Uma prova elementar do Teorema Fundamental da Álgebra

Doherty Andrade

Universidade Estadual de Maringá - doherty@dma.uem.br

Departamento de Matemática - 87020-900 Maringá-PR, Brazil

Sumário

1. Introdução	1
2. Resultados Preliminares	2
3. Polinômios Sobre um Corpo	5
4. O Teorema Fundamental da Álgebra	12
5. Prova do Teorema Fundamental	15

Resumo: Nestas notas apresentamos uma prova elementar do Teorema Fundamental da Álgebra.

1. Introdução

O problema de encontrar raízes de um polinômio é antigo. Já por volta de 1600 AC os babilônios possuíam tabelas que permitiam resolver equações quadráticas. Os gregos antigos resolviam equações quadráticas por meio de construções geométricas, não existia sinal algum de formulação algébrica até 100 DC. Os gregos tinham métodos aplicáveis a equações cúbicas envolvendo interseção de cônicas.

A solução algébrica da cúbica era desconhecida e em 1494 Pacioli em sua “Summa Arithmetica” observa que a solução das equações $x^3 + mx = n$ e $x^3 + n = mx$ eram impossíveis. Na Renascência os matemáticos de Bolonha descobriram que a equação cúbica geral podia ser reduzida a três casos básicos

$x^3 + px = q$, $x^3 = px + q$ e $x^3 + q = px$. A separação em casos foi necessário pois eles não conheciam números negativos.

Scipio del Ferro resolveu todos os três casos e certamente passou o seu método a um estudante, Fior. Nicollo Fontana (ou Tartaglia) em 1535 re-descobriu o método. Fontana demonstrou o seu método numa competição pública, mas recusou-se a revelar os detalhes. Finalmente ele foi convencido pelo físico Girolano Cardano a revelar o segredo, mas com a condição de não revelar a mais ninguém. Quando a “Ars Magna” de Cardano apareceu em 1545 ela continha uma completa discussão da solução de Fontana. Continha também o método de Ludovico Ferrari para resolver a equação de quarto grau por redução a uma cúbica. Girolano sentiu-se desobrigado de cumprir o trato com Tartaglia pois descobriu que o seu método de solução já era conhecido. A solução de Fontana para $x^3 + px = q$ é

$$x = \sqrt[3]{\frac{q}{2} + \sqrt{\frac{p^3}{27} + \frac{q^2}{4}}} + \sqrt[3]{\frac{q}{2} - \sqrt{\frac{p^3}{27} + \frac{q^2}{4}}}.$$

A expressão acima só envolve os coeficientes da equação, adição, subtração, multiplicação, divisão e extração de raiz. Tais expressões são conhecidas como expressões radicais.

Vamos apresentar nestas notas uma prova elementar do famoso teorema fundamental da Álgebra.

2. Resultados Preliminares

Seja $(A, +, \cdot)$ um anel. Um polinômio f sobre A é uma sequência

$$(a_0, a_1, \dots, a_n, \dots)$$

de elementos de A na qual apenas um número finito de termos são diferentes de zero do anel A .

Segue que para cada polinômio f existe um natural d , que depende de f , tal que para cada $n > d$ tem-se $a_n = 0$. Se $a_d \neq 0$, mas $a_n = 0$ para todo $n > d$, então d é chamado o grau do polinômio f .

Polinômios da forma $(a_0, 0, \dots, 0, \dots)$ são chamados de polinômios escalares. Se $a_0 = 0$ então o polinômio será dito polinômio nulo. O grau do polinômio nulo será admitido como sendo (-1) , embora alguns autores não definem o grau para este polinômio.

Observamos que os polinômios

$$(a_0, a_1, \dots, a_n, \dots) = (b_0, b_1, \dots, b_n, \dots)$$

se e somente se $a_i = b_i$.

O conjunto de todos os polinômios sobre A munido das operações abaixo se transformará em um anel:

Adição:

$$(a_0, \dots, a_n, \dots) + (b_0, \dots, b_n, \dots) = (a_0 + b_0, \dots, a_n + b_n, \dots),$$

Multiplicação:

$$(a_0, a_1, \dots, a_n, \dots) \cdot (b_0, b_1, \dots, b_n, \dots) = (c_0, c_1, \dots, c_k, \dots),$$

onde

$$c_k = \sum_{i+j=k} a_i b_{k-i}.$$

Denotaremos por $(A[x], +, \cdot)$ o anel dos polinômios sobre o anel A com as operações definidas acima. É fácil mostrar que se $(A, +, \cdot)$ é um anel comutativo com identidade então $(A[x], +, \cdot)$ também é um anel comutativo com identidade.

Note que se $f \neq 0$ e $g \neq 0$ são polinômios sobre o anel $(A, +, \cdot)$ então $\text{grau}(f + g) \leq \max\{\text{grau}(f), \text{grau}(g)\}$. Vale a igualdade se f e g têm graus diferentes. Além disso, $f \cdot g = 0$ ou $\text{grau}(f \cdot g) \leq \text{grau}(f) + \text{grau}(g)$. O anel $\mathbb{Z}_m[x]$ fornece exemplos para estas observações.

Quando $(A, +, \cdot)$ é um domínio de integridade, $f \neq 0$ e $g \neq 0$ são polinômios sobre A , o $\text{grau}(f \cdot g) = \text{grau}(f) + \text{grau}(g)$. E concluímos que $f \cdot g \neq 0$. Segue que se $(A, +, \cdot)$ é um domínio de integridade, então $(A[x], +, \cdot)$ é um domínio de integridade.

Observação 1 *É usual representar um polinômio*

$$f = (a_0, a_1, \dots, a_n, \dots)$$

sobre um anel A por

$$a_0 + a_1x + a_2x^2 + \dots + a_nx^n.$$

Neste caso também escrevemos

$$f(x) = a_0 + a_1x + a_2x^2 + \dots + a_nx^n.$$

Assim o polinômio $(a, 0, 0, \dots)$ representa o polinômio constante $ax^0 = a$. Segue que a representa ou um elemento de A ou um elemento de $A[x]$.

Definição 2 Uma função $\varphi : A \rightarrow A$ é chamada uma função polinomial se existe um polinômio $f(x) = a_0 + a_1x + \dots + a_nx^n$ sobre o anel A tal que

$$\varphi(b) = a_0 + a_1b + \dots + a_nb^n, \quad \forall b \in A.$$

É comum usar a mesma letra para representar a função polinomial e o polinômio que a representa.

Em $\mathbb{Z}_2[x]$ o polinômio $p(x) = x^2 - x$ não é o polinômio nulo, mas $\varphi : \mathbb{Z}_2 \rightarrow \mathbb{Z}_2$ dada por $\varphi(b) = b^2 - b$ é uma função identicamente nula.

Se $f(b) = 0$ dizemos que $b \in A$ é uma raiz da equação funcional $f(x) = 0$. Segue que todo elemento de A é uma raiz do polinômio nulo.

Seja $(A, +, \cdot)$ um anel e suponha que para algum $u \in A$ tem-se $a \cdot u = u \cdot a$, $\forall a \in A$. Existe uma aplicação dada por

$$\sum_{i=0}^n a_i \cdot x^i \mapsto \sum_{i=0}^n a_i \cdot u^i$$

que é claramente um homomorfismo de $A[x]$ em A .

Teorema 3 (Algoritmo da divisão) Seja $(A, +, \cdot)$ um anel comutativo com identidade $1 \in A$. Se $a(x) \in A[x]$ e $b(x) \in A[x]$ é um polinômio mônico, então existem polinômios $q(x), r(x) \in A[x]$ tais que

$$a(x) = b(x) \cdot q(x) + r(x)$$

com $r(x) = 0$ ou $\text{grau}(r(x)) < \text{grau}(b(x))$

Demonstração: Há dois casos a considerar:

1i) $\text{grau}(b) > \text{grau}(a)$:

Neste caso escolhemos $q = 0$ e $r = a$.

2i) $\text{grau}(b) \leq \text{grau}(a)$:

Neste caso a prova é por indução. Fixemos $b(x)$ polinômio de grau ≥ 0 .

Sejam

$$\begin{aligned} a(x) &= a_{n+s}x^{n+s} + \dots + a_0, \quad s \geq 0 \\ b(x) &= 1x^n + \dots + b_0, \end{aligned}$$

se $s = 0$ o teorema é óbvio. Suponha que o resultado seja verdadeiro para todo polinômio de grau menor $(n + s)$. Provaremos que o mesmo é verdade para polinômios de grau $(n + s)$. De fato, seja

$$a'(x) = a(x) - (a_{n+s}x^s b(x)).$$

Logo,

$$a(x) = a_{n+s}x^s b(x) + a'(x).$$

Como $\text{grau}(a') = (n - 1 + s) < (n + s) = \text{grau}(a)$, temos pela hipótese de indução que existem $q_0(x), r(x) \in A[x]$ tais que

$$a'(x) = b(x)q_0(x) + r(x)$$

onde $r = 0$ ou $\text{grau}(r) < \text{grau}(b)$.

Segue que

$$\begin{aligned} a(x) &= a_{n+s}x^s b(x) + b(x)q_0(x) + r(x) \\ &= [a_{n+s}x^s + q_0(x)]b(x) + r(x), \end{aligned}$$

com $r = 0$ ou $\text{grau}(r) < \text{grau}(b)$. ■

3. Polinômios Sobre um Corpo

Nesta seção veremos alguns resultados importantes da teoria dos polinômios sobre um corpo K .

Teorema 4 Seja K um corpo, a e $b \in K[x]$. Se $b \neq 0$, então existem polinômios únicos $q, r \in K[x]$ tais que

$$a = bq + r, \quad r = 0 \text{ ou } \text{grau}(r) < \text{grau}(b).$$

Demonstração: A existência é provado de modo análogo ao teorema anterior. Provaremos a unicidade.

Sejam $q_1(x), q_2(x), r_1(x)$ e $r_2(x)$ polinômios de $K[x]$ tais que

$$\begin{aligned} a(x) &= q_1(x)b(x) + r_1(x) \\ a(x) &= q_2(x)b(x) + r_2(x) \end{aligned}$$

onde $r_i(x) = 0$ ou $\text{grau}(r_i(x)) < \text{grau}(b(x))$, $i = 1, 2$.

Logo,

$$(q_1(x) - q_2(x)) \cdot b(x) = r_2(x) - r_1(x).$$

Então, o lado esquerdo é zero ou é um polinômio de grau maior ou igual ao grau de $b(x)$, enquanto o lado direito é zero ou tem grau menor que o grau de $b(x)$. Assim a igualdade só pode ocorrer se ambos os lados são iguais a zero. Logo, $r_1 = r_2$ e $q_1 = q_2$.

Corolário 5 (teorema do resto) Se $f(x) \in K[x]$ é qualquer polinômio e $(x - a) \in K[x]$, então

$$f(x) = (x - a) \cdot q(x) + f(a),$$

para algum $q(x) \in K[x]$.

Demonstração: Do teorema acima é imediato que

$$f(x) = (x - a) \cdot q(x) + r(x),$$

para algum $q(x) \in K[x]$ e $r(x) = 0$ ou $\text{grau}(r(x)) < 1$. Segue que $r(x) = r$ é polinômio constante. Mas $f(a) = r$, e assim

$$f(x) = (x - a) \cdot q(x) + f(a).$$

Corolário 6 (teorema da raiz) Seja $f(x) \in K[x]$ um polinômio e $a \in K$ raiz de f . Então $(x - a)$ divide $f(x)$.

Demonstração: Como $f(x) = (x - a) \cdot q(x) + f(a)$ e $f(a) = 0$, então $f(x) = (x - a) \cdot q(x)$. Isto é, $(x - a)$ divide $f(x)$. ■

Corolário 7 Seja K um corpo e $f(x) = a_0 + a_1x + \cdots + a_nx^n$ um polinômio não nulo em $K[x]$ de grau n . Então, f tem no máximo n raízes em K .

Demonstração: A demonstração é uma aplicação do algoritmo da divisão. Se f não possui raiz, não há o que provar. Se f tem grau 1, o resultado é verdadeiro. Suponha que o resultado seja verdadeiro para todos os polinômios de grau menor ou igual a $(n - 1)$. Seja f de grau n . Se f não tem raiz em K não há nada a ser provado. Caso contrário seja $a \in K$ uma raiz de f . Como $(x - a)$ divide f então podemos escrever

$$f(x) = (x - a)q(x)$$

para algum $q(x) \in K[x]$ de grau $(n - 1)$. Notemos que toda raiz de $q(x)$ é também raiz de f e por outro lado se $b \neq a$ é raiz de f então temos que $(b - a)q(b) = 0$ e portanto b é raiz de $q(x)$. Logo, as raízes de f são as raízes de $q(x)$ e a . Como $q(x)$ tem grau $(n - 1)$ segue da hipótese de indução que $q(x)$ tem no máximo $(n - 1)$ raízes. Logo, $f(x)$ tem no máximo n raízes. ■

Se L e K são dois corpos tais que $L \supset K$, dizemos que L é uma extensão de K . É imediato do teorema anterior que se $f(x) = a_nx^n + \cdots + a_1x + a_0$

é polinômio não nulo em $K[x]$ de grau n , então $f(x)$ possui no máximo n raízes em qualquer extensão L de K .

Dizemos que um corpo K é algebricamente fechado se todo polinômio não escalar de $K[x]$ tem pelo menos uma raiz em K . Segue do teorema da raiz, que se K é um corpo algebricamente fechado então todo polinômio não escalar de $K[x]$ tem todas as raízes em K .

Seja $f(x) \in K[x]$ com grau pelo menos 1. Dizemos que f é polinômio irredutível sobre K se toda vez que

$$f(x) = g(x) \cdot h(x), \quad g, h \in K[x]$$

implicar que $g(x) = a$ constante ou $h(x) = b$ constante.

Se f não for irredutível, então f é dito redutível sobre K .

Teorema 8 Sejam K um corpo e $p(x) \in K[x]$ polinômio. Então, $p(x)$ é irredutível sobre K se e somente se $\langle p(x) \rangle$ é ideal maximal.

Demonstração: Suponha $p(x)$ irredutível sobre K e $I = \langle p(x) \rangle$ ideal gerado por $p(x)$. Como $p(x)$ tem grau maior ou igual a 1, então $I \neq K[x]$.

Seja $J = \langle h(x) \rangle$ outro ideal de $K[x]$ tal que $I \subset J \subseteq K[x]$, com $I \neq J$. Provaremos que $J = K[x]$. Como $p(x) \in J$ segue que

$$p(x) = g(x) \cdot h(x)$$

para algum $g(x) \in K[x]$. Mas $p(x)$ é irredutível sobre K , assim $g(x) = a$ constante ou $h(x) = b$ constante. Se $g(x) = a$, então $a \neq 0$ e portanto $h(x) = a^{-1} \cdot p(x) \in I$ e portanto $J \subset I$ o que nos dá $I = J$, que é uma contradição. Por outro lado, se $h(x) = b$ constante, então $b \neq 0$ e portanto

$$J = \langle h(x) \rangle = \langle b \rangle = K[x].$$

Logo, $\langle p(x) \rangle$ é ideal maximal.

Suponha $I = \langle p(x) \rangle$ ideal maximal. Então, $I \neq K[x]$ e portanto $p(x)$ tem grau pelo menos 1. Provaremos que $p(x)$ é irredutível sobre K . Suponha que $p(x) = g(x) \cdot h(x)$. Assim, $I \subset J = \langle h(x) \rangle$ e como I é maximal então $I = J$ ou $J = K[x]$.

Se $I = J$ então $h(x) \in I = \langle p(x) \rangle$, e isto diz que

$$h(x) = f(x) \cdot p(x),$$

para algum $f(x) \in K[x]$. Segue que

$$p(x) = g(x) \cdot f(x) \cdot p(x)$$

e como $K[x]$ é domínio de integridade obtemos que

$$f(x) \cdot g(x) = 1.$$

Logo, $g(x) = a$ constante e portanto $p(x)$ é polinômio irredutível sobre K .

Se $J = K[x]$, segue que $h(x) = b \neq 0$ constante e portanto $p(x)$ é irredutível sobre K . ■

Corolário 9 Seja K um corpo e $p(x) \in K[x]$. São equivalentes:

- 1i) $p(x)$ é irredutível sobre K ,
- 2i) $I = \langle p(x) \rangle$ é ideal maximal em $K[x]$,
- 3i) $K[x]/I$ é um corpo.

Teorema 10 $\mathbb{R}[x]/I$ é um corpo isomorfo a $\mathbb{C}$, onde $I = \langle (x^2 + 1) \rangle$.

Demonstração: Como $p(x) = x^2 + 1$ é irredutível sobre $\mathbb{R}$, então $I = \langle (x^2 + 1) \rangle$ é um ideal maximal de $\mathbb{R}[x]$. Logo, $\mathbb{R}[x]/I$ é um corpo. Os elementos $\mathbb{R}[x]/I$ são classes residuais da forma

$$\overline{f(x)} = \{g(x) \in \mathbb{R}[x]; f(x) \equiv g(x) \pmod{(x^2 + 1)}\}.$$

Como

$$f(x) = q(x) \cdot (x^2 + 1) + r(x),$$

com $r(x) = 0$ ou $\text{grau}(r(x)) \leq 1$ então podemos associar a cada classe $\overline{f(x)}$ um único polinômio $r(x) = a + bx$.

Observando que $x^2 = -1$, definimos

$$\Psi : \mathbb{C} \rightarrow \mathbb{R}[x]/I$$

dada por $\psi(a + bi) = \overline{a + bx}$. Provaremos que Ψ é um homomorfismo de corpo. É claro que Ψ é sobrejetora, para provar que é homomorfismo

$$\begin{aligned} \Psi((a + a') + (b + b')i) &= \overline{(a + a') + (b + b')x} \\ &= \overline{(a + bx) + (a' + b'x)} \\ &= \Psi(a + bi) + \Psi(a' + b'i) \end{aligned}$$

Do mesmo modo provamos para a multiplicação:

$$\begin{aligned} \Psi((a + bi) \cdot (a' + b'i)) &= \Psi((aa' - bb') + i(ab' + ba')) \\ &= \overline{(ab' + ba')x + (aa' - bb')} \\ &= \overline{(a + bx)(a' + b'x)} \\ &= \Psi(a + bi)\Psi(a' + b'i) \end{aligned}$$

É fácil ver que o núcleo do homomorfismo é $\{0\}$ e portanto Ψ é um isomorfismo. ■

Seja K um corpo e $f(x), g(x) \in K[x]$. Dizemos que $d(x) \in K[x]$ é um máximo divisor comum de f e g se:

- 1i) $d|f$ e $d|g$,
- 2i) se $d' \in K[x]$ é tal que $d'|f$ e $d'|g$, então $d'|d$.

Lema 11 Se d é um MDC entre f e g , então cd é um MDC entre f e g , para todo $c \neq 0$.

Demonstração: Se $d' = cd$, então como $f = dq$, segue que $f = (cd)(\frac{1}{c}q)$. Ou seja, $d'|f$. Analogamente, $d'|g$. Além disso, se $p|f$ e $p|g$, então $p|d$ e portanto $p|(cd)$. Logo, d' é um MDC entre f e g . ■

O lema acima diz que existem infinitos $d \in K[x]$ que são máximo divisor comum para f e g .

Teorema 12 (teorema de Bezout) Dados f e g em $K[x]$, existe $d \in K[x]$ um máximo divisor comum entre f e g . Além disso, existem h_1 e h_2 em $K[x]$ tais que

$$d = f \cdot h_1 + g \cdot h_2.$$

Demonstração: Nesta prova usaremos que todo ideal de $K[x]$ é principal. Seja

$$I = \langle f, g \rangle = \{a(x)f(x) + b(x)g(x); a(x), b(x) \in K[x]\}$$

o ideal gerado por f e g . Como todo ideal de $K[x]$ é principal, então existe $d \in K[x]$ tal que $I = \langle d \rangle$. Provaremos que d é um máximo divisor comum entre f e g .

De fato, como $f \in I$ e $g \in I$, então

$$\begin{aligned} f(x) &= a_1(x)d(x) \\ g(x) &= b_1(x)d(x) \end{aligned}$$

para algum $a_1(x) \in K[x]$ e algum $b_1(x) \in K[x]$. Logo, $d|f$ e $d|g$. Além disso, como $d \in I$ segue que existem $h_1, h_2 \in K[x]$. tais que

$$d = h_1f + h_2g.$$

Assim, se $d' \in K[x]$ é tal que $d'|f$ e $d'|g$ então $d'|(h_1f)$ e $d'|(h_2g)$ ou seja $d'|d$, mostrando que d é um máximo divisor comum entre f e g . ■

Corolário 13 Seja K um corpo, $p, f, g \in K[x]$. Se p é irredutível sobre K e $p|(fg)$, então $p|f$ ou $p|g$.

Demonstração: Se p não divide f , então 1 é um máximo divisor comum entre f e p . Logo, pelo teorema de Bezout, existem h_1 e h_2 polinômios de $K[x]$ tais que

$$1 = p(x)h_1(x) + f(x)h_2(x).$$

Logo,

$$g(x) = [p(x)g(x)h_1(x) + [f(x)g(x)]h_2(x)].$$

Como p divide (fg) e p divide (pg) , então p divide g . ■

Corolário 14 Se $f = gq + r$, $r \neq 0$ e d é um máximo divisor comum entre f e g , então d é um máximo divisor comum entre g e r .

Demonstração: Seja d' um máximo divisor comum entre g e r . Como $r = f - gq$, então d' divide r . Logo, d' divide r e d' divide g e portanto d' divide d' . Por outro lado, como $f = gq + r$ e d' divide g e d' divide r , então d' divide f . Segue que d' divide f e d' divide g e portanto d' divide d . Logo, $d = c \cdot d'$ para alguma constante $c \in K$. ■

Observação 15 *Este corolário dá origem ao algoritmo das divisões sucessivas para determinar um máximo divisor comum entre dois polinômios. Neste algoritmo o último resto não nulo é um máximo divisor comum.*

Teorema 16 Seja K um corpo. Todo polinômio $f(x) \in K[x]$ de grau ≥ 1 é irredutível ou se decompõe num produto

$$p_1(x) \cdot p_2(x) \cdots p_n(x)$$

de polinômios irredutíveis.

Além disso, os polinômios $p_1, p_2, \dots, p_n$ são determinados de modo único, a menos de um rearranjo e a menos de fatores constantes não nulos.

Demonstração: Primeiro provaremos a possibilidade de fatoração. A prova é por indução sobre o grau(f). Se o grau de f é igual a 1, então é claro que f é irredutível.

Suponha que todo polinômio $g \in K[x]$ de grau menor que grau(f) pode ser escrito como produto de irredutíveis ou é irredutível. Vamos provar que o

mesmo vale para f . Se f é irredutível, não há o que provar. Se f é redutível, então

$$f = gh,$$

onde $g, h \in K[x]$ são polinômios de $K[x]$ com

$$\begin{aligned} \text{grau}(g) &< \text{grau}(f) \\ \text{grau}(h) &< \text{grau}(f). \end{aligned}$$

Pela hipótese de indução g e h são irredutíveis ou são produto de irredutíveis:

$$\begin{aligned} g(x) &= g_1(x) \cdot g_2(x) \cdots g_k(x) \\ h(x) &= h_1(x) \cdot h_2(x) \cdots h_l(x). \end{aligned}$$

Logo, $f(x)$ é irredutível ou é um produto de irredutíveis:

$$f(x) = g_1(x) \cdot g_2(x) \cdots g_k(x) \cdot h_1(x) \cdot h_2(x) \cdots h_l(x).$$

Provaremos agora a unicidade da decomposição:
suponha que

$$f(x) = p_1(x) \cdots p_r(x) = q_1(x) \cdots q_s(x)$$

onde p_i e q_i são irredutíveis. Desta igualdade temos que $p_1 | q_i$ para algum $i = 1, 2, \dots, s$. Como q_i é irredutível, então $p_1 = c_i q_i$, para alguma constante c_i . Rearranjando os polinômios q_i podemos supor que $q_i = p_1$. Segue que

$$\begin{aligned} g(x) &= g_1(x) \cdot g_2(x) \cdots g_k(x) \\ h(x) &= h_1(x) \cdot h_2(x) \cdots h_l(x). \end{aligned}$$

Cancelando temos

$$f(x) = p_2(x) \cdots p_r(x) = c_1 q_2(x) \cdots q_s(x).$$

Repetindo o argumento, concluímos que após uma possível permutação dos polinômios q_i , existem constantes c_i tais que

$$p_i(x) = c_i q_i(x), \quad i = 1 \cdots, s.$$

Isto prova a unicidade. ■

Corolário 17 Seja $f \in K[x]$ polinômio de grau pelo menos 1. Então f admite uma fatoração

$$f(x) = c p_1(x) \cdot p_2(x) \cdots p_r(x)$$

de polinômios irredutíveis mônicos, determinados de modo único a menos de uma permutação.

Corolário 18 Se K é um corpo algebricamente fechado, todo polinômio $f \in K[x]$ de grau ≥ 1 admite uma fatoração

$$f(x) = c(x - a_1) \cdot (x - a_2) \cdots (x - a_n)$$

com $a_i \in K$ e $c \in K$. Os fatores $(x - a_i)$ são determinados de modo único a menos de uma permutação.

Demonstração: A prova é imediato do teorema e do teorema da raiz.

4. O Teorema Fundamental da Álgebra

Nesta secção provaremos que $\mathbb{C}$ é algebricamente fechado, isto é, os únicos polinômios irreduzíveis de $\mathbb{C}[x]$ são os polinômios lineares $a + bx$.

O corpo $\mathbb{C}$ foi construído para conter todas as raízes de polinômios reais irreduzíveis, é o que provaremos a seguir. É fácil ver que o polinômio $g(x) = x^2 + ax + b$, com $a, b \in \mathbb{C}$ tem raízes em $\mathbb{C}$, pois

$$g(x) = \left(x + \frac{a}{2} + d\right) \cdot \left(x + \frac{a}{2} - d\right),$$

onde $\frac{a^2}{4} - b = d^2$. Assim todo polinômio de grau 2 se fatora num produto de dois polinômios complexos lineares.

Para polinômios de grau 3, $f(x) = x^3 + bx^2 + cx + d$, com coeficientes em $\mathbb{C}$, fazendo $h = -\frac{b}{3}$ obtemos

$$f(y + h) = y^3 + py + q, \quad p, q \in \mathbb{C}.$$

Agora usando a substituição de Viète $y = z - \frac{p}{3z}$ obtemos que

$$f\left(z - \frac{p}{3z}\right) = z^3 - \frac{p^3}{27z^3} + q.$$

Assim,

$$z^3 - \frac{p^3}{27z^3} + q = 0$$

é uma equação quadrada em z^3 e portanto

$$z_1^3 = \frac{-q + \sqrt{-\frac{D}{27}}}{2},$$

$$z_2^3 = \frac{-q - \sqrt{-\frac{D}{27}}}{2},$$

são as raízes, onde $D = -(4p^3 + 27q^2)$. Como

$$z^3 + z(-3rs + (r^3 + s^3)) = (z + r + s)(z + wr + w^2s)(z + w^2r + ws)$$

onde $p = -3rs$ e $q = r^3 + s^3$, segue que as raízes de $y^3 + py + q = 0$ são

$$\begin{aligned} y_1 &= z_1 + z_2 \\ y_2 &= wz_1 + w^2z_2 \\ y_3 &= w^2z_1 + wz_2, \end{aligned}$$

onde $w \in \mathbb{C}$ é a raiz cúbica da unidade.

A equação polinomial geral do quarto grau pode ser reduzida, via mudança de variáveis, para

$$y^4 + py^2 + qy + r = 0,$$

e em seguida reduzida, com $u, v, w \in \mathbb{C}$ convenientes, para a forma

$$\left(y^2 + \frac{u}{2}\right)^2 - (vy + w)2 = 0.$$

Comparando obtemos que

$$\begin{aligned} p &= u - v^2, \\ q &= -2vw, \\ r &= \frac{u^2}{4} - w^2. \end{aligned}$$

Substituindo em $r = \frac{u^2}{4} - w^2$ obtemos

$$v^6 + 2pqv^4 + (p^2 - 4r)v^2 - q^2 = 0,$$

que é uma equação cúbica em v^2 e as raízes desta equação determinar explicitamente por meio de radicais.

Até grau 4 as raízes são obtidas por meio de radicais. Não é verdade para polinômios gerais com graus maior ou igual a 5, este é o famoso teorema de Abel. Apesar do teorema de Abel, temos

Teorema 19 (Teorema Fundamental da Álgebra) Todo polinômio $p(z)$ em $\mathbb{C}[z]$ de grau maior ou igual a 1, tem uma raiz em $\mathbb{C}$. Isto é, $\mathbb{C}$, é algebricamente fechado.

A prova elementar que apresentaremos é basicamente a prova dada por Argand em 1814.

Observamos que um polinômio $p(z)$ com coeficientes complexos pode ser escrito da forma

$$p(z) = p(x + iy) = p_1(x, y) + ip_2(x, y),$$

onde $p_1(x, y)$ e $p_2(x, y)$ são polinômios reais nas variáveis reais x, y . Segue que

$$|p(z)| = \sqrt{p_1(x, y)^2 + p_2(x, y)^2},$$

que é claramente função contínua nas variáveis x, y . Na prova usaremos o fato básico do Cálculo que uma função contínua num disco fechado D do plano tem um mínimo em D . A prova está dividida em duas partes, provaremos que:

a) existe um ponto z_0 no plano complexo tal que

$$|p(z_0)| \leq |p(z)|, \quad \forall z \in \mathbb{C},$$

b) se z_0 é o ponto de mínimo global determinado na primeira parte, então $p(z_0) = 0$.

Primeiramente vamos provar um lema que será útil na prova do teorema fundamental.

Lema 20 Se $f(z) \in \mathbb{C}[z]$ é polinômio de grau maior ou igual a 1, então dado $M > 0$ existe $R > 0$ tal que se $|z| > R$, então $|f(z)| \geq M$.

Demonstração: A prova é sobre indução sobre o grau de f . Se o grau de f é igual a 1, então $f(z) = a + bz, b \neq 0$. Logo,

$$|f(z)| = |a + bz| \geq |bz| - |a| = |b| \cdot |z| - |a|.$$

Dado $M > 0$ escolha

$$R = \frac{M + |a|}{|b|}$$

e assim se $|z| > R$ então $|f(z)| > M$.

Assuma que o lema é verdade para polinômios de grau $(d - 1)$. Então $f(z)$ pode ser escrito na forma $f(z) = a + zf_1(z)$, onde $f_1(z)$ tem grau $(d - 1)$. Dado $M > 0$ escolha $R \geq 1$ tal que para $|z| > R$, $|f_1(z)| > M + |a|$, isto é possível pela hipótese de indução.

Então, para $|z| > R$,

$$\begin{aligned} |f(z)| &= |a + zf_1(z)| \\ &\geq |zf_1(z)| - |a| \\ &= |z| \cdot |f_1(z)| - |a| \\ &\geq |f_1(z)| - |a| \\ &\geq M + |a| - |a| = M, \end{aligned}$$

provando assim o lema.

5. Prova do Teorema Fundamental

Para provar o teorema fundamental, seja

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

Existe $R > 0$ tal que se $|z| > R$, então $|p(z)| > 1 + |a_0|$, para todo $z \in \mathbb{C}$.

Seja

$$D = \{z \in \mathbb{C}; |a| \leq R\}.$$

Como D é fechado e limitado no plano, então do Cálculo sabemos que existe $z_0 \in D$ tal que

$$|p(z_0)| \leq |p(z)|, \quad \forall z \in D.$$

Pela escolha de D , temos que

$$|p(z_0)| \leq |p(z)|, \quad \forall z.$$

Pois se $z \notin D$, então $|z| > R$ e assim $|p(z)| \geq 1 + |a_0| > |p(0)|$. Como $0 \in D$, $|p(0)| \geq |p(z_0)|$. Assim,

$$|p(z_0)| \leq |p(z)|, \quad \forall z \in D \text{ ou } z \notin D.$$

Agora provaremos que $p(z_0) = 0$. Fazendo a mudança de variáveis $w = z - z_0$, então

$$p(z) = p(w + z_0) = q_1(w)$$

é um polinômio em w e

$$|q_1(0)| = |p(z_0)| \leq |p(z)| = |q_1(w)|, \quad \forall w.$$

Assim q_1 tem mínimo global em $w = 0$.

Provaremos que $q_1(0) = 0$. Se este for o caso, não há o que fazer. Se $q_1(0) = a \neq 0$, chegaremos a uma contradição. Suponha $a \neq 0$ e seja $q_2(w) = \frac{1}{a}q_1(w)$. Então, $|q_2(w)|$ tem um mínimo em $w = 0$ se e, somente se, $|q_1(w)|$ tem um mínimo em $w = 0$.

Agora $q_2(w)$ tem a forma

$$q_2(w) = 1 + bw^m + b_1w^{m+1} + \dots + b_kw^{m+k},$$

onde $m + k = n$.

Seja r a m -ésima raiz de $(-\frac{1}{b})$. Então, $br^m = -1$. Seja $w = ru$ e $q(u) = q_2(ru) = q_2(w)$. Então, $|q(u)|$ tem um mínimo e $u = 0$ se e, somente se, $|q_2(w)|$ tem um mínimo e, $w = 0$. Agora, $q(u)$ tem a forma

$$\begin{aligned} q(u) &= 1 + b(ru)^m + \dots + b_k(ru)^{m+k} \\ &= 1 - u^m + u^{m+1}Q(u), \end{aligned}$$

onde

$$Q(u) = c_1 + c_2u + \dots + c_ku^{k-1}$$

é um polinômio em u com $c_j = b_jr^{m+j}$, $1 \leq j \leq k$. Note que $q(0) = 1$, assim 1 é um valor mínimo de $|q(u)|$.

Seja $t > 0$ real. Fazendo $u = t$, temos

$$\begin{aligned} |Q(t)| &= |c_1 + c_2t + \dots + c_kt^{k-1}| \\ &\leq |c_1| + |c_2t + \dots + c_kt^{k-1}|. \end{aligned}$$

Seja

$$Q_0(t) = |c_1| + |c_2t + \dots + c_kt^{k-1}|.$$

Quando $t \rightarrow 0$, temos que $tQ_0(t) \rightarrow 0$. Escolha $0 < t < 1$ tal que $tQ_0(t) < 1$.

Vamos mostrar que esta escolha de t , fazendo $u = t$ dá $|q(t)| < 1 = |q(0)|$, contradizendo a hipótese que $|q(u)|$ tem seu mínimo em $u = 0$. De fato,

$$\begin{aligned} |q(t)| &= |1 - t^m + t^{m+1}Q(t)| \\ &\leq |1 - t^m| + |t^{m+1}Q(t)| \\ &= (1 - t^m) + t^m|Q(t)| \\ &= (1 - t^m) + t^m(tQ_0(t)). \end{aligned}$$

Como t é escolhido de modo que $tQ_0(t) < 1$, este último número é menor do que

$$(1 - t^m) + t^m = 1 = |q(0)|.$$

Como $t \neq 0$, $|q(u)|$ não tem seu mínimo em $u = 0$. Contradição. Logo, $a = 0$ o que implica que $q_1(0) = 0$ e portanto $p(z_0) = 0$. ■