MAT 225 - FUNÇÕES ANALÍTICAS

Instituto de Matemática e Estatística da USP

Ano 2015

Professor Oswaldo R. B. de Oliveira

http://www.ime.usp.br/~oliveira oliveira@ime.usp.br

Capítulo 3 - POLINÔMIOS

Capítulo 1

NÚMEROS COMPLEXOS

Capítulo 2

TOPOLOGIA DO PLANO $\mathbb{C}$

Capítulo 3

POLINÔMIOS

3.1 - O Teorema Fundamental da Álgebra (TFA).

Em geral, o teorema fundamental da álgebra é provado em cursos de Análise Complexa como corolário do Teorema de Liouville, o qual segue da Fórmula Integral de Cauchy. Em cursos de Álgebra o TFA é comumente provado via Teoria de Extensões de Corpos, ou via Teoria de Galois, além de algum teorema de Análise (em geral, o teorema do valor intermediário). Também é usual provar o TFA em cursos de Topologia Algébrica. A prova nestas notas se apóia em resultados básicos em $\mathbb{R}$ e em aritmética simples com números complexos. Tal prova evita funções e números transcendentais (as funções trigonométricas, a função exponencial complexa, e os números e e π) e a extração de raízes n-ésimas arbitrárias de um número complexo qualquer. Tais extrações são geralmente feitas com a função exponencial complexa introduzida no Capítulo 7. Para uma prova do TFA que evita também a extração de raízes quadradas, vide *The Fundamental Theorem of Algebra: from the four basic operations*, de Oliveira, O. R. B., Amer. Math. Monthly, **119** no. 9 (2012) 753–758, http://dx.doi.org/10.4169/amer.math.monthly.119.09.753.

Raízes Quadradas. A equação $z^2 = a + ib$, dados $a, b \in \mathbb{R}$, é solúvel em $\mathbb{C}$, com

$$\pm z = \sqrt{\frac{a}{2} + \frac{\sqrt{a^2+b^2}}{2}} + i\mathrm{sgn}(b)\sqrt{-\frac{a}{2} + \frac{\sqrt{a^2+b^2}}{2}}\ , \text{ onde } \mathrm{sgn}(b) = \begin{cases} \frac{b}{|b|} \text{ se } b \neq 0 \\ \mathrm{sgn}(0) = 1\ . \end{cases}$$

Com tal fórmula, por iteração achamos as 2^j-raízes de ± 1 e $\pm i$, para todo $j \in \mathbb{N}$.

3.1 Teorema (TFA). *Seja $P(z) = a_0 + a_1 z + \cdots + a_n z^n$ um polinômio complexo, de grau $n \geq 1$. Então, existe z_0 em $\mathbb{C}$ tal que $P(z_0) = 0$.*

Prova. Dividamos a prova em duas partes.

(A) Pela desigualdade triangular segue $|P(z)| \geq |a_n||z|^n - |a_0| - \cdots - |a_{n-1}||z|^{n-1}$ e

$$\lim_{|z|\to+\infty} |P(z)| = +\infty.$$

Logo, existe $r > 0$ tal que $|P(z)| > |P(0)|$ se $|z| > r$. Por continuidade, $|P(z)|$ restrita ao compacto $D(0;r)$ tem um mínimo $|P(z_0)| \leq |P(0)|$, com z_0 em $D(0;r)$. Assim sendo, para todo z em $\mathbb{C}$ temos $|P(z)| \geq |P(z_0)|$.

(B) O polinômio $P(z_0 + z)$ tem grau n e $\min\{|P(z_0+z)| : z \in \mathbb{C}\} = |P(z_0)|$. Logo, podemos supor $z_0 = 0$. Como P não é constante, temos

(1) $\quad P(z) = P(0) + z^k Q(z)\,,\;$ com $Q(z)$ um polinômio, $Q(0) \neq 0$ e $k \geq 1$.

Seja $z = r\omega$, com $r > 0$ e $\omega \in S^1 = \{\omega \in \mathbb{C} : \; |\omega| = 1\}$. Pelo provado em (A),

(2) $\quad |P(r\omega)|^2 - |P(0)|^2 \geq 0\,,$ para quaisquer $r > 0$ e $\omega \in S^1$.

Computando (1) em $z = r\omega$, substituindo em (2) e cancelando $|P(0)|^2$ segue

$$2r^k \mathrm{Re}\Big[\overline{P(0)}\omega^k Q(r\omega)\Big] + r^{2k}\big|Q(r\omega)\big|^2 \geq 0, \text{ para quaisquer } r > 0 \text{ e } \omega \in S^1.$$

Fixando $\omega \in S^1$, cancelando r^k e então obtendo o limite para $r \to 0^+$ segue

(3) $\quad \mathrm{Re}\Big[\,\overline{P(0)}Q(0)\,\omega^k\,\Big] \geq 0\;,\;$ com ω arbitrário em S^1.

Seja $\alpha = \overline{P(0)}Q(0)$. Fatorando potências de 2 temos $k = 2^j m$, com m ímpar. Substituindo $\omega = 1$ em (3) temos $\mathrm{Re}[\alpha] \geq 0$. Escolhendo (podemos) ω tal que $\omega^{2^j} = -1$ obtemos $\mathrm{Re}[\alpha] \leq 0$ e concluímos $\mathrm{Re}[\alpha] = 0$. Escolhendo ω tal que $\omega^{2^j} = i$ obtemos $\{\omega^k, \overline{\omega}^k\} = \{i, -i\}$ e então, substituindo ω e $\overline{\omega}$ em (3), concluímos $\mathrm{Im}[\alpha] = 0$. Logo, $\alpha = 0$ e, como $Q(0) \neq 0$, obtemos $P(0) = 0$♣

Exercício. Seja $P(z)$ um polinômio complexo de grau $n \geq 1$. Mostre que se $z_1 \in \mathbb{C}$ é um zero de $P(z)$ então [pelo algoritmo da divisão de Euclides para polinômios] $z - z_1$ divide $P(z)$. Ainda mais, é válida a fatoração $P(z) = (z-z_1)^{k_1} \ldots (z-z_m)^{k_m}$ onde $\{z_1, \ldots, z_m\}$ são os m zeros complexos distintos de $P(z)$, para algum $m \leq n$, e k_j é a multiplicidade algébrica de z_j como zero de $P(z)$ e, ainda, $k_1 + \cdots + k_m = n$.

3.2 - Uma Raiz Primitiva para as Raízes n-ésimas da Unidade.

Fixemos n em $\{1, 2, \ldots\}$. Pelo TFA a equação $z^n = 1$, tem n soluções em $\mathbb{C}$, ditas raízes n-ésimas da unidade. Denotemos por w uma arbitrária raiz n-ésima da unidade. Dada w, temos

$$\begin{cases} z^n - 1 = z^n - w^n = (z-w)Q(z), \ \text{com } Q(z) = \sum_{j=0}^{n-1} z^{n-1-j}w^j \ \text{um polinômio e} \\ Q(w) = nw^{n-1} \neq 0, \end{cases}$$

e portanto w é um zero simples do polinômio $z^n - 1$, com z em $\mathbb{C}$. Logo, existem n distintas raízes n-ésimas da unidade.

Dado k arbitrário em $\mathbb{N}^*$, um cálculo simples mostra que $\overline{w} = w^{-1}$ e w^k são raízes n-ésimas da unidade. Ainda mais,

$$|w^{k+1} - w^k| = |w^k(w-1)| = |w-1|.$$

Se w é real ou imaginário puro, então w pertence a $\{1, -1, i, -i\}$.

Dizemos que w é uma raiz primitiva das raízes n-ésimas da unidade se

$$w, w^2, \ldots, w^n \quad (\text{obviamente } w^n = 1)$$

são todas as n raízes n-ésimas da unidade.

Para provar a existência de uma raiz primitiva para as raízes n-ésimas da unidade, podemos supor n par. Pois, se w é uma raiz primitiva para as raízes $2n$-ésimas da unidade então $w^2, \ldots, w^{2n}$ são todas as n soluções distintas de $z^n = 1$. Melhor ainda, os casos $n = 2$ e $n = 4$ são triviais e podemos também supor $n \geq 6$.

Dado n par e $n \geq 6$, a equação $z^n = 1$ tem uma solução w não real e não imaginária pura. Também $\pm w$ e $\pm\overline{w}$ são soluções de $z^n = 1$. Portanto, existe uma raiz n-ésima da unidade com partes real e imaginária estritamente positivas.

Desta forma, existe uma raiz n-ésima da unidade:

$$\begin{cases} \zeta = \zeta(n) = a + ib, \ \text{com } 0 < a < 1 \text{ e } 0 < b < 1, \\ \text{satisfazendo } 0 < |\zeta - 1| = r, \ \text{onde } r = \min\{|w-1| : \ w^n = 1 \text{ e } \mathrm{Im}(w) > 0\}. \end{cases}$$

Destacamos que ζ satisfaz $r^2 = |\zeta - 1|^2 = (a-1)^2 + b^2 = 2 - 2a$. Ainda mais, ζ é a única raiz n-ésima da unidade satisfazendo $|\zeta - 1| = r$ e $\mathrm{Im}(\zeta) > 0$.

No que segue, consideramos um inteiro par $n \geq 6$ e mantemos a notação acima.

3.2 Lema. *Dado x em $[-1,1]$, seja $z_x = x + i\sqrt{1-x^2}$. Vale o que segue.*

(A) A função

$$\varphi : [-a,1] \to [-1,a], \text{ onde } \varphi(x) = \mathrm{Re}(\zeta z_x) = ax - b\sqrt{1-x^2},$$

é bijetora e estritamente crescente. Sua inversa é

$$\psi : [-1,a] \to [-a,1], \text{ onde } \psi(y) = \mathrm{Re}(\zeta^{-1} z_y) = ay + b\sqrt{1-y^2}.$$

(B) Para $x \in [-1,-a] \cup [a,1]$, temos $(z_x)^n = 1$ se e somente se $x \in \{\pm 1, \pm a\}$.

Prova. Comecemos vendo que φ e ψ estão bem definidas.

Dado x em $[-a,1]$, é bem trivial ver que $-1 \le \mathrm{Re}(\zeta z_x) = ax - b\sqrt{1-x^2} \le a$. Analogamente, dado y em $[-1,a]$ temos $-a \le ay \le ay + b\sqrt{1-y^2} = \mathrm{Re}(\zeta^{-1} z_y) \le 1$.

Apesar de não necessária à prova, pode ser útil ao leitor a figura abaixo.

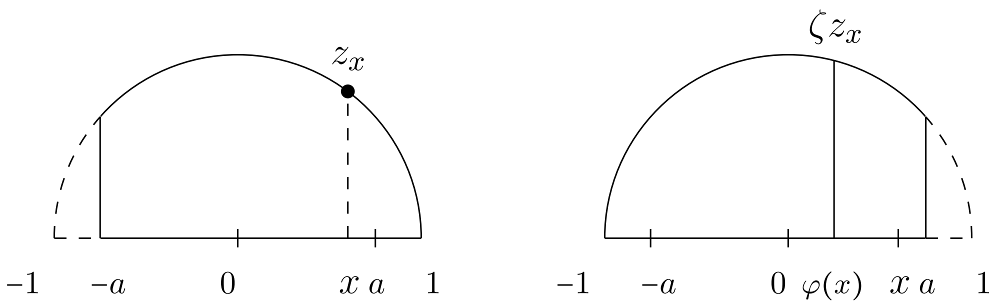

Figura 3.1: Interpretação para $\varphi : [-a,1] \to [-1,a]$.

(A) Se x está em $[-a,1]$, então $\mathrm{Im}(\zeta z_x) = a\sqrt{1-x^2} + bx$ é positivo em $[-a,0]$ (crescendo de 0 até a) e em $[0,1]$. Portanto, $y = \mathrm{Re}(\zeta z_x)$ satisfaz

$$z_y = \zeta z_x \quad [\text{com } y = \varphi(x)]. \tag{3.2.1}$$

Donde, $\psi(y) = \mathrm{Re}(\zeta^{-1} z_y) = x$.

Se y está em $[-1,a]$, então $\mathrm{Im}(\zeta^{-1} z_y) = a\sqrt{1-y^2} - by$ é positivo em $[-1,0]$ e também em $[0,a]$ (pois decresce de a até 0 ao longo de $[0,a]$). Logo, $x = \mathrm{Re}(\zeta^{-1} z_y)$ satisfaz $z_x = \zeta^{-1} z_y$ e então segue $\varphi(x) = \mathrm{Re}(\zeta z_x) = y$.

Evidentemente, φ restrita a $[0,1]$ e ψ restrita a $[-1,0]$ são crescentes, com $\psi([-1,0]) = [-a,b]$. Portanto, $\varphi = \psi^{-1}$ restrita a $[-a,b]$ é crescente. Sendo assim, a bijeção φ é estritamente crescente em $[-a,1]$.

(B) Se x está em $(a,1)$, então temos $|z_x - 1|^2 = 2 - 2x < 2 - 2a = r^2$. Assim, pela definição de r, obtemos $(z_x)^n \neq 1$. Se $x \in \{a,1\}$, é óbvio que $(z_x)^n = 1$.

O caso x em $[-1,-a]$ é redutível ao caso acima. Pois, n é par e $z_x = -\overline{z_{-x}}$♣

3.3 Teorema. *$\zeta = \zeta(n)$ é uma raiz primitiva das raízes n-ésimas da unidade.*

Prova.

Definamos por iteração a sequência $x_k = \varphi(x_{k-1})$, com $x_0 = 1$ e $k \geq 1$ tal que x_{k-1} está em $[-a,1]$, o domínio de φ. A fórmula (3.2.1) mostra que $z_{x_k} = \zeta z_{x_{k-1}}$, com $z_{x_0} = 1 = \zeta^0$. Por iteração segue

$$z_{x_k} = \zeta^k \quad \big[\text{e} \ \ x_k = \text{Re}(\zeta^k)\big].$$

Pelo Lema 3.2(A), concluímos que a função φ é estritamente crescente e satisfaz $x_2 = \varphi(x_1) < x_1 = \varphi(x_0) = a < x_0 = 1$. Então, por iteração,

$$x_k < x_{k-1} < \cdots < x_0 = 1.$$

Como há n n-ésimas raízes da unidade, existe o maior p em $\mathbb{N}$ satisfazendo

$$-1 \leq x_p < x_{p-1} < \cdots < x_2 < x_1 < x_0 = 1.$$

Dado $k = 2, \ldots, p$, a função φ é uma bijeção de $[x_{k-1}, x_{k-2}]$ sobre $[x_k, x_{k-1}]$. Logo, por indução em k, a fórmula $z_{\varphi(x)} = \zeta z_x$ e o Lema 3.2(B), existem apenas dois valores de x em $[x_k, x_{k-1}]$ tais que $(z_x)^n = 1$. A saber, $x = x_k$ e $x = x_{k-1}$.

- ◇ Mostremos $x_p = -1$. Se x_p está no domínio de φ, definindo $x_{p+1} = \varphi(x_p)$ obtemos $x_{p+1} = \varphi(x_p) < \varphi(x_{p-1}) = x_p$, contra a definição de p. Portanto, x_p está em $[-1,-a)$ e $(z_{x_p})^n = 1$. Pelo Lema 3.2(B) segue $x_p = -1$ (e $\zeta^p = -1$).

Os subintervalos $[x_k, x_{k-1})$, com $k = 1, \ldots, p$, formam uma partição de $[-1,1)$ e a cada subintervalo corresponde só uma raiz n-ésima da unidade no hemisfério superior $\{z \in \mathbb{C} : |z| = 1 \text{ e } \text{Im}(z) \geq 0\}$. Assim, $\zeta^0, \zeta, \ldots, \zeta^p$ são todas as raízes n-ésimas da unidade no hemisfério superior e $\zeta^0, \ldots, , \zeta^p, \overline{\zeta}, \ldots, \overline{\zeta^{p-1}}$ são todas as n raízes n-ésimas da unidade. Logo, $n = 2p$. Para completar, dado k temos

$$\overline{\zeta^{p-k}} = \zeta^{-(p-k)} = \zeta^{2p}\zeta^{-p+k} = \zeta^{p+k}$$

e então

$$\left\{\overline{\zeta^{p-1}}, \overline{\zeta^{p-2}}, \ldots, \overline{\zeta}\right\} = \left\{\zeta^{p+1}, \zeta^{p+2}, \ldots, \zeta^{2p-1}\right\}$$ ♣

Comentários.

- O Lema 3.2(A) pode ser provado de forma breve (e obscura), via derivação. A função $\varphi : [-a, 1] \to [-1, a]$ é contínua, satisfaz $\varphi(-a) = -1$ e $\varphi(1) = a$, e

$$\varphi'(x) = a + \frac{bx}{\sqrt{1-x^2}} = \frac{a\sqrt{1-x^2} + bx}{\sqrt{1-x^2}}, \text{ para todo } x \text{ em } (-a, 1).$$

  Então, dado x em $[0, 1)$, temos $\varphi'(x) \geq a > 0$. Se $-a < x < 0$, temos

$$\sqrt{1-x^2} > \sqrt{1-a^2} = b \quad \text{e} \quad a\sqrt{1-x^2} + bx > ab - ab = 0.$$

  Donde, φ é estritamente crescente e, pelo teorema do valor-intermediário, sua imagem é $[-1, a]$.

- Se n é primo e $w \neq 1$ é uma raiz n-ésima da unidade, uma argumentação simples mostra que w é uma raiz primitiva das raízes n-ésimas da unidade.

- Dado m em $\mathbb{N}^*$ e ζ, uma raiz primitiva das raízes n-ésimas da unidade, é trivial ver que

$$\zeta^m \text{ é uma raiz primitiva de tais raízes se e só se } \mathrm{mdc}(m, n) = 1.$$

- Seja ζ uma raiz primitiva das raízes n-ésimas da unidade. Então, dado um número c in $\mathbb{C}$, com $c \neq 0$, e z, uma raiz n-ésima arbitrária de c, é imediato provar que

$$\zeta^0 z, \zeta^1 z, \ldots, \zeta^{n-1} z$$

  são todas as n distintas raízes n-ésimas de c.

- Usando a função exponencial complexa, é fácil ver que

$$e^{i\frac{2\pi}{n}} \text{ é uma raiz primitiva das raízes } n\text{-ésimas da unidade.}$$

  Um cálculo trivial mostra

$$e^{i\frac{2\pi}{n}} = \zeta.$$

3.3 - As Desigualdades de Gutzmer-Parseval e de Cauchy, para Polinômios.

3.4 Teorema (Desigualdade de Gutzmer-Parseval). *Consideremos um polinômio complexo* $P(z) = \sum_{j=0}^{n} a_j z^j$ *e a constante* $M(r) = \sup_{|z|=r} |P(z)|$, *onde* $r > 0$. *Temos,*

$$\sum_{j=0}^{n} |a_j|^2 \, |r|^{2j} \leq M(r)^2.$$

Prova. Consideremos ω uma raiz primitiva das raízes $2n$-ésimas da unidade (logo, $\omega^n = -1$) e os $2n$ polinômios, na variável z,

$$P_k(z) = P(z\omega^k)\,, \quad \text{com} \quad 0 \leq k \leq 2n-1.$$

Fixado k temos

$$|P_k(z)|^2 = \left(\sum_{\nu=0}^{n} a_\nu z^\nu \omega^{k\nu}\right)\left(\overline{\sum_{\mu=0}^{n} a_\mu z^\mu \omega^{k\mu}}\right) = \sum_{\mu=0}^{n}\sum_{\nu=0}^{n} a_\nu z^\nu \overline{a_\mu}\, \overline{z}^\mu \omega^{k\nu} \overline{\omega}^{k\mu} =$$

$$= \sum_{0 \leq j \leq n} |a_j|^2 \, |z|^{2j} \;+\; 2 \sum_{0 \leq \mu < \nu \leq n} \mathrm{Re}\left[\, a_\nu z^\nu \overline{a_\mu}\, \overline{z}^\mu \omega^{k\nu} \overline{\omega}^{k\mu} \,\right].$$

Se $\mu < \nu$, então $\nu - \mu$ percorre $\{1, \ldots, n\}$. Escrevendo $\omega^{k\nu}\overline{\omega}^{k\mu} = \omega^{k(\nu-\mu)}$ obtemos

$$\sum_{k=0}^{2n-1} \omega^{k(\nu-\mu)} = \frac{1 - \omega^{2n(\nu-\mu)}}{1 - \omega^{\nu-\mu}} = 0\,, \qquad \text{se } 0 \leq \mu < \nu \leq n\,,$$

donde segue a identidade $\sum_{k=0}^{2n-1} \left[\, a_\nu z^\nu \overline{a_\mu}\, \overline{z}^\mu \omega^{k\nu} \overline{\omega}^{k\mu} \,\right] = 0$. Assim, é fácil ver que

$$\sum_{k=0}^{2n-1} |P_k(z)|^2 = 2n \sum_{j=0}^{n} |a_j|^2 \, |z|^{2j}\ .$$

Por outro lado, pela igualdade $\max_{|z|=r} |P_k(z)| = \max_{|z|=r} |P(z)|$ segue

$$\sum_{k=0}^{2n-1} |P_k(z)|^2 \leq 2nM(r)^2 \ \text{, if } |z| = r.$$

O teorema segue então das duas últimas fórmulas em destaque e acima♣

3.5 Corolário (Desigualdade de Cauchy para polinômios).

$$|a_j| \leq \frac{M(r)}{r^j}\ .$$

Prova. Trivial ♣