Ano 2015

ALGORITMO DE EUCLIDES PARA A DIVISÃO DE POLINÔMIOS

Professor Oswaldo Rio Branco de Oliveira

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

Dados $n+1$ números complexos $a_n, a_{n-1}, \ldots, a_1, a_0$ e a indeterminada z (a teoria segue analogamente para um corpo K arbitrário) dizemos que a soma formal

$$a_n z^n + \cdots + a_1 z + a_0$$

é um polinômio com coeficientes complexos $a_n, \ldots, a_0$ e na indeterminada z. Tal apresentação embute duas identificações. A saber, $a_0 \equiv a_0 z^0$ e $z \equiv z^1$. O polinômio acima é também descrito como

$$a_n z^n + \cdots + a_0 z^0.$$

Tradicionalmente, a indeterminada é indicada por X. A indeterminada, denotada X ou z ou qualquer letra, é um objeto formal e não indica uma variável. Isto é, a indeterminada não percorre valores em um conjunto.

Como desejamos que, por exemplo,

$$1 + 2z - 3z^2 \quad \text{e} \quad 1 + 2z - 3z^2 + 0z^3 + 0z^4$$

representem o mesmo polinômio, aprimoramos a definição dada acima. Dizemos então que um polinômio é uma soma formal infinita

$$a_0 z^0 + a_1 z + \cdots + a_n z^n + \cdots$$

em que $\{j : a_j \neq 0\}$ é finito (e z é a indeterminada). Denotemos tal polinômio por $P(z)$. Como a notação para a soma formal $P(z)$, na indeterminada z, é a mesma que para a função $P(z)$, na variável z, faremos a distinção com os devidos nomes.

Se $a_n \neq 0$ e $a_j = 0$ para todo $j > n$, escrevemos o polinômio $P(z)$ como

$$P(z) = a_n z^n + \cdots + a_1 z + a_0$$

e dizemos que a_n é o coeficiente dominante. O termo a_0 é o termo independente. Ainda neste caso, dizemos que o polinômio $P = P(z)$ tem grau n e escrevemos

$$\text{grau}(P) = n.$$

Façamos alguns comentários.

Se $a_0 = 0$ mas nem todos os coeficientes de $P(z)$ são nulos, é usual omitir a_0.

Por exemplo, abreviamos $P(z) = 7z^2 + 6z + 0$ por $P(z) = 7z^2 + 6z$.

Dado a em $\mathbb{C}$, o polinômio $P(z) = az^0 \equiv a$ é dito um polinômio constante.

Dizemos que o polinômio nulo (todos os coeficientes são nulos) tem grau $-\infty$.

O polinômio nulo é o polinômio constante $P(z) = 0$.

O polinômio $1z^n$, onde $n = 0, 1, 2, \ldots$, é denominado monômio de grau n com coeficiente dominante 1. Utilizamos a notação

$$1z^n = z^n, \text{ para } n = 0, 1, 2, \ldots.$$

Escrevemos $P \in \mathbb{C}[z]$ se P é um polinômio complexo na indeterminada z.

Segue diretamente da definição que dois polinômios complexos

$$\begin{cases} P(z) &= a_0 z^0 + a_1 z + a_2 z^2 + \cdots \\ \text{e} & \\ Q(z) &= b_0 z^0 + b_1 z + b_2 z^2 + \cdots \end{cases}$$

são iguais se e somente se temos $a_j = b_j$ para todo $j = 0, 1, 2, \ldots$.

A definição da soma de dois polinômios com coeficientes complexos e a definição da multiplicação de um polinômio (com coeficientes complexos) por um escalar complexo λ são dadas coeficiente a coeficiente. Isto é,

$$\begin{cases} (P+Q)(z) &= (a_0 + b_0)z^0 + (a_1 + b_1)z + (a_2 + b_2)z^2 + \cdots \\ \text{e} & \\ (\lambda P)(z) &= \lambda a_0 z^0 + \lambda a_1 z + \lambda a_2 z^2 + \cdots. \end{cases}$$

É trivial verificar que o conjunto dos polinômios com coeficientes complexos, munido de tais operações, é um espaço vetorial complexo.

Oswaldo Rio Branco de Oliveira

Definição (Produto de Polinômios).

- *Dados dois monômios z^n e z^m, definimos o produto (comutativo)*

$$z^n.z^m = z^{n+m}.$$

- *Sejam $P = P(z) = a_n z^n + \cdots + a_0 z^0$ e $Q = Q(z) = b_m z^m + \cdots + b_0 z^0$ polinômios. Definimos [estendendo linearmente a fórmula para produto de monômios]*

$$(PQ)(z) = \sum_{1\le j\le n, 1\le k\le m} a_j b_k z^{n+m}.$$

Tal produto é evidentemente comutativo.

Com a notação na definição acima, é trivial ver que

$$(PQ)(z) = \sum_{p=0}^{n+m} \left(\sum_{j+k=p} a_j b_k \right) z^p = a_n b_m z^{n+m} + \cdots + (a_0 b_1 + a_1 b_0) z + a_0 b_0 z^0.$$

Indicamos o polinômio $(PQ)(z)$ por $P(z)Q(z)$.

Proposição 1. *Se $P(z)$ é um polinômio complexo de grau n e $Q(z)$ é um polinômio complexo de grau m, então $P(z)Q(z)$ tem grau $n+m$. Isto é,*

$$grau(PQ) = grau(P) + grau(Q).$$

Prova. Trivial, se P ou Q é nulo e também trivial se P e Q não são nulos♣

É bem fácil ver que

$$\text{grau}(P+Q) \le \max\{\text{grau}(P), \text{grau}(Q)\}.$$

Se $P(z) = 8z^5 + z^3 + 7$ e $Q(z) = -8z^5$, então

$$\text{grau}(P+Q) = 3 < 5 = \text{grau}(P) = \text{grau}(Q).$$

Teorema 2 (Algoritmo de Euclides). *Consideremos dois polinômios complexos $P = P(z)$ e $D = D(z)$, com D não nulo. Então, existe um único par de polinômios complexos $Q = Q(z)$ e $R = R(z)$ verificando as condições*

$$P = DQ + R \quad e \quad grau(R) < grau(D).$$

Prova. O caso $\text{grau}(D) = 0$ é trivial.

Existência.

- Se $\text{grau}(P) < \text{grau}(D)$, pomos $Q = 0$ e $R = P$.
- Supondo $0 < \text{grau}(D) = m \leq n = \text{grau}(P)$, escrevamos

$$\begin{cases} P(z) = a_n z^n + a_{n-1} z^{n-1} + \cdots + a_1 z + a_0\,, & \text{com } a_{j's} \in \mathbb{C} \text{ e } a_n \neq 0\,, \\ D(z) = b_m z^m + b_{m-1} z^{m-1} + \cdots + b_1 z + b_0\,, & \text{com } b_{j's} \in \mathbb{C} \text{ e } b_m \neq 0\,. \end{cases}$$

Definindo os polinômios

$$Q_1(z) = \frac{a_n}{b_m} z^{n-m} \quad \text{e} \quad R_1 = P - Q_1 D,$$

segue $\text{grau}(R_1) < n$ e $P = Q_1 D + R_1$. Fim do sub-caso $\text{grau}(R_1) < m$.

Se $\text{grau}(R_1) \geq m$, aplicando um argumento análogo ao polinômio R_1 determinamos $Q_2 \in \mathbb{C}[z]$ tal que o polinômio $R_2 = R_1 - Q_2 D$ satisfaz

$$\text{grau}(R_2) < \text{grau}(R_1) \text{ e a identidade } R_1 = Q_2 D + R_2.$$

Se $\text{grau}(R_2) < m$, a tarefa se encerra. Caso contrário, por iteração obtemos

$$R_{k-1} = Q_k D + R_k, \text{ com } \text{grau}(R_k) < m,$$

e encontramos $P = Q_1 D + Q_2 D + \cdots + Q_k D + R_k = (Q_1 + \cdots + Q_k) D + R_k$.

Definindo $Q = Q_1 + \cdots + Q_k$ e $R = R_k$ completamos a prova da existência.

Unicidade. Sejam quatro polinômios complexos Q_1, Q_2, R_1 e R_2 tais que

$$\max(\text{grau}(R_1), \text{grau}(R_2)) < \text{grau}(D) \quad \text{e} \quad Q_1 D + R_1 = P = Q_2 D + R_2.$$

Obtemos $(Q_1 - Q_2) D = R_2 - R_1$. Logo,

$$\text{grau}[(Q_1 - Q_2) D] = \text{ grau } (Q_1 - Q_2) + \text{ grau}(D) = \text{ grau}(R_1 - R_2).$$

Donde segue $Q_1 - Q_2 = 0$ e $R_1 - R_2 = 0$♣

Os polinômios Q e R são ditos quociente e resto da divisão inteira de P por D.

Temos o seguinte mnemônico

$$\begin{array}{c|c} P & D \\ \hline R & Q \end{array}.$$

Se o resto R é zero (o polinômio nulo) dizemos que D divide P.

A seguir, distinguimos polinômio de função polinomial. Dado um polinômio

$$P(z) = a_n z^n + a_{n-1} z^{n-1} + \cdots + a_1 z + a_0 z^0,$$

passamos a tratar z como variável complexa [distinguindo-a de indeterminada].

Convenção. Definamos $z^0 = 1$, para todo z em $\mathbb{C}$.

Obtemos então a função polinomial

$$P : \mathbb{C} \to \mathbb{C}, \quad \text{dada por } P(z) = a_n z^n + \cdots + a_1 z + a_0 \text{ para cada } z \in \mathbb{C}.$$

Definição. *Seja $P(z)$ um polinômio complexo não nulo. Um número complexo α é um* zero *[ou* raiz*] de $P(z)$ se $P(\alpha) = 0$ [isto é, a função $P(z)$ se anula em α].*

Corolário 3 (Teorema de Descartes). *Seja α um número complexo. Temos*

$$P(\alpha) = 0 \ \text{ se e somente se } \ z - \alpha \ \text{ divide } \ P(z).$$

Prova.

($\Rightarrow$) Pelo Algoritmo de Euclides temos

$$P(z) = (z - \alpha)D(z) + R(z), \text{ com } \operatorname{grau}(R) < 1.$$

Logo, R é uma constante não nula ou o polinômio nulo. Substituindo $z = \alpha$ na expressão achada para $R(z)$, obtemos $R(\alpha) = 0$. Logo, $R(z)$ é o polinômio nulo. Donde segue $P(z) = (z - \alpha)D(z)$.

($\Leftarrow$) Seja $D(z)$ tal que $P(z) = (z - \alpha)D(z)$. Logo, $P(\alpha) = 0$♣

Teorema 4. *Seja $P(z)$ um polinômio complexo de grau $n \geq 1$. Então, $P(z)$ tem no máximo n zeros distintos em $\mathbb{C}$.*
Prova.

O caso $n = 1$ é trivial. Suponhamos $n \geq 2$.

Sejam $\alpha_1, \ldots, \alpha_n$ zeros distintos de $P(z)$. Pelo último corolário temos

$$P(z) = (z - \alpha_1)Q_1(z), \text{ com } \text{grau}(Q_1) = n - 1.$$

Logo, $Q_1(\alpha_2) = 0$ e temos

$$Q_1(z) = (z - \alpha_2)Q_2(z), \text{ com } \text{grau}(Q_2) = n - 2.$$

Por indução, encontramos

$$P(z) = (z - \alpha_1)\cdots(z - \alpha_n)Q_n(z), \text{ com } \text{grau}(Q_n) = 0.$$

Então, o polinômio Q_n é uma constante não nula. É agora evidente que $P(z)$ não tem nenhuma outra raiz além de $\alpha_1, \ldots, \alpha_n$♣

Corolário 5 (Princípio de Identidade Polinomial). *Seja $P(z)$ um polinômio complexo com grau$(P) \leq n$. Se $P(z)$ tem $n + 1$ zeros, então $P(z)$ é o polinômio nulo (todos os seus coeficientes são nulos).*
Prova. Segue imediatamente do corolário acima♣

Comentário 1. Dado um corpo finito $K = \{k_1, \ldots, k_n\}$, existe um polinômio não nulo $P(X)$, com coeficientes em K e na indeterminada X, tal que

$$P : K \to K, \text{ onde } P(k) = k \text{ para todo } k \in K, \text{ é a função polinomial nula.}$$

De fato, basta definirmos o polinômio (de grau n)

$$P(X) = (X - k_1)\cdots(X - k_n).$$

Comentário 2. Existe uma bijeção evidente entre o conjunto dos polinômios complexos na indeterminada z e o conjunto das sequências complexas quase-nulas

$$\{(a_j) = (a_j)_{j\in\mathbb{N}} : \text{ existe } n \in \mathbb{N} \text{ tal que } a_j = 0 \text{ para todo } j > n\}.$$

O conjunto das sequências quase-nulas, com as operações

$$(a_j) + (b_j) = (a_j + b_j) \quad \text{e} \quad \lambda(a_j) = (\lambda a_j),$$

é um espaço vetorial e uma base (algébrica) deste espaço é dada por

$$e_0 = (1, 0, 0, \dots,), \quad e_1 = (0, 1, 0, 0, \dots), \quad e_2 = (0, 0, 1, 0, 0, \dots), \dots.$$

Se (a_j) é uma sequência quase-nula com $a_j = 0$ para todo $j > n$, então temos

$$(a_n) = a_0 e_0 + a_1 e_1 + \cdots + a_n e_n.$$

As operações de adição de polinômios e multiplicação de um polinômio por um escalar, tornam o conjunto dos polinômios um espaço vetorial complexo.

A seguir, dado um polinômio $P(z) = a_n z^n + \cdots + a_1 z + a_0$ adotemos a notação

$$P(z) = a_0 z^0 + a_1 z^1 + \cdots + a_n z^n, \text{ com } z_0 = 1$$

Então, é trivial ver que a bijeção

$$\sum a_j z^j \mapsto (a_j)$$

é um isomorfismo entre espaços vetoriais. Identificamos o espaço dos polinômios complexos com o espaço das sequências complexas quase-nulas. Por tal bijeção,

$$z^n \text{ corresponde ao vetor } e_n, \quad \text{para cada } n = 0, 1, 2, \dots.$$

Identificando $z^n \equiv e_n$, o espaço dos polinômios complexos na indeterminada z é o espaço vetorial complexo gerado pelo conjunto linearmente (logo, uma base)

$$\{z^0, z = z^1, z^2, z^3, \dots\}.$$

Todo polinômio $P(z)$ não nulo é dado por uma única combinação linear finita, com coeficientes não nulos, de elementos da base (de monômios) $\{z^0, z, z^2, \dots\}$.

Comentário 3. Seja V um espaço vetorial complexo (de dimensão finita ou não - o comentário também vale para espaços vetoriais reais). Consideremos um operador linear

$$T : V \to V$$

O conjunto dos operadores lineares definidos em V é um espaço vetorial.

No espaço dos operadores lineares de V em V, introduzimos um produto. Dados dois operadores $T : V \to V$ e $S : V \to V$, definimos o **produto** (composição)

$$S \circ T : V \to V.$$

Notação. $ST = S \circ T$.

Fixemos um operador linear $T : V \to V$. Seja $I : V \to V$ o operador identidade. Definamos, por indução,

$$T^0 = I \quad \text{e} \quad T^n = T \circ T^{n-1}, \text{ se } n \geq 1 \qquad [\text{logo, } T^1 = T].$$

Dados n e m, é trivial ver que [por indução em $n + m$ e $n + m = 0$ é óbvio]

$$T^n T^m = T^{n+m}.$$

Seja $P(X) = a_n X^n + \cdots + a_0 X^0$ um polinômio na indeterminada X e com coeficientes complexos. Definimos

$$P(T) = a_n T^n + \cdots + a_0 T^0.$$

Analogamente, dado $Q(X) = b_m X^m + \cdots + b_0 X^0$ com coeficientes complexos, segue

$$Q(T) = b_m T^m + \cdots + b_0 T^0.$$

Proposição 6. *Mantenhamos a notação neste comentário. Temos*

$$P(T)Q(T) = \sum_{\substack{0 \leq j \leq n \\ 0 \leq k \leq m}} (a_j T^j)(b_k T^k) = \sum_{\substack{0 \leq j \leq n \\ 0 \leq k \leq m}} a_j b_k T^{j+k} = (PQ)(T) \clubsuit$$

Exemplo 1. Consideremos o polinômio com coeficientes complexos

$$P(X) = a_n X^n + \cdots + a_1 X + a_0 X^0 \quad [\text{na indeterminada } X].$$

Consideremos o espaço vetorial complexo

$$C^\infty(\mathbb{R};\mathbb{C}) = \{f : \mathbb{R} \to \mathbb{C} : f \text{ é infinitamente derivável}\}.$$

[As curvas infinitamente deriváveis no plano complexo (isomorfo a $\mathbb{R}^2$).]

Indiquemos a variável real pela letra t. Consideremos o operador linear

$$D : C^\infty(\mathbb{R};\mathbb{C}) \to C^\infty(\mathbb{R};\mathbb{C})$$

definido por

$$D(f)(t) = f'(t).$$

É claro que D (operador derivação de primeira ordem) é linear. Escrevamos

$$D = \frac{d}{dt}.$$

Dada uma função f em $C^\infty(\mathbb{R};\mathbb{C})$, são usuais as notações

$$f^{(n)} = \frac{d^n f}{dt^n} \qquad \text{e} \qquad f^{(0)} = f.$$

É óbvio que

$$f^{(n)} = \left(\frac{d}{dt}\right)^n (f).$$

Seja $I : C^\infty(\mathbb{R};\mathbb{C}) \to C^\infty(\mathbb{R};\mathbb{C})$ o operador identidade. Escrevamos

$$\frac{d^0}{dt^0} = \left(\frac{d}{dt}\right)^0 = I.$$

Com as notações introduzidas temos

$$P\left(\frac{d}{dt}\right) = a_n \frac{d^n}{dt^n} + \cdots + a_1 \frac{d}{dt} + a_0 I.$$

Suponhamos que valha a seguinte fatoração para o polinômio $P(X)$,

$$P(X) = Q(X)R(X).$$

A Proposição 6 então garante

$$P\left(\frac{d}{dt}\right) = Q\left(\frac{d}{dt}\right) R\left(\frac{d}{dt}\right) \clubsuit$$

Fatorar operadores é muito importante na resolução de problemas.

Exemplo 2. Analogamente ao Exemplo 1, consideremos um espaço de Hilbert H (isto é, H é um espaço vetorial complexo, com produto interno e completo).

Sejam $T : H \to H$ um operador linear e um polinômio complexo

$$P(X) = a_n X^n + \cdots + a_0 X^0 \qquad [\text{na indeterminada } X].$$

Então,

$$P(T) = a_n T^n + \cdots + a_0 T^0 \qquad [\text{com } T^0 = I],$$

é um operador linear definido no espaço de Hilbert H ♣

Agradecimentos. Agradeço aos comentários e sugestões de Paulo Agozzini.

REFERÊNCIAS

1. Fraleigh, J. B., *A First Course In Abstract Algebra*, 7th ed., Addison-Wesley, 2003.

Departamento de Matemática
Universidade de São Paulo
e-mail: oliveira@ime.usp.br
`http://www.ime.usp.br/~oliveira`