$

$$x^6 \in \{0,1\}; x^7 \in \{0,1,2,3,4\}; x^8 \in \{0,1\}; x^9 \in \{0,1,2,3,4\}; \tag{160}$$

Eu descobri a progressão aritmética, nas potências da equação (eq.159) experimentalmente, logo lhe mostro abaixo como. Mas a razão é que são potências e o grupo multiplicativo tem quatro elementos, então

$$x^{n+4} = x^n; \tag{161}$$

Isto me sugere que os polinômios de $\mathbf{Z}_5[x]$ tenham apenas cinco coeficientes que correspondem aos monômios $1, x, x^2, x^3, x^4$.

Posso fazer a hipótese, e tenho que provar, x^n é periódica com período 4. E a prova é fácil

$$x \in \{0,1,2,3,4\} \text{ módulo } 5$$

então

$$\begin{cases} x \in \{0,1,2,3,4\} \text{ módulo } 4 \\ \overline{x}^n \in \{0,1,2,3,4\}, \{0,1,4\}, \{0,1,2,3,4\}, \{0,1\}, \\ \{0,1,2,3,4\}, \{0,1,4\}, \{0,1,2,3,4\}, \{0,1\}, \ldots; \end{cases} \tag{162}$$

na mesma ordem. Eu obtive esta sequência rodando o programa

```
define f(x,n) {return power(x,n)%5;}; ## calcula a classe mod 5
j=0;k=0; for(k=0;k<16;k++) {
  print k,'^','j = ','\{',;
  for(j=0;j<6;j++) print f(k,j),;
  print '\}'; }
0 ^ j =  { 0 0 0 0 0 }
1 ^ j =  { 1 1 1 1 1 }
2 ^ j =  { 2 4 3 1 2 }
3 ^ j =  { 3 4 2 1 3 }
4 ^ j =  { 4 1 4 1 4 }
5 ^ j =  { 0 0 0 0 0 }
6 ^ j =  { 1 1 1 1 1 }
7 ^ j =  { 2 4 3 1 2 }
8 ^ j =  { 3 4 2 1 3 }
9 ^ j =  { 4 1 4 1 4 }
10 ^ j =  { 0 0 0 0 0 }
11 ^ j =  { 1 1 1 1 1 }
12 ^ j =  { 2 4 3 1 2 }
13 ^ j =  { 3 4 2 1 3 }
14 ^ j =  { 4 1 4 1 4 }
15 ^ j =  { 0 0 0 0 0 }
```

Os elementos de $\mathbf{Z}_5[x]$, observe o que eu disse acima identificando polinômios com os seus coeficientes, são os arranjos com repetição dos elementos de $\mathbf{Z}_5$ e a quantidade destes arranjos é $3125 = 5^5$ portanto $\mathbf{Z}_5[x]$ "*teria*" 3125 polinômios diferentes. Mas eles não são todos diferentes e os testes feitos acima mostraram que há uma equivalência entre eles. Uma pista, $3125 = 5^5$ e eu *devo ter um divisor deste número* para a quantidade de polinômios que houver em $\mathbf{Z}_5[x]$.

Vou usar a notação da linguagem `C` porque vou raspar e colar num terminal rodando `calc` que usa a mesma sintaxe do `C`. Também vou usar as seguintes funções para testar os valores de um determinado polinômio

```
define g(x) {return P(x)%5;}  ### exibe a classe módulo 5
define P(x) {return
     x**2 + 3*x**3 + 2*x**4 + 4*x**5 + 3*x**6 + 2*x**7 + 3*x**8;}
for(i=0;i<10;i++) print g(P(i)), ###  mostra imagem de P
```

a definição de P vai mudar a cada teste, e o "`for`" está "*formatado*" para imprimir tudo numa única linha, é a razão da vírgula ao final. Você pode replicar o resultado aplicando este teste em um polinômio qualquer, desde que você escreva um par de polinômios equivalentes, e você pode se guiar pelos exemplos que estou dando.

$$
\left\{\begin{array}{l}
\left\{\begin{array}{l}
P(x) = x**2 + 3*x**3 + 2*x**4 + 4*x**5 + 3*x**6 + 2*x**7 + 3*x**8; \\
P(x) \in \{0, 3\};
\end{array}\right. \\
\left\{\begin{array}{l}
P(x) = 4*x + 4*x**2; \\
P(x) \in \{0, 3\};
\end{array}\right. \\
\left\{\begin{array}{l}
P(x) = 3*x + 3*x**2 + x**3 + 2*x**4 + 4*x**5; \\
P(x) \in \{0, 1, 2, 3\};
\end{array}\right. \\
\left\{\begin{array}{l}
P(x) = 3*x + 3*x**2 + x**3 + 2*x**4 + 4*x; \\
P(x) \in \{0, 1, 2, 3\};
\end{array}\right. \\
\left\{\begin{array}{l}
P(x) = x**2 + 3*x**3 + 2*x**5 + 4*x**7 + 3*x**9 + 2*x**11 + 3*x**19; \\
P(x) \in \{0, 3, 4\};
\end{array}\right. \\
\left\{\begin{array}{l}
P(x) = x**2 + x**3 + x**3; \\
P(x) \in \{0, 3, 4\};
\end{array}\right. \\
\left\{\begin{array}{l}
P(x) = x**3 + 3*x**5 + 2*x**7 + 4*x**9 + 3*x**11 + 2*x**13 + 3*x**15; \\
P(x) \in \{0\};
\end{array}\right. \\
\left\{\begin{array}{l}
P(x) = 4*x + 4*x**3; \\
P(x) \in \{0\};
\end{array}\right. \\
\left\{\begin{array}{l}
P(x) = x; \\
P(x) \in \{0, 1, 2, 3, 4\}
\end{array}\right. \\
\left\{\begin{array}{l}
P(x) = x**5 \\
P(x) \in \{0, 1, 2, 3, 4\}
\end{array}\right. \\
\left\{\begin{array}{l}
P(x) = x**2 \\
P(x) \in \{0, 1\}
\end{array}\right. \\
\left\{\begin{array}{l}
P(x) = x**6 \\
P(x) \in \{0, 1\}
\end{array}\right. \\
\left\{\begin{array}{l}
P(x) = x**3 \\
P(x) \in \{0, 1, 2, 3, 4\}
\end{array}\right. \\
\left\{\begin{array}{l}
P(x) = x**7 \\
P(x) \in \{0, 1, 2, 3, 4\}
\end{array}\right. \\
\left\{\begin{array}{l}
P(x) = x**4 \\
P(x) \in \{0, 1\}
\end{array}\right. \\
\left\{\begin{array}{l}
P(x) = x**8 \\
P(x) \in \{0, 1\}
\end{array}\right. \\
\left\{\begin{array}{l}
P(x) = x \\
P(x) \in \{0, 1, 2, 3, 4\}
\end{array}\right. \\
\left\{\begin{array}{l}
P(x) = x**9 \\
P(x) \in \{0, 1, 2, 3, 4\}
\end{array}\right.
\end{array}\right. \tag{163}
$$

Os testes feitos com `calc` foram

```
define  P(x) {return x;}
0 1 2 3 4 0 1 2 3 4 ;
define  P(x) {return x**5;}
0 1 2 3 4 0 1 2 3 4 ;
define  P(x) {return  x**2;}
0 1 1 1 1 0 1 1 1 1 ;
define  P(x) {return   x**6;}
```

```
0 1 1 1 1 0 1 1 1 1 ;
define  P(x) {return   x**3;}
0 1 2 3 4 0 1 2 3 4 ;
define  P(x) {return x**7;}
0 1 2 3 4 0 1 2 3 4 ;
define  P(x) {return x**4;}
0 1 1 1 1 0 1 1 1 1 ;
define  P(x) {return  x**8;}
0 1 1 1 1 0 1 1 1 1 ;
define  P(x) {return  x**9;}
;0 1 2 3 4 0 1 2 3 4 ;
define  P(x) {return x;}
0 1 2 3 4 0 1 2 3 4 ;
```

que mostra as equivalências entre monômios que usei na determinação das expressões equivalentes para os polinômios.

Voltando à análise de P, na equação (eq.163), é uma combinação linear, em $\mathbf{Z}_5$ dos elementos de $\mathbf{Z}_5$ então

$$(\forall x)(P(x) \in \mathbf{Z}_5); \tag{164}$$

mas um polinômio é uma lista finita qualquer de coeficientes então na verdade P é uma lista qualquer com n elementos, que é o grau do polinômio com coeficientes em $\mathbf{Z}_5$. Os polinômios do grau n serão todos os arranjos, com repetição, dos elementos do conjunto

$$\{0,1,2,3,4\}; \mathcal{A}_5^5 = 5^5$$

esta é a descrição dos coeficientes dos polinômios de grau n, para qualquer que seja n. Ou ainda, $\mathbf{Z}_5[x]$ é o conjunto de todos os arranjos com repetição dos elementos do conjunto

$$\{0,1,2,3,4\} = \mathbf{Z}_5$$

Mas a equivalência descoberta entre as potências me dizem que módulo uma relação de equivalência, são descritos pelos polinômios até o grau 4, uma vez que $x^5 \equiv x$. Confere com o que está dito acima, os polinômios de $\mathbf{Z}_5[x]$ tem exatamente 5 coeficientes tirados de $\mathbf{Z}_5$.

Então

$$x^2 + 1 = (x+a)(x+b) = x^2 + (a+b)x + ab; a+b = 0; ab = 1 \tag{165}$$

$$x^2 + 1 = (x+3)(x+2); (a,b) \in \{(2,3),(1,4)\}; \tag{166}$$

$$x^2 + 2 = (x+a)(x+b); (a,b) \in \text{ irredutível}; \tag{167}$$

$$(x^2+2)\mathbf{Z}_5[x] \text{ ideal maximal}; \qquad x^2 + 3 = (x+a)(x+b); (a,b) \in \text{ irredutível}; \tag{168}$$

$$(x^2+3)\mathbf{Z}_5[x] \text{ ideal maximal}; \qquad x^2 + 4 = (x+a)(x+b) = (x+1)(x+4); \tag{169}$$

São dois ideais impróprios, resta verificar quem são os ideais gerados por $j \in \{2,3,4\}$ cada um deles será o conjunto dos arranjos com repetição do conjunto $j\{0,1,2,3,4\}$

$$2 \mapsto \{0,1,2,3,4\}; 3 \mapsto \{0,1,2,3,4\}; 4 \mapsto \{0,1,2,3,4\}; \tag{170}$$

então o único ideal próprio, I, é o conjunto dos arranjos com repetição dos elementos do conjunto $\{0,2,4\}$. Ele é também maximal então as classes quociente por ele são o corpo $\mathbf{Z}_5[x]/I$ quer dos restos na divisão de um polinômio qualquer de $\mathbf{Z}_5[x]$ na divisão pelo polinômio.

Faço uma conjectura

$$2 + 4x \text{ é o polinômio mínimo de } I; \tag{171}$$

e justifico, se o primeiro coeficiente for 0 posso colocar x em evidência e não teria um *polinômio mínimo* porque seria divisível por x, seria um *polinômio redutível*. Então

$$a_0 + a_1x + a_2x^2 + a_3x^2 + a_4x^4 + a_5x^5/(2 + 4x) = \tag{172}$$

$$= q(x) + r(x); \tag{173}$$

$$(2 + 4x)\mathbf{Z}_5[x] = I = 2\mathbf{Z}_5[x] + 4x\mathbf{Z}_5[x] \tag{174}$$

- **ângulo** é um conceito típico da geometria euclidiana ainda que usualmente deixado pouco claro. Ângulo é um conceito plano, quer dizer de um espaço de dimensão dois porque representa um uma medida associada a dois segmentos de reta. Isto não me impede de falar de ângulo num espaço de dimensão maior apenas tudo vai se passar como se acontecesse dentro de um plano deste espaço.

Vou aqui definir ângulo como um número, é um número que mede um arco do círculo trigonométrico $\mathbf{S}^1$. Na figura (fig 8), página 39, você pode ver o ângulo α que a reta r faz com o eixo OX. Mas se considerarmos o *círculo trigonométrico*, $\mathbf{S}^1$ como um padrão, podemos simplificar a linguagem dizendo apenas o *ângulo da reta* r, querendo com isto dizer que colocamos o centro de $\mathbf{S}^1$ sobre a reta e encontramos o arco α determinado a partir da origem de $\mathbf{S}^1$ até o ponto em que r corta $\mathbf{S}^1$.

Vou abstrair o plano cartesiano e redefinir ângulo entre duas retas quaisquer usando uma representação de $\mathbf{S}^1$ no plano que estas duas reta determinam.

- Se os dois segmentos de reta forem paralelos, o ângulo entre eles é zero.
- Se os dois segmentos de reta não forem paralelos, então eles determinam um plano e suas retas suporte são concorrentes num ponto P e podemos traçar um círculo com centro em P sobre o qual as retas suporte determinam quatro segmentos de círculo iguais dois a dois. Considere P como a origem comum destas retas e o raio como sendo a unidade então o círculo considerado é unitário, $\mathbf{S}^1$. O menor segmento de círculo determinado pelas reta é o ângulo entre elas, determinando também a origem de $\mathbf{S}^1$.

Precisei criar a convenção de que o círculo traçado seria $\mathbf{S}^1$, o círculo unitário e este círculo tem um ponto inicial que é o ângulo zero. Se trata de uma *convenção*, ou uma *codificação*, escolhermos o *ponto inicial*, onde $\mathbf{S}^1$ corta o semieixo positivo horizontal, no caso do plano cartesiano, ou o ponto que vai determinar o menor segmento do círculo unitário quando estivermos determinando o ângulo entre duas retas quaisquer.

Como $\mathbf{S}^1$ tem raio 1, as coordenadas de qualquer ponto $p \in \mathbf{S}^1$ serão os números $\cos(\alpha), \sin(\alpha)$ do arco marcado a partir do *ponto inicial*. E isto funciona perfeitamente em qualquer plano do espaço em que as duas retas se encontrarem, um conceito plano, portanto.

$\mathbf{S}^1$ funciona como um *transferidor universal* para determinar ângulos: a medida dum arco determinado neste *transferidor*.

Ângulo é um número que fica no intervalo $[0, \pi)$ e diremos que duas retas são perpendiculares se determinarem o ângulo $\frac{\pi}{2}$, paralelas se se determinarem o ângulo 0. Podemos estender o conceito de ângulo ao perímetro do círculo trigonométrico e então seria um número no intervalo $[0, 2\pi)$.

Algumas vezes precisamos de estender ainda mais o conceito de ângulo então é um número real qualquer... medindo o perímetro de uma curva que envolva o círculo trigonométrico. Conceitos associados: *grau*, *número de voltas de uma curva*.

Se atribui a Euler a fórmula

$$P = (\cos(\alpha), \sin(\alpha)); P \in \mathbf{S}^1; \tag{175}$$
$$e^{i\alpha} = (\cos(\alpha) + i\sin(\alpha)) \equiv (\cos(\alpha), \sin(\alpha)); \tag{176}$$
$$e^{i\alpha}e^{i\beta} = e^{i(\alpha+\beta)} = (\cos(\alpha+\beta), \sin(\alpha+\beta)); \tag{177}$$
$$(\cos(\alpha) + i\sin(\alpha))(\cos(\beta) + i\sin(\beta)) = \tag{178}$$
$$= \cos(\alpha)\cos(\beta) - \sin(\alpha)\sin(\beta) + i(\cos(\alpha)\sin(\beta) + \sin(\alpha)\cos(\beta)) \tag{179}$$

que permite facilmente encontrar cosseno, seno e tangente dos arcos soma. Na equação (eq. 179) você

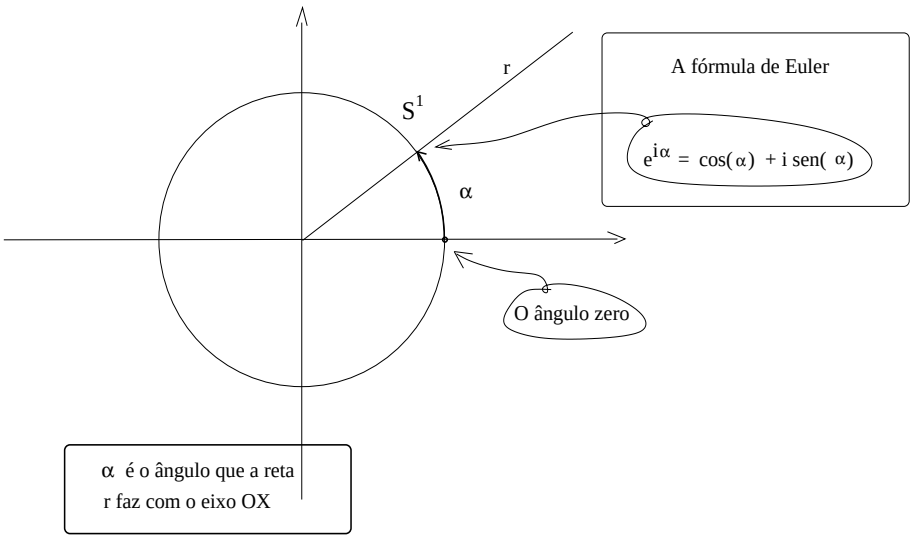

Figura 8: O ângulo da reta r

vê na primeira e na segunda coordenadas a expressão da soma de arcos para $\cos$ e $\sin$, respectivamente. Confira trigonometria.

Ao longo do tempo a Humanidade escolheu diversas formas como medição para arcos. Duas chegaram a até nós, o grau hexadecimal baseado numa divisão de $\mathbf{S}^1$ em 360 partes chamadas *grau* e a centesimal baseada numa divisão de $\mathbf{S}^1$ em 400 partes chamadas grau centesimal. Aqui estou falando da medida natural do ângulo, ou ainda chamada de $\pi-$radiano.

A *medida natural* é que melhor se adapta ao trabalho científico uma vez que é definida por uma medida tomada em cima de um padrão que é o *círculo trigonométrico*. Confira a tabela de equivalências entre estas três medidas para algumas medidas naturais bem conhecidas.

medida natural	grau hexadecimal	grau centesimal
0	0^o	0^o
$\frac{\pi}{4}$	45^o	50^o
$\frac{\pi}{2} = \frac{2\pi}{4}$	90^o	100^o
$\frac{3\pi}{4}$	135^o	150^o
$\pi = \frac{4\pi}{4}$	180^o	200^o
$\frac{5\pi}{4}$	225^o	250^o
$\frac{3\pi}{2} = \frac{6\pi}{4}$	270^o	300^o
$\frac{7\pi}{4}$	315^o	350^o
$2\pi = \frac{8\pi}{4}$	360^o	400^o

- **ângulo central**, na geometria euclidiana é o angulo determinado por dois vetores de mesmo módulo, $\vec{u}, \vec{v}$. Confira a figura (fig 10), página 41, e sua medida corresponde à medida do segmento equivalente

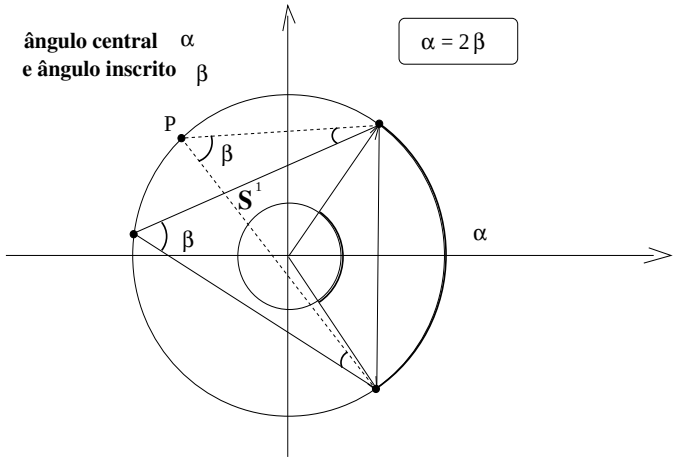

Figura 9: ângulo central

do círculo trigonométrico que as retas suporte destes vetores determinam. Na figura (fig 10), o círculo trigonométrico $\mathbf{S}^1$ está representando como um círculo de raio menor que o círculo determinado pelos dois vetores $\vec{u}, \vec{v}$. Confira também *ângulo inscrito*.

O ângulo inscrito mede a metade do ângulo central se ambos determinarem o mesmo arco de círculo.

- **ângulo inscrito**, na *geometria euclidiana* é o angulo determinado por dois segmentos de reta de mesma origem P, em que P é um ponto sobre um círculo.

A figura (fig 10), página 41 mostra um exemplo de *ângulo inscrito* β comparado com o correspondente *ângulo central*, α.

O *ângulo inscrito* mede a metade do *ângulo central* relativamente ao mesmo arco de círculo, confira a figura (fig 10).

Dem:

Dado um segmento dum círculo, considere a figura (fig 10), é possível ter-se-lhe associado um ângulo central α e uma infinidade de ângulos inscritos.

Para obter um ângulo inscrito, selecione um ponto no complemento do arco α e ligue-o aos extremos do segmento α do círculo.

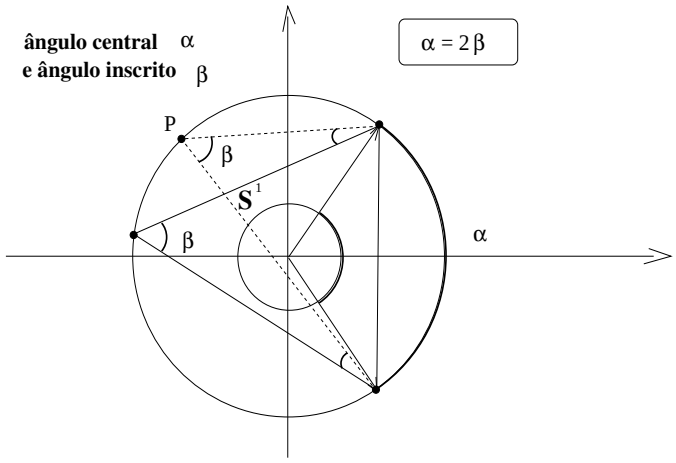

Figura 10: ângulo central

Vou mostrar que

- todos os ângulos assim obtidos são iguais ao ângulo β, confira a figura (fig. 10),
- $\beta = \frac{\alpha}{2}$.

Tire do ponto P uma perpendicular à mediatriz do ângulo inscrito γ determinando com a mediatriz um triângulo retângulo tendo um dos catetos com origem em P, $\overline{PQ}$, chame este triângulo *primeiro*.

A mediatriz de β sendo perpendicular à corda associado ao arco α determina dois triângulos retângulos um dos quais com o vértice P, chame este triângulo de *segundo* e considere o cateto $\overline{PM}$. As etiquetas "1"e "2"que identificam estes triângulos se encontram próximas das respectivas hipotenusas na figura (fig. 10).

Os triângulos retângulos *primeiro* e *segundo* são semelhantes porque

- O ângulo entre o cateto $\overline{PQ}$ sendo perpendicular à mediatriz de γ determina com a reta suporte do cateto $\overline{PM}$, do *segundo* triângulo, o mesmo ângulo entre as mediatrizes de β e γ.
-

Para demonstrá-lo vou colocar-me numa situação particular que em nada restringe a geral como depois vou deixar claro ao final.

Vou supor que o círculo na figura (fig. 11), página 42, é o círculo trigonométrico $\mathbf{S}^1$. Se considerar o arco α centrado em volta da origem de $\mathbf{S}^1$ então os extremos deste arco serão $\pm\frac{\alpha}{2}$.

O ponto P tem coordenadas $P = (\cos(\gamma), \sin(\gamma)); |\gamma| > \frac{\alpha}{2}$ e os vetores que determinam o ângulo inscrito no ponto P são, respectivamente

$$\begin{cases} u = (\cos(\gamma), \sin(\gamma)) - (\cos(\frac{\alpha}{2}), \sin(\frac{\alpha}{2})); \\ v = (\cos(\gamma), \sin(\gamma)) - (\cos(-\frac{\alpha}{2}), \sin(-\frac{\alpha}{2})); \end{cases} ; \tag{180}$$

$$\begin{cases} u = (\cos(\gamma) - \cos(\frac{\alpha}{2}), \sin(\gamma) - \sin(\frac{\alpha}{2})); \\ v = (\cos(\gamma) - \cos(-\frac{\alpha}{2}), \sin(\gamma) - \sin(-\frac{\alpha}{2})); \end{cases} \tag{181}$$

$$\begin{cases} u = (\cos(\gamma) - \cos(\frac{\alpha}{2}), \sin(\gamma) - \sin(\frac{\alpha}{2})); \\ v = (\cos(\gamma) - \cos(\frac{\alpha}{2}), \sin(\gamma) + \sin(\frac{\alpha}{2})); \end{cases} \tag{182}$$

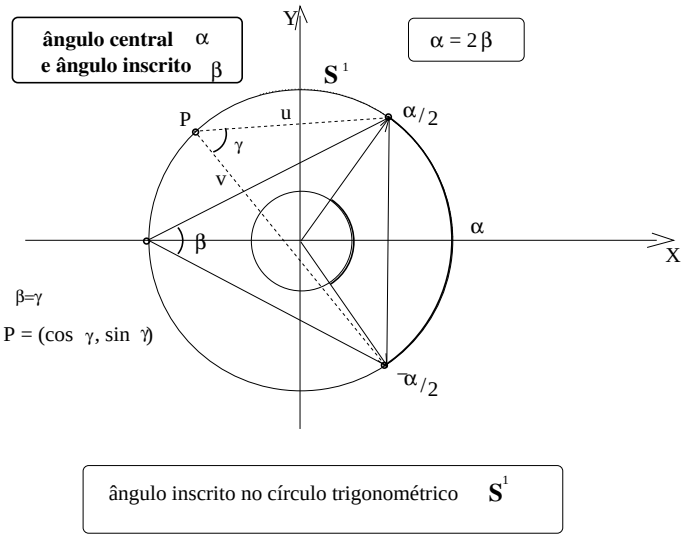

Figura 11: ângulo inscrito, círculo trigonométrico $\mathbf{S}^1$

O produto escalar entre estes vetores é

$$< u, v >= (\cos(\gamma) - \cos(\tfrac{\alpha}{2}))(\cos(\gamma) - \cos(\tfrac{\alpha}{2})) + (\sin(\gamma) - \sin(\tfrac{\alpha}{2}))(\sin(\gamma) + \sin(\tfrac{\alpha}{2})) \tag{183}$$

$$< u, v >= \cos^2(\gamma) + \cos^2(\tfrac{\alpha}{2}) - 2\cos(\gamma)\cos(\tfrac{\alpha}{2}) + \sin^2(\gamma) - \sin^2(\tfrac{\alpha}{2}); \tag{184}$$

$$< u, v >= 1 + \cos^2(\tfrac{\alpha}{2}) - \sin^2(\tfrac{\alpha}{2}) - 2\cos(\gamma)\cos(\tfrac{\alpha}{2}); \tag{185}$$

$$< u, v >= 1 + \cos(\alpha) - 2\cos(\gamma)\cos(\tfrac{\alpha}{2}); \tag{186}$$

$$< u, v >^2= 1 + \cos^2(\alpha) + 4\cos^2(\gamma)\cos^2(\tfrac{\alpha}{2}) + 2\cos(\alpha) - 4\cos(\gamma)\cos(\tfrac{\alpha}{2}) - 4\cos(\alpha)\cos(\gamma)\cos(\tfrac{\alpha}{2}); \tag{187}$$

$$< u, v >^2= \tag{188}$$

$$|u|^2 = (\cos(\gamma) - \cos(\tfrac{\alpha}{2}))^2 + (\sin(\gamma) - \sin(\tfrac{\alpha}{2}))^2; \tag{189}$$

$$|u|^2 = \cos^2(\gamma) + \cos^2(\tfrac{\alpha}{2}) - 2\cos(\gamma)\cos(\tfrac{\alpha}{2}) + \sin^2(\gamma) + \sin^2(\tfrac{\alpha}{2}) - 2\sin(\gamma)\sin(\tfrac{\alpha}{2}) \tag{190}$$

$$|u|^2 = 1 + 1 - 2cos(\gamma + \tfrac{\alpha}{2}); \tag{191}$$

$$|u|^2 = 2 - 2cos(\gamma + \tfrac{\alpha}{2}); \tag{192}$$

$$|v|^2 = (\cos(\gamma) - \cos(\tfrac{\alpha}{2}))^2 + (\sin(\gamma) + \sin(\tfrac{\alpha}{2}))^2 \tag{193}$$

$$|v|^2 = \cos^2(\gamma) + \cos^2(\tfrac{\alpha}{2}) - 2\cos(\gamma)\cos(\tfrac{\alpha}{2}) + \sin^2(\gamma) + \sin^2(\tfrac{\alpha}{2}) + 2\sin(\gamma)\sin(\tfrac{\alpha}{2}); \tag{194}$$

$$|v|^2 = 1 + 1 + 2\cos(\gamma + \tfrac{\alpha}{2}) = 2 + 2\cos(\gamma + \tfrac{\alpha}{2}); \tag{195}$$

$$\frac{<u,v>^2}{|u|^2|v|^2} = \frac{}{(2-2cos(\gamma+\frac{\alpha}{2}))(2+2\cos(\gamma+\frac{\alpha}{2}))} = \tag{196}$$

$$\frac{<u,v>^2}{|u|^2|v|^2} = \frac{}{4-4cos^2(\gamma+\frac{\alpha}{2})} = \tag{197}$$

$$\frac{<u,v>^2}{|u|^2|v|^2} = \frac{}{4\sin^2(\gamma+\frac{\alpha}{2})} \tag{198}$$

q.e.d .

- **animação** ou vídeo clips que podem ser feitos com *gnuplot*.

1. Faça um programa, em *gnuplot* ou n'outra linguagem de modo a criar uma sequência de imagens do tipo `.gif`, este tipo de imagem funciona com *gnuplot*. Você deve ter o cuidado de dar nomes

aos arquivos de modo que eles fiquem em ordem alfabética e isto é possível fazer com *gnuplot*, um exemplo é `TaylorPolinomioTres.gnuplot`.

2. Depois abra os arquivos com no método de `arquivos` do `gimp`, parece-me que infelizmente é preciso selecionar todos usando `shift` e seguir com a `seta`.

3. quem reproduz é um `filtro`, abra este método e selecione `reproduzir`.

- **antecedente** numa implicação $A \implies B$ B é o consequente e A é o antecedente.

- **apótema** é um dos itens que está ligado ao triângulo que determina o ângulo central α no círculo de raio r.

Confira a figura (fig 13), página 46,
em que estas três noções da geometria, *apótema*, *corda* e *arco* estão ilustradas no caso dum polígono regular convexo com $n = 6$ lados. Para qualquer outro polígono com n lados você pode diretamente substituir tudo que eu aqui disser porque vale para n qualquer. Uma das importâncias do *apótema* reside no fato de que ele me permite deduzir a área dum polígono regular convexo dado n e o raio, r, do círculo em que ele pode ser inscrito. Depois, um *limite notável* vai me permitir de deduzir a área do círculo de r da fórmula da área dum polígono de n lados inscrito no círculo de raio r.

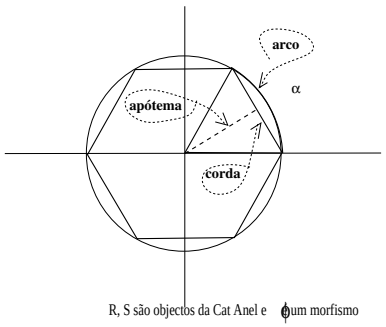

Figura 12: apótema e a corda

$$\text{ângulo central } \alpha = \frac{2\pi}{n}; \tag{199}$$

$$\text{lado do polígono } l = 2r\sin(\tfrac{\pi}{n}); \tag{200}$$

$$\text{apótema } a = r\cos(\tfrac{\pi}{n}); \tag{201}$$

$$\text{área do triângulo } = A = r\cos(\tfrac{\pi}{n})2r\sin(\tfrac{\pi}{n})/2 = \tag{202}$$

$$= r\cos(\tfrac{\pi}{n})r\sin(\tfrac{\pi}{n}) = r^2\cos(\tfrac{\pi}{n})\sin(\tfrac{\pi}{n}) = \tag{203}$$

$$= \frac{r^2\sin(\frac{2\pi}{n})}{2}; \tag{204}$$

$$\text{área do polígono } \frac{nr^2\sin(\frac{2\pi}{n})}{2}; \tag{205}$$

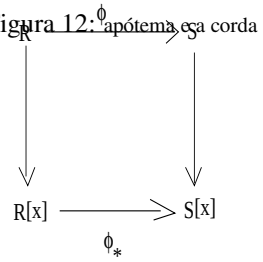

Figura 7:

Na equação (eq.200) e usei a metade do ângulo central para obter a metade do lado e assim obter o valor de l multiplicando por dois.

Na equação (eq.201) e usei a metade do ângulo central para obter a altura do triângulo que é o *apótema*.

Na equação (eq.203) eu posso identificar o *seno do arco* α porque tenho uma expressão do tipo $\cos(\beta)\sin(\beta); \beta = \frac{\pi}{n}$ o que me permite substituir este produto pelo $\frac{\sin(\alpha)}{2}$ o que fiz na equação (eq.204). Na equação (eq.205) em multipliquei por n, o número de triângulos do polígono, para obter a área do polígono regular convexo de n lados.

Como $n\sin(\frac{1}{n})$ é um *limite notável* e vale 1 quando $n = \infty$ então eu posso deduzir da equação (eq.205) o valor da área círculo de raio r usando este limite para obter

$$n\frac{r^2\sin(\frac{2\pi}{n})}{2} \longrightarrow \pi r^2 \tag{206}$$

Você pode calcular este limite, com uma pequena transformação, usando a *regra de L'Hôpital*.

- **aproximação** É um método pelo qual construímos objetos, dentro de um conjunto (ou espaço), que representam um outro objeto com um erro aceitável.

Por exemplo, $\sqrt{2}$ não é um número racional, o que significa que

$$\sqrt{2} \neq \frac{p}{q}; \tag{207}$$

não existe nenhuma fração que *represente* $\sqrt{2}$. E as frações são números exatos, mesmo frações do tipo

$$\frac{1}{3} = 0.333(3) \tag{208}$$

que é uma *dízima periódica*, ainda assim ela tem uma representação que eu posso usar *exatamente* nas contas, e isto é coisa que eu não posso fazer com $\sqrt{2}$. Se você digitar $\sqrt{2}$ numa máquina de calcular você vai ver no visor algo do tipo

$$1.4142135623730950488\ldots \tag{209}$$

isto se for uma calculadora potente...com 19 dígitos significativos que é o significado das reticências "*e continua*"...

A calculadora *fez uma aproximação de* $\sqrt{2}$, quer dizer, ela *representou* $\sqrt{2}$ com um número racional que é um tipo de número como aquele *número racional*, uma *dízima periódica*, que aparece na equação (eq.209).

$\sqrt{2}$ não é uma *dízima periódica*, é uma *dízima não periódica*, e a calculadora apresentou uma aproximação de $\sqrt{2}$ como número racional. Todos os números com que você pode fazer contas num computador são números racionais muitos dos quais estão criando uma representação racional de alguma dízima não periódica como $\sqrt{3}, \sqrt{5}, \pi, \ldots$

Um outro exemplo é a imagem transmitida à distância que não corresponde a uma cópia exata do objeto captado, há um erro que é consequência da necessidade que temos de considerar apenas uma quantidade finita pixeis (no caso da imagem) para compor a *representação* do objeto no espaço de chegada.

Mas um outro exemplo é o número π, que é obtido, aproximadamente, quando consideramos o quociente entre o perímetro de um polígono regular convexo com n lados inscrito no círculo unitário dividido pelo diâmetro que mede 2. O resultado deste quociente é uma aproximação de π. Maior o número n de lados, melhor a aproximação obtida de π.

π, $\sqrt{2}$, são dois números irracionais com os quais somente podemos trabalhar usando uma *representação* racional.

Todos os exemplos numéricos que dei acima são números reais e o conjunto dos números reais é uma ótima fonte de exemplos de *aproximação*. $\mathbf{R}$, o conjunto dos números reais se divide em duas grandes classes, os *decimais periódicos*, que são os números racionais, os números da forma $\frac{p}{q}$ em que p, q são inteiros com a restrição de que o denominador não pode ser zero, e os *decimais não periódicos*, que são os números irracionais, aqueles que não podem ser expressos como uma fração. $\pi, \sqrt{2}$ são *decimais não periódicos*.

Aproximação em espaços de funções

Um outro exemplo de *aproximação* fica dentro da Álgebra Linear. Considere dois espaços vetoriais E, F. Se E for *dimensão infinita* e F for de *dimensão finita* então *existe uma imagem isomorfa de* F *em* E que vou seguir chamando de F porque são dois espaços vetoriais isomorfos e *isomorfismo* é uma relação de equivalência. A transformação linearemphdimensão!infinita

$$\mathcal{P} : E \to F; \mathcal{P}(\mathcal{P}(x)) = x; \tag{210}$$

é única e se chama de *projeção* de E em F. Então, dado qualquer vetor de $x \in E$ a imagem $\mathcal{P}(x)$ é uma *aproximação* em dimensão finita de x. Este exemplo é bem semelhante ao da transmissão da imagem até porque se trata da projeção num espaço vetorial de *dimensão finita* dum objeto que pertence a um espaço de *dimensão infinita*. Deixe-me explicar o "*por quê*" da diferença entre as dimensões.

Você certamente já ouviu falar de que as imagens são *vetoriais* quer dizer, uma imagem é um vetor, uma sucessão de dígitos. Deixe-me introduzir uma terminologia para facilitar a conversa e chamar de *imagem original* o objeto real que está sendo fotografado ou filmado, que é a *imagem real*. Ele é uma *dízima*... que pode ser não periódica, mas o que vai ser transmitido é uma *dízima periódica* que dizer que sequências de dígitos vai ser cortada num certo momento, vai se produzir uma *aproximação*. Uma imagem é uma sequência de dígitos, um vetor e o que você na tela do computador, ou da máquina fotográfica, é uma aproximação da realidade e basta que você dê um *zoom* e logo você passa a ver quadrados que são os pixeis de que está formada a *imagem aproximada*.

Outro exemplo de projeção são os polinômios de Taylor, então $\mathcal{P}(f)$ é o *polinômio de Taylor* de ordem n da função diferenciável pelo menos n vezes e neste caso E é o espaço de dimensão infinita das funções n vezes diferenciáveis. A *imagem real* é uma *série de Taylor* que pode nem existir, e o *polinômio de Taylor* é a *imagem aproximada*.

Outro exemplo de projeção são os polinômios trigonométricos de funções contínuas definidas no intervalo $[0, 2\pi]$. Um *polinômio trigonométrico* é uma reduzida de ordem n da série de Fourier duma função contínua definida no intervalo $[0, 2\pi]$. Obviamente, o intervalo pode ser genérico $[a, b]$ com a fórmula para o cálculo dos coeficientes de Fourier específica para este intervalo. A *imagem real* é uma *série de Fourier* é o *polinômio de trigonométrico* é a *imagem aproximada*.

Conceitos relacionados:

- *projeção*, é uma transformação linear dum espaço vetorial E noutro espaço vetorial F tal que $E \subset F$, como os $\mathbf{Q} \to \mathbf{R}$.
- *aproximação de funções*, *polinômio de Taylor* e *polinômio trigonométrico* são projeções em espaços de séries de funções. Confira *polinômio de Taylor* e *polinômio trigonométrico*
- splines, são polinômios por pedaços que de uma certa forma generalizam os polinômios de Taylor, mas produzem diretamente como imagem um elemento dum espaço de funções diferenciáveis definidas num determinado intervalo $[a, b]$, confira *splines*.

- **arco** é um dos itens que está ligado ao triângulo que determina o ângulo central α no círculo de raio r.

Confira a figura (fig 13), página 46,

em que estas três noções da geometria, *apótema*, *corda* e *arco* estão ilustradas no caso dum polígono regular convexo com $n = 6$ lados. Para qualquer outro polígono com n lados você pode diretamente substituir tudo que eu aqui disser porque vale para n qualquer. Uma das importâncias do *apótema* reside no fato de que ele me permite deduzir a área dum polígono regular convexo dado n e o raio, r, do círculo em que ele pode ser inscrito. Depois, um *limite notável* vai me permitir de deduzir a área do círculo de r da fórmula da área dum

polígono de n lados inscrito no círculo de raio r.

$$\text{ângulo central } \alpha = \tfrac{2\pi}{n}; \tag{211}$$

$$\text{lado do polígono } l = 2r\sin(\tfrac{\pi}{n}); \tag{212}$$

$$\text{apótema } a = r\cos(\tfrac{\pi}{n}); \tag{213}$$

$$\text{área do triângulo } = A = r\cos(\tfrac{\pi}{n})2r\sin(\tfrac{\pi}{n})/2 = \tag{214}$$

$$= r\cos(\tfrac{\pi}{n})r\sin(\tfrac{\pi}{n}) = r^2\cos(\tfrac{\pi}{n})\sin(\tfrac{\pi}{n}) = \tag{215}$$

$$= \tfrac{r^2\sin(\frac{2\pi}{n})}{2}; \tag{216}$$

$$\text{área do polígono } \tfrac{nr^2\sin(\frac{2\pi}{n})}{2}; \tag{217}$$

Na equação (eq.212) e usei a metade do ângulo central para obter a metade do lado e assim obter o valor de l multiplicando por dois.

Na equação (eq.213) e usei a metade do ângulo central para obter a altura do triângulo que é o *apótema*.

Na equação (eq.215) eu posso identificar o *seno do arco* α porque tenho uma expressão do tipo $\cos(\beta)\sin(\beta); \beta = \frac{\pi}{n}$ o que me permite substituir este produto pelo $\frac{\sin(\alpha)}{2}$ o que fiz na equação (eq.216). Na equação (eq.217) em multipliquei por n, o número de triângulos do polígono, para obter a área do polígono regular convexo de n lados.

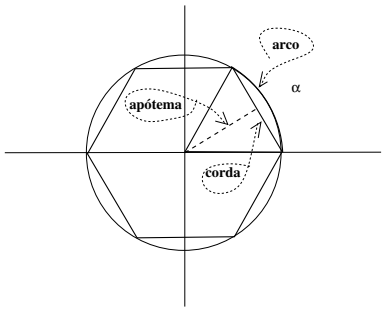

Figura 13: apótema e a corda

Como $n\sin(\frac{1}{n})$ é um *limite notável* e vale 1 quando $n = \infty$ então eu posso deduzir da equação (eq.217) o valor da área círculo de raio r usando este limite para obter

$$n\frac{r^2\sin(\frac{2\pi}{n})}{2} \longrightarrow \pi r^2 \tag{218}$$

Você pode calcular este limite, com uma pequena transformação, usando a *regra de L'Hôpital*.

- **<u>área</u>** é um tipo de medida, a medida das *variedades de dimensão dois*, as superfícies, as figuras geométricas planas, polígonos, por exemplo. Dizer *das variedades de dimensão 2* é mais abrangente, porque inclui as superfícies dos corpos dos espaços de dimensão três. Este conceito nos auxilia a sair da *prisão tridimensional* em que a *geometria euclidiana* nos confina. Vou usar o palavra *variedade* para *infiltrar, subversivamente*, este conceito no vocabulário popular de quem estuda Matemática, entenda *variedade* como sinônimo de *objeto geométrico*.

A área básica da qual as demais <u>todas</u> são deduzidas, é de um quadrado do plano, que estabelece como padrão de unitário de área, esta é a ideia do sistema métrico universal, produto da Revolução Francesa. Em seguida, qualquer *objeto geométrico* é comparado com este quadrado padrão sendo sua área obtida pelo "método da contagem", quantas vezes o quadrado padrão estiver contido no *objeto* cuja área eu desejo medir. Obviamente este número pode ser fracionário ou mesmo um número não racional.

A área padrão é dum retângulo de lado 1.

E por consequência os ingleses insistem em ignorar e manter o arcaico sistema que eles chamam de *imperial*

Deixe-me ser mais claro: as únicas áreas que nós sabemos calcular são as área de retângulos. As outras <u>todas</u> são obtidas por dedução geométrica como as áreas dos paralelogramos, dos losangos e dos triângulos.

A área dos retângulos é definida como o *produto* das *medidas dos lados*. Se estes números forem inteiros, o resultado da medida "*conta*" quantas vezes o quadrado padrão está contido no retângulo. Se algum dos *multiplicandos* não for inteiro, a multiplicação representa uma generalização da *contagem*.

Cabe lembrar o significado do *produto de números* como soma repetida:

$$3 \times 4 = 4 + 4 + 4 = 3 + 3 + 3 + 3; \tag{219}$$

e continua válido mesmo que os números sejam fracionários:

$$3,5 \times 4 = 4 + 4 + 4 + \frac{4}{2} = 4 + 4 + 4 + 2 = (3 \times 4) + (0,5 \times 4) = 12 + 2; \tag{220}$$

A área dos retângulos segue o mesmo princípio da *contagem de ovos* numa cartela: você conta a quantidade de ovos na base, conta as fileiras que tiver em paralelo com a base, e finalmente multiplica estas duas quantidades.

No caso da área dos retângulos precisamos das medidas dos lados, são os comprimentos de segmentos de reta é um outro tipo de medida, neste caso das *variedades* de dimensão 1. Comprimento dos segmentos de reta é a distância entre os pontos que definem o segmento. Então a área dum retângulo é o produto destas duas medidas: *medida da base* X *medida da altura*. Confira a figura (fig 14), página 47.

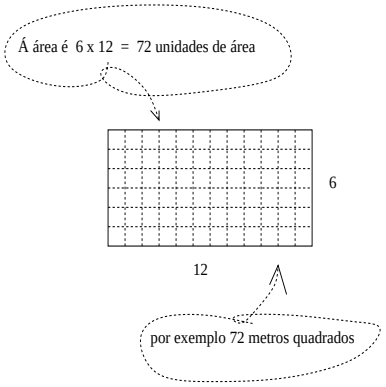

Figura 14:

O passo seguinte é a área de losangos, que é *base* X *altura*. A base é qualquer dos lados, e altura é o comprimento do segmento de reta que for baixado perpendicularmente à base, ou sua extensão, a partir dum vértice que não esteja na base. Confira a figura (fig 15), página 47. É um teorema da geometria que o resultado é independente da escolha do lado que você quiser considerar como base.

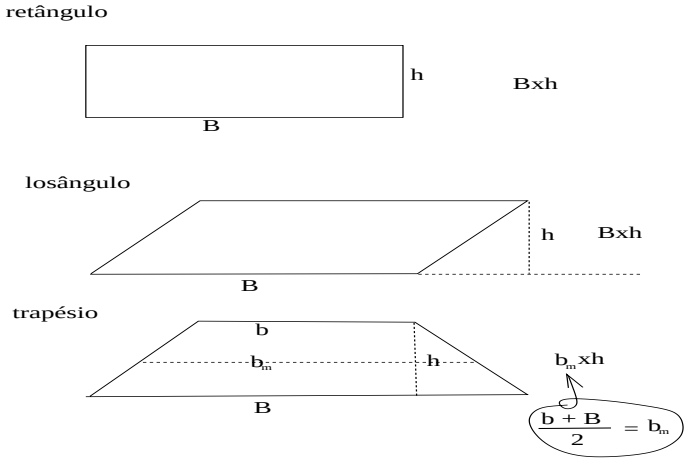

Figura 15: retângulo, losango, trapézio

A figura (fig 15), página 47. mostra como se faz o cálculo da área das figuras geométricas planas, básicas, retângulo, losango e trapézio. Nelas se identifica a altura, h e a base, B sendo a área ao produto $B \times h$ que "*conta*" quantos quadrados unitários ficam contidos na figura.

Num losango, a altura é calculada relativamente ao lado que for considerado a base. No trapézio, se calcula uma *base média* $b_m = \frac{B+b}{2}$ que corresponde a transformar o trapézio num retângulo se você cortar o triângulo excedente, como aparece na figura (fig 15) e colocá-lo na outra ponta. O resultando seria uma retângulo cuja base é a *base média*.

Área dum triângulo é a metade da área do losango que é possível construir com ele, replicando-o. Na figura (fig 16), página 48, você vê o processo de construção dum losango a partir dum triângulo, copiando,

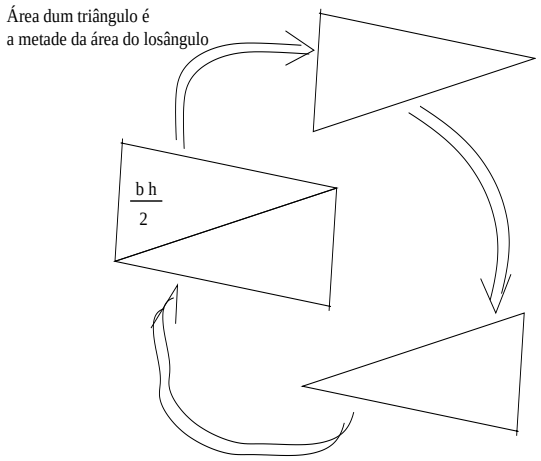

Figura 16: área dum triângulo e do losango

rodando, transladando, ou apenas usando régua e esquadro. Então a área do triângulo é a metade da área do losango que é *base* X *altura*, $\frac{bh}{2}$, a metade do produto da base pela altura. A altura pode ser a medida de qualquer segmento baixado dum vértice perpendicularmente ao lado que não contém o vértice. É um teorema que precisa ser demonstrado: *que o resultado não depende da escolha do vértice*, um teorema da geometria. Mas demonstração é simples, e a figura (fig 17), página 49, lhe mostra duas maneiras de construir um losango a partir dum triângulo qualquer usando régua e esquadro para produzir dois lados paralelos.

A área dum quadrilátero qualquer será obtida subdividindo-o em triângulos e losangos. Há alguns casos particulares em que podemos obter fórmulas diretas, como é o caso dos trapézios em que se calcula uma *base média* ou *altura média* para multiplicar pela altura ou base. Fixando o conceito de *base média*, como o valor médio dos comprimentos das bases, e "*bases*" são os dois lados paralelos. Calcula-se a altura de modo semelhante como descritos nos casos acima, é o comprimento do segmento de reta traçado perpendicularmente entre as "*bases*", e a área é o produto da altura pela *base média*.

A área dos demais polígonos é obtida pela decomposição deles em triângulos ou losangos.

Se uma figura plana não for um polígono, se tiver *lados* curvos, a área somente pode ser calculada *aproximadamente*. E agora estou mencionando outro conceito, "*aproximação*". Dificilmente conseguimos calcular qualquer coisa *exatamente*. Falar em fazer cálculos exatos é um preconceito inútil. Com *cálculos aproximados* se colocam os satélites em órbita.

Há alguns casos em que se conhecem fórmulas para o cálculo, como é o caso do círculo ou de partes dum círculo. Confira as figuras específicas e a área associadas às mesmas, por exemplo, *cone, área*. Mesmo no caso do círculo o resultado é *aproximado* porque, depende da constante de Arquimedes, π para a qual não temos um valor exato.

$$\pi \approx 3.14159265358979323848\ldots$$

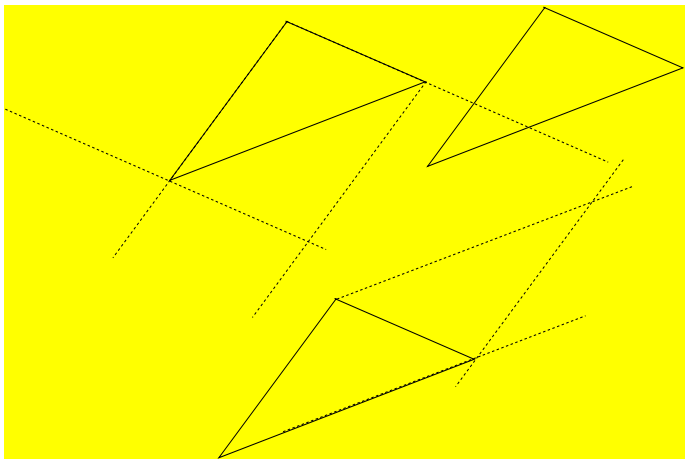

Figura 17:

Deixe-me mostrar-lhe como calcular a área dum círculo que se deduz da fórmula da área do triângulo. Na sequência de figuras (fig **??**), (fig 19), (fig 20), página **??**, eu estou *sugerindo* que área do hexágono e do dodecágono inscritos num círculo de raio 1 são obtidas por uma transformação que leva a paralelogramos que tem por base o *semiperímetro* e altura é o apótema, em cada caso. Daí estou deduzindo que área do círculo é igual a área dum quadrado que tem por base o *semiperímetro* que mede π e por altura o raio 1. Este é a fórmula da área dum triângulo que tenha por base o semiperímetro e por altura o apótema no caso dos polígonos o que me leva a concluir que área do círculo o produto do semiperímetro pela altura que é o raio.

São iguais, sendo a base do triângulo o perímetro do círculo e a altura do triângulo o raio do círculo. Se chega a esta ideia inscrevendo no círculo polígonos regulares convexos, cortando um destes polígonos ao longo de uma lados dos triângulos de que eles são compostos, se obtém uma aproximação para perímetro do círculo e para área do círculo como soma das áreas dos triângulos sendo a área do círculo o limite desta sucessão de medidas. Como em qualquer dos elementos da sucessão vale a regra para o cálculo da área a expressão da fórmula do triângulo, ela se transfere, como limite, para área do círculo, como se fosse um triângulo.

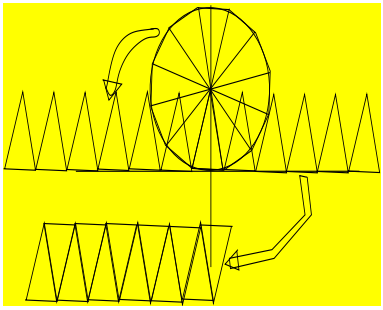

Figura 19:

É esta sugestão contida na figura figura (fig 20), página 50.

O número π foi descoberto pelos gregos como uma relação constante entre perímetro e diâmetro dum objeto circular: perímetro = $2\pi r$ em que r é o raio da circunferência. "π" é a letra grega que corresponde ao nosso "p" e a palavra grega para perímetro

Os gregos descobriram, ou ficaram sabendo que outros matemáticos anteriores a eles haviam descoberto que a razão entre o perímetro e o diâmetro dum objeto circular é constante e o valor desta razão é aproximadamente 3 mas não é um número racional que eles chamaram

$$\pi \approx 3.14159265358979323848\ldots \tag{221}$$

περιμετρο

Nos tempos *modernos*, onde nós vivemos, é a integral, um dos métodos do Cálculo Diferencial e Integral, é uma generalização do conceito de área para medir a região compreendida entre o gráfico duma função e o eixo OX, no contexto do Cálculo a área passa a ser *área algébrica* podendo ser nula ou negativa. Confira *soma!de Riemann*

Conceitos relacionados:

Algumas áreas mais importantes

- Área do quadrado de lado l é l^2;
- área do retângulo de lados m, n é mn;
- área dum triângulo de base l e altura h é $\frac{lh}{2}$, é a metade da área dum losango de base l e altura h;
- área dum triângulo de lados a, b, c, fórmula de Heron,

$$A = \sqrt{s(s-a)(s-b)(s-c)}; s = \frac{a+b+c}{2} \tag{222}$$

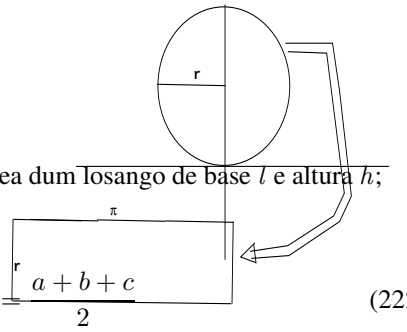

Figura 20:

- área dum losango de base l e altura h é lh;
- área dum trapézio de bases m, n e altura h é $\frac{m+n}{2}h$. O número $\frac{m+n}{2}$ se chama *base média*
- área dum polígono regular convexo de n lados cujo lado meça l é $\frac{nl}{2}a$ em que a é o *apótema*, ou altura de cada um dos triângulos em que o polígono se divide. Um polígono regular convexo está inscrito num círculo de raio r

$$r = \frac{l}{2\sin(\theta)}; \theta = \frac{\pi}{n}; \tag{223}$$

$$a = \frac{l\cos(\theta)}{2\sin(\theta)}; \tag{224}$$

  O número $\frac{nl}{2}$ se chama de *semiperímetro*. A denominação *polígono regular convexo* existe mas é precária. A ausência do adjetivo *convexo* supõe que os ângulos entre os lado deixe de ser iguais, o que é possível mas então cria uma variedade imensa de polígonos regulares.

- área do círculo de raio r é πr^2 e o perímetro do mesmo círculo é $2\pi r$.
- área da esfera de raio r é $4\pi r^2$.
- Somas de Riemann.

- **área da elipse** pode ser obtida

- **área do círculo**

- **área do cone**

- **aritmética** O objeto da *Aritmética* é a descoberta das propriedades gerais dos números naturais $1, 2, 3, \ldots$. Esta é a frase inicial do livro de Davenport, um discípulo e continuador do trabalho de G. Hardy que junto com Littlewood foram os dois pioneiros da Matemática inglesa na área da teoria dos números dentro da qual se encontra a *Aritmética* como pedra fundamental.

Numa tradução livre...

Os números naturais se dividem em duas classes, os *números primos*, que, por definição, somente podem ser divididos por eles mesmos, e portanto não podem ser fatorados, e os demais números naturais. A sequência dos números primos continua sendo, hoje, um dos mais *intrigantes segredos da Matemática*, se sabe muito sobre os números primos e também que há ainda muito o que descobrir sobre eles. Na prática tudo que sabemos é que uma sucessão infinita de números naturais, e isto é um dos *teoremas da Aritmética*. Um dos resultados mais recentes sobre os números primos, provado por um matemático chinês que vive na América, *Yitang Zhang* é que há um salto dos números primos. Zhang descobriu, [2]

Teorema 7 (salto) *de Zhang dos números primos*

Existe um número muito grande,s_0 tal que se p for um número primo, então há um outro número primo no intervalo $[p, p + s_0]$. $s_0 < 70.000.000$

em um pouco depois dois outros matemáticos conseguiram melhorar este teorema descobrindo s_1 que substitui s_0, mas a busca prossegue por $s_2 \ldots$

Não apresento a demonstração do *teorema de Zhang* porque não há conheço e é um dos resultados difíceis da *teoria dos números*. Mas não afasto a possibilidade de incluí-la aqui num certo futuro, confira [2].

Outro exemplo inicial, e dos mais conhecidos, é o *teorema da fatoração* dos números naturais.

Teorema 8 (da) *fatoração dos números naturais*

Todo número natural pode ser fatorado de maneira única num produto de números primos elevados a alguma potência. Esta fatoração é única.

Dem :

Se $n \in \mathbf{N}$ não for primo, então existe um número primo p_1 tal que

$$p_1 | n; n = p_1 n_1 + r_1 \tag{225}$$

pelo algoritmo da divisão euclidiana Então

$$p_1, n_1, r_1 < n; p_1 | n; n_1 | n; r_1 = 0; \tag{226}$$

uma vez que tanto p_1, n_1 dividem n deixando o resto r_1, como, por hipótese n não é primo então $r_1 = 0$. Ou seja, se não for possível encontrar entre os números primos que forem menores que n de maneira que se possa escrever a equação (eq.226) então n é primo e a demonstração termina, porque descobrimos um novo número primo. Então supondo que a (eq.226) seja possível vou passar a verificar se n_1 é primo. Se for está terminada a demonstração com a fatoração expressa na equação (eq.226) porque $r_1 = 0$. Se n_1 não for primo então pode ser fatorado o que vai produzir uma sucessão finita

este é o método da busca por novos números primos.

$$n_1, n_2, \cdots, n_k \tag{227}$$

de fatores primos para n. Como alguns dos números primos nesta sucessão podem ser iguais e foram obtidos em ordem decrescente, então a demonstração finaliza com a expressão

$$n = n_1^{m_1} \cdots n_j^{m_j}; j \leq k; \tag{228}$$

que é fatoração de n num produto de números primos. **q.e.d .**

Observe que para fazer referência ao *primeiro* e mais fundamental dos teoremas da *Aritmética* eu me vi forçado a passar por um teorema mais recente, o *teorema de Zhang*, que garante a infinitude da sequência dos números primos porque ele estabelece a existência duma progressão aritmética que entre cujos termos se

"primeiro", depende do autor.

encontram **todos os números primos**. É uma forma complicadíssima de provar que a sucessão dos números primos é infinita mas oferece outra vantagem na busca por números primos. O livro de Davenport afirma que a *Aritmética* é a mais pura das partes da Matemática e que praticamente não tem aplicações. É uma *afirmação errada* e lembra o ponto de vista de Hardy, certamente o mentor de Davenport, que dizia algo do tipo "*se eu souber que aquilo que estou estudando tem alguma aplicação, eu mudo imediatamente o rumo dos meus estudos*" mal sabia ele que *teoria dos números*, em particular o estudo dos números primos, seria a parte central da *criptografia* do mais alto interesse para os banqueiros e para o comércio eletrônico. Fora a vitória contra a Alemanha nazista em que o matemático *Alan Turing* teve papel importante quebrando a criptografia dos nazistas e assim decifrando seus segredos de guerra, aplicações da *pura Aritmética*!

A *Aritmética* é apresentada às crianças desde o começo quando a aprendem as quatro operações duas das quais são falhas, a *divisão* e *subtração* e não deveriam ser ensinadas, pelo menos da forma como o são. A *multiplicação*, na *Aritmética*, é uma soma repetida. Quando um dia os professores forem aqueles que organizem a Escola, então poderemos ver a *divisão* adquirir uma melhor funcionalidade e se tornando até divertida com uma compreensão do *algoritmo da divisão euclidiana* que até mesmo permite compreender melhor a *subtração*.

A *adição* tem quatro propriedades.

1. comutatividade, $a + b = b + a$,
2. associatividade, $(a + b) + c = a + (b + c)$, que incrivelmente importante porque é quem permite multiplicar n números e também permite tornar algumas contas mais fáceis.

$$17 + 14 = (10 + 7) + 14 = (10 + 7) + (10 + 4) = 20 + (7 + 4) = 20 + 11; \tag{229}$$

   em que também usei a *comutatividade*. E isto poderiam ser jogos para avançar o entediamento das crianças no ensino da Matemática induzindo pelo uso o aprendizado da tabuada e evitando ter que decorá-la de forma abruta.

3. distributividade que permite que a gente conte rapidamente quantos ovos tem nas bandejas no mercado quando estas forem diferentes. Uma bandeja tem na lateral b ovos alinhados em a linhas, e a outra tem c ovos alinhados em a linhas, então

$$a \times (b + c) = ab + ac \tag{230}$$

   é a quantidade de ovos nas duas bandejas.

4. o elemento neutro, o 0 da adição e do inverso aditivo que falha no conjunto $\mathbf{N}$

Numa Escola futurista vamos encontrar logo os professores mostrando que estas propriedades podem ser vistas num relógio e em seguida falar do resto na divisão para em seguida mostrar que há uma infinidade de sistemas aritméticos que são

$$\mathbf{Z}_2, \mathbf{Z}_3, \mathbf{Z}_4, \mathbf{Z}_5, \mathbf{Z}_6, \mathbf{Z}_7, \ldots \tag{231}$$

e levar a criançada a ver a diferença entre $\mathbf{Z}_2, \mathbf{Z}_3, \mathbf{Z}_5, \mathbf{Z}_7$ porque são os restos na divisão por um *número primo*. Devagar, com profundidade divertida, estarão levando as crianças à ciência da Matemática e tirando-as do horror habitual que a Matemática provoca. Nos conjuntos dos restos se tem as quatro propriedades todas funcionando com a adição, são exemplos de *Aritmética finita*. E no caso dos primos as duas operações, *adição e multiplicação* são completas.

Também é possível neste momento mostrar que os números naturais são defeituosos do ponto de vista da *multiplicação* que tem um elemento neutro mas não tem inverso. Isto pode sair do $\mathbf{Z}_p$ como comparação, e para corrigir $\mathbf{N}$ foram criados os números inteiros $\mathbf{Z}$.

E neste momento novo problema aparece que permite outro avanço, $(\mathbf{Z}, \cdot)$, com a multiplicação, tem o mesmo defeito que $(\mathbf{N}, +)$. Com isto termino de imaginar o Ensino de Matemática da Escola Fundamental com outra formatação que a leva para fora da Idade Média em que se encontra porque vai aparecer o conceito de *grupo* também levando a outra visão da geometria abrindo espaço para compreender um pouco de química. Claro nada disto é compatível com um *sinistro* na Educação.

Possivelmente esta metodologia introduz de forma natural o *conserto* de $\mathbf{Z}$ para chegar em $\mathbf{Q}$. Claro, esta crítica do ensino é incompleta, o ensino da geometria precisa ter lugar na Escola Fundamental apenas não cabe neste tópico, *Aritmética*, discutir uma forma evoluída de ensinar geometria que respeite a inteligência das crianças.

O método do ensino pela solução de problemas é muito produtivo, ele induz o gosto pela pesquisa. Uma análise da aparência, como

$$1 = 1^2, 1 + 3 = 2^2, 1 + 3 + 5 = 3^2, 1 + 3 + 5 + 7 = 4^2 \dots \tag{232}$$

será sempre verdade que a soma dos sucessivos números ímpares, seja uma sucessão de números naturais ao quadrado? Os números ímpares formam uma p.a. então eu posso descrever esta propriedade como

$$P(N) : \sum_{k=0}^{N} 2k + 1 = N^2; \tag{233}$$

Parece ser verdadeiro e inclusive uma linha de programação serve para ilustrar a sentença na equação (eq.233)

```
S =0; for(k=0;k<20;k+=2) {S+=k; print,k, S}
 k S
 1 1
 3 4
 5 9
 7 16
 9 25
 11 36
 13 49
 15 64
 17 81
 19 100
```

e até programação pode ser introduzida na Escola, este é um comando do `Python` uma linguagem de domínio público que é muito fácil de ser introduzida nas Escolas e pode ser usada para fazer testes aritméticos como este. Mas é verdade a sentença na equação (eq.233)?

Deixe-me supor que seja, que até um certo número N seja verdadeiro, a listagem me diz que vale até $N = 9$. Que acontece com $N + 1$?

$$P(N+1) : \sum_{k=0}^{N} 2k + 1 + 2N + 1 = N^2 + 2N + 1 = (N+1)^2; \tag{234}$$

$$P(N) \;\; \Rightarrow \;\; P(N+1); \tag{235}$$

é o *Princípio da Indução Finita* que deve ser divertido ensinar numa Escola Futurista que tenha rompido com suas ligações medievais. E agora ficou provado que aquela listagem de computador revelou um *teorema* da *Aritmética*. .

Eu chamei a "*indução finita*" de "*princípio*" que é quase um sinônimo de "postulado" ou "axioma". De fato, este "*princípio*" equivale *aos axiomas* que o matemático italiano Peano construiu para definir os números naturais.

Conceitos relacionados:

- Aritmética modular, a aritmética dos $\mathbf{Z}_p$.
- Teorema fundamental da aritmética.
- Princípio da Indução Finita.

- **arranjo** é um item da Análise Combinatória que é a parte elementar da *combinatória*. Confira também *arranjo com repetição, combinação, permutação*.

A *análise combinatória* estuda *arranjos, permutações, combinações* e os *arranjos* podem ser *simples* ou *com repetição*. Os *arranjos simples* também são chamados de *arranjos sem repetição*.

As *combinações* são *exatamente os subconjuntos dum conjunto dado* e seria interessante que você começasse a leitura pelo verbete dedicado à *combinação*, que eu vou começar analisando as combinações, quando a maioria dos textos começa pelos arranjos, mas não é exatamente para ser diferente e sim porque desta forma vou conseguir chegar rapidamente a uma fórmula para calcular as combinações da qual vou deduzir a fórmula dos arranjos. E você logo vai ver que é um método mais concreto.

Se você tiver um conjunto A com n objetos, por exemplo,

$$A = \{1, 2, 3, \ldots, n\} \tag{236}$$

então você pode produzir *arranjos* com estes elementos.

Considere um conjunto com 3 elementos: $A = \{1, 2, 3\}$.

Posso agora extrair vários subconjuntos de A, e vou começar pelo subconjunto vazio, todo conjunto tem o vazio como subconjunto.

- $C_3^0 = 1$ é o número de subconjuntos com zero elementos tirados de A, o vazio é único!
- C_3^1 = 3 é o número de subconjuntos unitários que podem ser tirados de A: $\{1\}, \{2\}, \{3\}$.
- C_3^2 = 3 é o número de subconjuntos 2-a-2 que podem ser tirados de A: $\{1, 2\}, \{1, 3\}, \{2, 3\}$. Agora você pode ver a diferença entre *arranjos* e *combinações*. Os *arranjos* 2-a-2 serão

  $$(1, 2), (2, 1), (1, 3), (3, 1), (2, 3), (3, 2)$$

  totalizando 6 arranjos, 2-a-2, que posso fazer com os elementos do conjunto A. Cada *subconjunto* "gerou" dois arranjos porque seus elementos foram *permutados*:

  $$A_3^2 = 2C_3^2 = 2 * 3;$$

- C_3^3 = 1 é o número de subconjuntos 3-a-3 que podem ser tirados de A: $\{1,2,3\} = A$, somente o subconjunto A. Mas os arranjos serão 6:

$$(1,2,3),(1,3,2),(2,1,3),(2,3,1),(3,1,2),(3,2,1); \tag{237}$$

$$(1,2,3) \neq (1,3,2); \tag{238}$$

$$A_3^3 = 6C_3^3 = 6 * 1; \tag{239}$$

Pense nos arranjos de flores, um assunto comum. Tudo muda se você trocar as flores de lugar: são *arranjos de flores*, não são *subconjuntos de flores*.

Se 1 representar o branco, dois o verde e três o vermelho:

- $(1,2,3)$ é a flor branca seguida da verde e depois da vermelha,
- $(1,2,3)$ é a flor branca seguida da vermelha e depois da verde.

Os arranjos são deduzidos dos subconjuntos e a quantidade deles é obtida por uma multiplicação, observe como.

- $C_3^0 = 1 = A_3^0$ é o número de subconjuntos 0-a-0 tirados de A que é apenas o vazio. A quantidade de arranjos 0-a-0 é ainda 1. E aqui se trata de uma abstração, precisamos em Matemática de arranjos 0-a-0, não tente usar as flores agora! $C_3^0 = 1 = A_3^0$;
- $C_3^1 = 3$ é o número de subconjuntos 1-a-1 que podem ser tirados de A: $\{1\},\{2\},\{3\}$ e aqui não tem como alterar a ordem uma vez que cada subconjunto tem apenas um elemento: $C_3^1 = 3 = A_3^1$;
- $C_3^2 = 3$ é o número de subconjuntos 2-a-2 que podem ser tirados de A: $\{1,2\},\{1,3\},\{2,3\}$ e já vimos que cada subconjunto podia ser repetido então $A_3^2 = 2 * 3 = 2 * C_3^2 = 6$;
- C_3^3 = 1 é o número de subconjuntos 3-a-3 que podem ser tirados de A: $\{1,2,3\}$ = A, apenas o próprio A, $A_3^3 = 1 * 6 = 6$.

E tudo que precisamos saber é *que fator é este* que nos fornece o número de arranjos a partir do número de combinações:

$$A_n^p = K * C_n^p; K \text{ depende de } p; \tag{240}$$

logo acima você leu que dos subconjuntos foram feitas as *permutações dos seus elementos* para obter todos os arranjos.

Quantas são as P_p, permutações de p elementos? É este o número K que vai nos dar o valor de A_n^p multiplicando C_n^p.

As permutações são um caso particular dos arranjos e a notação é a seguinte:

$$P_p = A_p^p; \tag{241}$$

E você já viu nas equações acima:

- $P_0 = 1 = 0!$;
- $P_1 = 1 = 1!$;
- $P_2 = 2 = 2!$;

- $P_3 = 6 = 3!$;

Se você tiver n elementos,

- o primeiro pode pode ser escolhido de $n = A_n^1$ maneiras diferentes;
- mas para escolher o segundo, sem repetição, você já tem apenas $n - 1$ possibilidades,

$$A_n^2 = n(n-1);$$

- para escolher o terceiro, sem repetição, você já tem apenas $n - 2$ possibilidades:

$$A_n^3 = n(n-1)(n-2) = \frac{n!}{(n-3)!};$$

- e sucessivamente, para escolher o $n-$ésimo, só lhe resta uma escolha:

$$A_n^n = P_n = n(n-1((n-2)\ldots 1 = n! = \frac{n!}{0!}$$

- $P_n = n!$

E chegamos à fórmula dos arranjos a partir das combinações:

$$A_n^p = p!C_n^p = p!\frac{n!}{(n-p)!p!} = \frac{n!}{(n-p)!} = \frac{P_n}{P_{(n-p)}}; \tag{242}$$

$$A_n^p = \frac{n!}{(n-p)!}; \tag{243}$$

porque será possível construir $p!$ arranjos $p - a - p$ com cada subconjunto com p elementos.

A fórmula que você vai encontrar em qualquer livro é esta da equação (eq. 243).

- **arranjo com repetição** é um item da Análise Combinatória que é a parte elementar da *combinatória*. Confira também *arranjo simples, combinação, permutação*.

Dado um conjunto $A = \{1, 2, \ldots, n\}$ o conjunto dos arranjos, $p - a - p$, com repetição destes n elementos é o *produto cartesiano*

$$A^p = \underbrace{A \times A \times \cdots \times A}_{p \text{ fatores}} \tag{244}$$

e o número dos elementos de um produto cartesiano é o produto dos números de elementos de cada conjunto fator então

$$\mathcal{A}_n^p = n^p \tag{245}$$

O símbolo $\mathcal{A}_n^p$ não é universalmente adotado.

Os arranjos com repetição ocorrem quando houver sentido em se repetirem os elementos dum conjunto, como é o caso com os números, *número de telefone*, *placa de carro*, palavras de uma linguagem que são *arranjos com repetição* das letras de um determinado alfabeto.

- **Atiyah, Michael Francis** matemático, nascido em 22 abril de 1929 e que morreu em 11 de janeiro 2019 aos 89 anos.

Estudou no Trinity College, Cambridge, onde defendeu sua tese de doutorado, assumiu posição no Institute for Advanced Study de Princeton, Princeton, Cambridge e em Oxford como Savilian professor de geometria 1963-69. Em 1966 ganhou a Medalha Fields. Em 1990 se tornou mestre do Trinity College, Cambridge, e diretor do Isaac Newton Institute for Mathematical Sciences, Cambridge.

Atiyah sempre atuou na divulgação da Matemática apresentando palestras formatadas com um objetivo popular tentando mostrar a beleza da paixão de sua vida, a Matemática. Entre muitos outros livros, ele escreveu Introduction To Commutative Algebra.

- **atlas** um conceito de geometria diferencial e também da topologia de variedades.

A ideia intuitiva vem do *atlas múndi*, como a Terra *pertence a classe topológica da* esfera, é impossível definirmos uma única função de uma região do plano na superfície da Terra, então precisamos de vários mapas formando um *atlas* para descrever com peças planas a superfície da Terra. É esta a ideia de um atlas em topologia ou em geometria diferencial.

Definição 4 (atlas) *Atlas Se $\mathcal{V}$ for uma variedade de dimensão n, dizemos que $((U_i, \phi_i)_{i\in I}$ é um atlas para $\mathcal{V}$ se $(R_i)_{i\in I}$ for uma coleção de abertos do $\mathbf{R}^n$ e $(R_i \xrightarrow{\phi_i} U_i)_{i\in I}$ for uma coleção de aplicações injetivas contínuas (homeomorfismos) de abertos do $\mathbf{R}^n$ em abertos de $\mathcal{V}$ satisfazendo às condições seguintes:*

- $\bigcup_{i\in I} U_i = \mathcal{V}$, *que garante que os mapas cobrem a variedade;*
- *para qualquer par (i, j) de índices, $R_i \cap R_j \neq$, que garante que não haja regiões com mapas incompatíveis junto com a próxima condição;*
- *para qualquer par (i, j) de índices, as aplicações ϕ_i, ϕ_j coincidem na interseção $R_i \cap R_j$ que garante que não haja regiões com mapas incompatíveis;*

Se a variedade $\mathcal{V}$ for diferenciável (em geometria diferencial e topologia diferencial) se precisa que ϕ_i sejam difeomorfismos

Cada aplicação

$$R_i \xrightarrow{\phi_i} U_i$$

se chama um mapa do atlas.

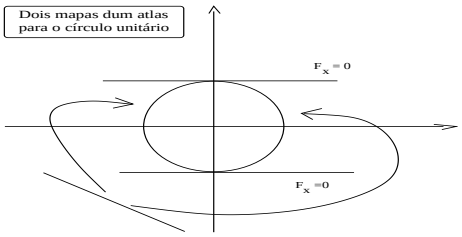

Figura 21: Dois mapas dum atlas para o círculo unitário

Na figura (21), página 57, você dois mapas para o círculo, mas é preciso de quatro mapas para formar um atlas para o círculo, para isto para selecionar dois pares de *pontos antípodas*, diferentes, e a cada um destes pares corresponde um par de mapas.

- **átomo** de uma partição da unidade é um das funções positivas e a suporte compacto duma família que define uma *partição da unidade*. Confira *partição da unidade*.

Uma maneira simples de produzir uma *partição da unidade* consiste em considerar a família das *funções características* dos elementos duma *partição*, ou *conjunto quociente* dum *espaço* Ω. Os átomos desta *partição da unidade* não serão contínuas mas a convolução dum *núcleo* com os seus elementos produz uma *partição da unidade* cujos átomos podem ter uma classe de diferenciabilidade alta.

Se os *átomos* duma partição da unidade forem splines, esta partição da unidade define um *projetor de interpolação* que é polinomial.

Conceitos relacionados:

- *conjunto quociente* e relação de equivalência.
- *núcleo*, uma função positiva, cuja integral é 1. Rudin define *núcleo* como uma família de tais funções que convergem fracamente para a medida de Dirac.
- *projetor de interpolação*
- *splines*

- **automorfismo** é um isomorfismo duma estrutura nela mesma. Os morfismos são funções que preservam a estrutura e os isomorfismos identificam estruturas semelhantes.

- morfismo topológico são as funções abertas bijetivas, aquelas que preservam os *abertos* da topologia. A composição de duas funções abertas é uma função aberta, a identidade é uma função aberta. Se f, g forem funções abertas, então fog é uma função aberta. Eu preciso provar a última afirmação. Considere os espaços topológicos X, Y, Z e $\mathcal{O} \subset X$ um aberto,

$$f : X \longrightarrow Y; gY \longrightarrow Z; \tag{246}$$
$$f(\mathcal{O}) \text{ é um aberto} \quad \Rightarrow \quad g(f(\mathcal{O})) \text{ é um aberto ;} \tag{247}$$
$$(fog)(\mathcal{O}) \text{ é um aberto.} \tag{248}$$

  Se $X = Y = Z$ então as funções abertas bijetivas de X são automorfismos topológicos de X.

- Vale para as funções contínuas injetivas mas usando agora as imagens inversas uma vez que as funções contínuas preservam os abertos via imagem inversa, por definição.

$$f : X \longrightarrow Y; gY \longrightarrow Z; \tag{249}$$
$$g^{-1}(\mathcal{O}) \text{ é um aberto} \quad \Rightarrow \quad f^{-1}(g^{-1}(\mathcal{O}) \text{ é um aberto;} \tag{250}$$
$$(fog)^{-1}(\mathcal{O}) \text{ é um aberto;} \tag{251}$$

  o que prova que a composição de funções contínuas é uma função contínua. As bijeções contínuas do espaço topológico X são automorfismos topológicos.

- Uma bijeção contínua é aberta?

  Se $X = Y = Z$ então as funções contínuas bijetivas em X são automorfismos topológicos de X.

- Se X for um espaço de Hausdorff então é possível separar seus pontos por abertos e dados $x, y \in X$ existem abertos disjuntos $O_x \cap O_y = \emptyset$. Dada uma função aberta, f

$$f^{-1}(O_x \cap O_y) = \emptyset = f^{-1}(O_x) \cap f^{-1}(O_y) \tag{252}$$

  que é um fechado/aberto da topologia portanto f não seria uma função aberta se não for injetiva.

- Nos espaços de Hausdorff o conjunto das funções abertas injetivas é um grupo relativamente à composição. Nos casos anteriores se tem também o grupo dos automorfismos.

- **autovalor** da Álgebra Linear, associado ao conceito de *autovetor*. Confira o sinônimo *valor próprio*.

- **autovetor** da Álgebra Linear, associado ao conceito de *autovalor* ou *valor próprio*. Confira o sinônimo *vetor próprio*.

- **axiomas de Zermelo-Fraenkel** é um conjunto de axiomas estabelecidos por Fraenkel e simultaneamente pelo noruegues Thoralf Albert Skolem fundamentando a teoria dos conjuntos.

1. axioma da extensão Dois conjuntos são iguais se eles tiverem os mesmos elementos.

$$A = B \iff (\forall x)(x \in A \iff x \in B) \tag{253}$$

2. Axioma da regularidade Todo conjunto não vazio X possui algum elemento y

Conceitos relacionados:

- teoria dos conjuntos.
- fundamentos da Matemática.
- Matemática construtivista

Índice Remissivo

Referências Bibliográficas

[1] R. Creighton Buck. *Advanced Calculus*. McGraw-Hill. Inc, 1978.

[2] Yitang Zhang. Bounded gaps between primes. *Annals of Mathematics*, 2014.

[3] American Mathematical Society. 2010 mathematics subject classification. http://www.ams.org/mathscinet/msc/msc2010.html.

[4] R. C. Boyce, William E e Diprima. *Equações diferenciais elementares e problemas de valores decontorno*. Editora: LTC - ISBN-13: 9788521614999, 2006.

[5] J. Dieudonné. *Calcul Infinitésimal*. Herman Éditeurs, 1968.

[6] S.V. Gelfand, I.M. e Fomin. *Calculus of variations*. Dover, 2000.

[7] Richard Courant. *Differential and Integral Calculus II*. Interscience Publishers Wiley classics library, 1988.

[8] Richard Courant. *Differential and Integral Calculus I*. Interscience Publishers Wiley classics library, 1988.

[9] William Dunham. *Euler: The Master of us all*. The Mathematical Association of America, 1999.

[10] Foundation for Free Software. Gpl - general public license. Technical report, http://www.FSF.org, 2011.

[11] P.Smith D.W.Jordan. *Non Linear Ordinary Differential Equations*. Oxford Applied Mathematics and Computing Science Series, 1977.

[12] Kai Lai Chung. *A course in probability theory*. Academic Press, INC. 1985, 2001.

[13] T Praciano-Pereira. Página de cálculo i. 2013.

[14] V. I. Arnold. *Mathematics: Frontiers and Perspectives*, chapter Poltmathematics: Is Mathematics a Single Science or a Set of Arts?, pages 1–403. American Mathematical Society, 1999.

[15] T Praciano-Pereira. Programas para cálculo numérico. Technical report, http://www.calculo-numerico.sobralmatematica.org/programas/, 2009.

[16] T Praciano-Pereira. Programando em gnuplot. Préprints da Sobral Matemática no 2008.1 - 2008 http://www.sobralmatematica.org/preprints/programando_gnuplot.pdf, 01 2008.

[17] Tarcisio Praciano-Pereira. *Cálculo Numérico Computacional*. Sobral Matematica, 2007.

[18] Tarcisio Praciano-Pereira Stálio Rodrigues dos Santos. *Introdução à Matemática Universitária*. Sobral Matemática, 2009.

[19] G.F. Simmons. *Differential Equations with Applications and Historical Notes*. McGraw-Hill - Book Company, 1979.

[20] G.F. Simmons. *Introduction to Topology and Modern Analysis*. McGraw-Hill - Book Company, 1968.

[21] Stephen Smale Morris W. Hirsch. *Differential Equations, Dynamical Systems, and Linear Algebra*. Academic Press, 1974.

[22] Wikimedia Foundation. Wikipedia, enciclopédia livre na internet. http://www.wikipedia.org.

[23] Wikipedia. *Wikipedia, a free enciclopedia*. http://pt.wikipedia.org/wiki/, 2003.

[24] the free enciclopedia in the Internet Wikipedia. Wikipedia, the free enciclopedia in the internet. http://en.wikipedia.org/wiki/Joseph_Fourier.

[25] Per-Olov Löwdin. Group algebra, convolution algebra, and applications to quantum mechanics. *Reviews of Modern Physics*, 39:29, 1967.