Základná veta algebry. *Ľubovoľný komplexný polynóm kladného stupňa má aspoň jeden komplexný koreň.*

Dôkaz. Nech $p(z) = a_n z^n + a_{n-1} z^{n-1} + \cdots + a_1 z + a_0$ je polynóm s komplexnými koeficientami, $n \geq 1$ a $a_n \neq 0$. Vetu dokážeme v štyroch krokoch.

Krok 1: Začneme s dôkazom jednoduchej, ale dôležitej nerovnosti. Pretože pre $z \neq 0$ platí

$$|p(z)| = |a_n z^n + \cdots + a_0| = |z|^n \left| a_n + \frac{a_{n-1}}{z} + \frac{a_{n-2}}{z^2} + \cdots + \frac{a_1}{z^{n-1}} + \frac{a_0}{z^n} \right|,$$

pre $|z|$ dostatočne veľké, absolútna hodnota súčtu všetkých členov napravo od a_n môže byť urobená menšou ako povedzme $|a_n|/2$. Naozaj, pre $|z| > 1$ máme

$$\left| \frac{a_{n-1}}{z} + \frac{a_{n-2}}{z^2} + \cdots + \frac{a_1}{z^{n-1}} + \frac{a_0}{z^n} \right| \leq \frac{|a_{n-1}|}{|z|} + \frac{|a_{n-2}|}{|z|^2} + \cdots + \frac{|a_1|}{|z|^{n-1}} + \frac{|a_0|}{|z|^n} \leq$$
$$\leq \frac{M}{|z|} + \frac{M}{|z|^2} + \cdots + \frac{M}{|z|^{n-1}} + \frac{M}{|z|^n} \leq \sum_{i=1}^{\infty} \frac{M}{|z|^i} = \frac{M}{|z| - 1},$$

kde

$$M = \max(|a_{n-1}|, |a_{n-2}|, \ldots, |a_1|, |a_0|).$$

Stačí už len overiť, že platí

$$\frac{M}{|z| - 1} \leq \frac{|a_n|}{2} \quad \text{práve vtedy, keď} \quad |z| \geq 1 + \frac{2M}{|a_n|}.$$

Pre takéto z potom máme[1)]

$$\left| a_n + \frac{a_{n-1}}{z} + \frac{a_{n-2}}{z^2} + \cdots + \frac{a_1}{z^{n-1}} + \frac{a_0}{z^n} \right| \geq$$
$$\geq |a_n| - \left| \frac{a_{n-1}}{z} + \frac{a_{n-2}}{z^2} + \cdots + \frac{a_1}{z^{n-1}} + \frac{a_0}{z^n} \right| \geq |a_n| - \frac{|a_n|}{2} = \frac{|a_n|}{2}.$$

Teda

$$|p(z)| \geq \frac{|a_n|}{2} \cdot |z|^n, \text{ pre } |z| \text{ dostatočne veľké.} \tag{4.38}$$

Krok 2: Teraz ukážeme, že existuje číslo $c \in \mathbb{C}$ také, že $|p(c)| \leq |p(z)|$ pre všetky $z \in \mathbb{C}$. Dôkaz vyžaduje Bolzano-Weierstraßovu vetu. Definujme

$$m := \inf A, \text{ kde } A := \{|p(z)| : z \in \mathbb{C}\}.$$

Infimum určite existuje, pretože A je neprázdna a ohraničená zdola nulou. Pretože m je najväčšie dolné ohraničenie množiny A, pre každé $k \in \mathbb{N}$ číslo $m + 1/k$ už nie je dolným ohraničením množiny A, teda existuje číslo $z_k \in \mathbb{C}$ také, že

$$m \leq |p(z_k)| < m + 1/k.$$

1) Použili sme nerovnosť $|r + s| \geq |r| - |s|$.

Podľa (4.38) musí byť $\{z_k\}_{k=1}^{\infty}$ ohraničená postupnosť[2]. Podľa Bolzano-Weierstraß-ovej vety táto postupnosť musí mať konvergentnú podpostupnosť $\{w_k\}_{k=1}^{\infty}$. Ak c je limitou tejto podpostupnosti, zo spojitosti polynomickej funkcie vyplýva, že $|p(w_k)| \to |p(c)|$ a pretože $m \le |p(z_k)| < m + 1/k$ pre všetky $k \in \mathbb{N}$, podľa vety o troch limitách musí platiť $|p(c)| = m$.

Krok 3: Zvyšok dôkazu zahŕňa ukázanie, že minimum m musí byť nula, čo dáva výsledok $p(c) = 0$ a teda c je koreň polynómu $p(z)$. Aby sme to urobili, zavedieme pomocný polynóm $q(z)$ nasledujúcim spôsobom. Budeme predpokladať za účelom dosiahnutia sporu, že $p(c) \neq 0$. Definujme $q(z) := p(z+c)/p(c)$. Potom $|q(z)|$ má minimum v čísle $z = 0$, pričom toto minimum je rovné $|q(0)| = |1| = 1$. Pretože $q(0) = 1$, môžeme písať

$$q(z) = b_n z^n + \cdots + 1 = b_n z^n + \cdots + b_k z^k + 1,$$

kde k je najmenšie také prirodzené číslo, pre ktoré platí $b_k \neq 0$. V nasledujúcom kroku ukážeme, že 1 v skutočnosti nemôže byť minimom funkcie $|q(z)|$, čo bude spor.

Krok 4: Pretože každé komplexné číslo má k-tu odmocninu, existuje komplexné číslo a také, že platí $a^k = -1/b_k$. Potom platí

$$q(az) = 1 + b_k(az)^k + \cdots = 1 - z^k + \cdots ,$$

kde $\cdots$ reprezentujú členy vyššieho stupňa ako k. Potom môžeme písať

$$q(az) = 1 - z^k + z^{k+1} r(z),$$

kde $r(z)$ je polynóm. Nech $z = x$ je reálne číslo s vlastnosťou $0 < x < 1$, ktoré je také malé, že platí[3] $x|r(x)| < 1$. Potom pre toto reálne číslo x máme

$$|q(ax)| = |1 - x^k + x^{k+1} r(x)| \le |1 - x^k| + x^{k+1}|r(x)| < 1 - x^k + x^k \cdot 1 = 1 = |q(0)|,$$

t. j. $|q(ax)| < |q(0)|$. To však ukazuje, že $|q(z)|$ nenadobúda minimum v čísle $z = 0$, čo je v spore s tým, čo sme uviedli vyššie. Teda náš predpoklad $p(c) \neq 0$ musí byť nepravdivý a dôkaz je týmto ukončený.

Spracované podľa:

Paul Loya, Amazing and Aesthetic Aspects of Analysis: On the incredible infinite.

---

[2] $|z_k| \to \infty \Rightarrow |p(z_k)| \to \infty$

[3] Pretože reálna funkcia reálnej premennej $|r(x)|$ je spojitá, na uzavretom intervale je ohraničená. Teda existuje $K > 1$ také, že pre každé reálne číslo $x \in \langle 0, 1 \rangle$ platí $|r(x)| \le K$. Stačí vybrať ľubovoľné reálne číslo x také, že $0 < x < 1/K$. Potom $x|r(x)| \le xK < 1$.