Teorema Fundamental da Álgebra

Roberta Regina Delboni - RA: 027122
UNICAMP - IMECC

Disciplina: Elementos de Álgebra

Professor Fernando Torres

1 Introdução - História

Já por volta de 1600 a.C. 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 d.C.

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 $x^3 + px = q$, $x^3 + q = px$ e $x^3 = px + q$.A separação em casos foi necessário porque eles não conheciam números negativos. Scipio del Ferro resolveu os três casos que foi redescoberto em 1535 por Nicollo Fontana (Tartaglia). Em 1545 a "Ars Magna" de Cardamo continha uma completa discussão da solução de Fontana e o método de Ludovico Ferrari para resolver a equação de quarto grau por redução a uma cúbica.

Em 1608, Peter Rothe, escreveu no seu livro "Arithmetica Philosophica", que uma equação polinomial de grau n (com coficientes reais) pode ter n soluções. Albert Girard, no seu livro "L'invention nouvelle en l'Algèbre" (publicado em 1629), afirmou que uma equação polinomial de grau n tem n soluções, mas não disse que tais soluções eram necessariamente números complexos. Além disso, ele disse que a sua afirmação era válida (a menos que a equação seja incompleta), querendo dizer com isto que nenhum coeficiente é igual a 0. No entanto, quando ele explica em detalhe o que quer dizer, torna-se claro que, de fato, ele acredita que a afirmação dele é válida em todos os casos; por exemplo, ele mostra que a equação $x^4 = 4x - 3$, embora incompleta, tem quatro soluções: $1, 1, -1 + i\sqrt{2}$ e $-1 - i\sqrt{2}$.

Em 1637, Descartes escreve em "La géométrie" o que anos antes Harriot havia descoberto - se a é raiz de um polinômio, então $x-a$ divide o polinômio. Descartes afirmou também que para todas as equações de grau n, podemos imaginar n raízes, mas estas podem não corresponder a quantidades reais.

Uma conseqüência do teorema fundamental da Álgebra é que qualquer polinômio com coeficientes reais e grau superior a 0 pode ser escrito como produto de polinômios com coeficientes reais de graus 1 ou 2. No entanto,em 1702 Leibniz afirmou que nenhum polinômio do tipo x^4+a^4 (com a real e não nulo) pode ser obtido sob aquela forma. Anos mais tarde, Nikolaus Bernoulli afirmou o mesmo relativamente ao polinômio $x^4-4x^3+2x^2+4x+4$, mas recebeu uma carta de Euler em 1742 na qual lhe foi explicado que o seu polinômio era de fato igual a

$$(x^2-(2+\alpha)x+1+\sqrt{7}+\alpha)(x^2-(2-\alpha)x+1+\sqrt{7}-\alpha)$$

sendo α a raiz quadrada de $4+2\sqrt{7}$, enquanto que

$$x^4+a^4=(x^2+a\sqrt{2}x+a^2)(x^2-a\sqrt{2}x+a^2)$$

Uma primeira tentativa de demonstrar o teorema foi levada a cabo por d'Alembert em 1746, mas na altura a demonstração foi considerada incorreta. Entre outros problemas, usava implicitamente um teorema (atualmente designado por teorema de Puiseux) que só viria a ser demonstrado um século mais tarde e cuja demonstração se pensava depender do teorema fundamental da álgebra. No entanto, hoje em dia há quem defenda que a demonstração de D'Alembert foi mal compreendida, e que de fato não depende do teorema fundamental da álgebra ou seja, não é circular. Outras tentativas foram levadas a cabo por Euler (1749), de Foncenex (1759), Lagrange (1772) e Laplace (1795). Estas últimas quatro tentativas recorreram à tese de Argand; mais precisamente, a existência de raízes era dada como certa e o que faltava provar era que eram da forma $a+bi$ para números reais a e b. Em terminologia moderna, Euler, de Foncenex, Lagrange e Laplace estavam a supor a existência de um corpo de decomposição do polinômio $p(z)$.

No fim do século 18 foram publicadas duas novas demonstrações que não supunham a existência de raízes. Uma delas, da autoria de James Wood e sobretudo algébrica, foi publicada em 1798 e completamente ignorada. A demonstração de Wood tinha uma falha de natureza algébrica. A outra demonstração foi publicada por Gauss em 1799 e era sobretudo geométrica, mas tinha uma falha topológica.

Uma demonstração rigorosa foi publicada por Argand em 1806; foi aqui que, pela primeira vez, o teorema fundamental da Álgebra foi enunciado para polinômios com coeficientes complexos e não apenas para polinômios com coeficientes reais. Gauss publicou mais duas demonstrações em 1816 e uma nova versão da primeira demonstração em 1849.

O primeiro manual universitário a conter uma demonstração do teorema foi o Cours d'analyse de l'École Royale Polytechnique, de Cauchy (1821). A demonstração em questão é a de Argand, embora este não seja mencionado.

Nenhuma das demonstrações até agora mencionadas é construtiva. Foi Weierstrass quem levantou pela primeira vez, em 1891, o problema de encontrar uma demonstração construtiva do teorema. Tal demonstração foi obtida por Hellmuth Kneser em 1940 e simplificada pelo seu filho Martin Kneser em 1981.

2 Teorema Fundamental da Álgebra

Theorem 1 ***(Teorema Fundamental da Álgebra):*** *Todo polinômo $p(z)$ 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 será apresentada é basicamente a prova dada por Argand em 1814.

Observamos que um polinômio $p(z)$ com coeficientes complexos pode ser escrito na 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:

1. existe um ponto z_0 no plano complexo tal que

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

2. 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.

Lemma 2 *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 $|f(z)| \geq M$.*

Demontração: A prova é sobre indução sobre o grau de f. Se o grau de f é igual a 1, então $f(z) = a + b(z)$, $b \neq 0$. 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 $vert f(z) > M$.

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 $|z| > R$, $|f(z)| > M + |a|$, isto é possível pela hipótese de indução.

Então, para $|z| > R$,

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

provando assim o lema.

3 Prova do Teorema Fundamental

Para provar o teorema fundamental, seja

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

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

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

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

$$q_2(w) = 1 + bw^m + b_1 w^{m+1} + ... + b_k w^{m+k},$$

onde $m + k = n$.

Seja r a $m-$ésima rais de $\left(-\frac{1}{b}\right)$. 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

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

onde

$$Q(u) = c_1 + c_2 u + ... + c_k u^{k-1}$$

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

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

$$|Q(t)| = |c_1 + c_2 t + ... + c_k t^{k-1}| \leq |c_1| + |c_2 t + ... + c_k t^{k-1}|.$$

Seja

$$Q_0(t) = |c_1| + |c_2 t + ... + c_k t^{k-1}|$$

Quando $t \to 0$, temos que $tQ_0(t) \to 0$. 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 de que $|q(u)|$ tem seu mínimo em $u = 0$. De fato,

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

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 $p(z_0) = 0.\blacksquare$

References

[1] http://pt.wikipedia.org/wiki/Teorema_fundamental_da_%C3%A1lgebra

[2] http://www.dma.uem.br/ ~doherty/kit.html