Základní věta algebry

Tomáš Faikl
tomas.faikl@fjfi.cvut.cz

6. prosince 2022

Abstrakt

1 Úvod

Každý nekonstantní polynom má právě n komplexních kořenů, kde n je stupeň polynomu. Takovou větu student alespoň technického zaměření musel někdy za svoje studium slyšet. Pro kvadratické polynomy je tvrzení jasné, vždyť máme explicitní formulku. Podobně to je i pro řády tři a čtyři. Pro vyšší polynomy už je tvrzení ovšem více abstraktní, neboť dokonce žádné takové formulky vyjádřené pomocí odmocnin pro obecné polynomy ani existovat nemohou, jak dokázal roku 1813 Ital Paolo Ruffini a roku 1824 norský matematik N. H. Abel. Nyní existuje zhruba přes sto do různé míry odlišných důkazů a často platí, že při zrodu nové matematické oblasti se zrodí i nový důkaz Základní věty. Často se uvádí, že Základní věta algebry není ve skutečnosti věta základní, protože moderní algebrou můžete projít bez zaznamenání této větym a není to vlastně ani věta z algebry, ale spíše z analýzy.

Abychom se vyznali v historických pokusech o důkaz tohoto tvrzení, uveďme si neprve několik moderních algebraických definic.

Definice 1 (Algebraická uzavřenost)**.** Nechť T je těleso. Pokud každý nekonstantní polynom v $T[x]$ má kořen v T, řekneme, že T je algebraicky uzavřené.

Definice 2 (Algebraický uzávěr)**.** Nechť T je těleso. Řekneme, že K je algebraický uzávěr T, pokud $T \subset K$, K je algebraicky uzavřený a každé jiné algebraické uzavřené rozšíření T je obsaženo v K. Značíme $K = \overline{T}$.

A důležité tvrzení, které chybělo, či jeho obdoba, v několika historicky prvních důkazech, které byly jinak bezchybné. Často se uvažovalo, že kořeny polynomů existují „někde“ a následně se ukázalo, že alespoň jeden z nich je komplexní číslo.

Věta 3 (O existenci algebraického uzávěru)**.** *Každé těleso T má algebraický uzávěr $\overline{T}$. Algebraický uzávěr $\overline{T}$ je jednoznačný až na izomorfismus.*

Důkaz posledního tvrzení je veden pomocí Zornova lemmatu (popřípadě slabšího „ultrafilter“ lemma, které plyne z, ale není ekvivalentní, axiomu výběru).

Poznamenejme, že tvrzení, že každý nekonstantní komplexní polynom má alespoň jeden komplexní kořen je ekvivalentní, neboť potom můžeme původní polynom iterovaně redukovat faktorem $x - c$, kde c je kořen původního polynomu.

2 Historický vývoj

Peter Roth v roce 1608 uvádí, že rovnice n-tého řádu mají nanejvýš n řešení. Viete (1540–1603) byl schopný nalézt rovnice n-tého řádu, které z konstrukce mají n kořenů. Matematik Albert Girard později, motivován příklady, pronesl, že kořenů existuje právě n — avšak bez důkazu. Ovšem netvrdí, že všechny kořeny jsou tvaru $a+b\sqrt{-1}$, $a, b \in \mathbb{R}$. V jazyku moderní algebry navrhuje naśledující:

Věta 4 (Girardova domněnka)**.** *Pro každý polynom $f \in \mathbb{R}[x]$ stupně n existuje těleso $K \supset \mathbb{R}$, že f má právě n kořenů v K. Připouští, že $K \neq \mathbb{C}$.*

Descartes (1596–1650). V jeho knize *La géométrie* z roku 1637 dává stručné shrnutí o problematice polynomiálních rovnic. Zmiňuje dříve známou větu, že každý polynom s kořenem c je dělitelný faktorem $x - c$. K domněnce Girarda se staví neurčitě.

Leibniz (1646-1716). Při integraci racionálních funkcí je výhodné použít parciálních zlomků. Leibnize tak přirozeně napadla myšlenka, jestli každý reálný polynom lze rozložit na součin reálných faktorů prvního a druhého stupně. Jinými slovy, každý reálný polynom má kořen v $\mathbb{C}$ (plyne z toho, že reálné polynomy druhého stupně mají kořeny v $\mathbb{C}$). V roce 1702 uvedl názor, že tomu tak není: jako protipříklad uvedl polynom

$$x^4 + a^4 = (x^2 - a^2 i)(x^2 + a^2 i) = (x + a\sqrt{i})(x - a\sqrt{i})(x + a\sqrt{-i})(x - a\sqrt{-i}), \qquad (1)$$

zdá se tedy, že ho nenapadlo, že by výraz $\sqrt{i}$ mohl být vyjádřen jako komplexní číslo. Ve skutečnosti však platí $\sqrt{\pm i} = \frac{1}{2}(1 \pm i)$ a výrazy se zkombinují na dva reálné faktory druhého stupně.

Euler (1707–1783). V dopisu Nikolasi Bernoullimu z roku 1742 uvádí Euler tvrzení v přesně stejném tvaru jako dříve Leibniz (který si myslel, že tvrzení není pravdivé). Bernoulli navrhuje protipříklady, které se však ukážou neplatné. Později, roku 1743, v dopisu Goldbachovi, Euler znovu uvádí stejné tvrzení, ale dodává, že se mu nepodařilo ho plně dokázat — pouze „zhruba“, podobně jako u Fermata. Podařilo se mu dokázat následující pro stupně $n \leq 6$.

Věta 5 (Základní věta algebry pro reálné polynomy)**.** *Každý polynom n-tého stupně $f \in \mathbb{R}[x]$ má právě n kořenů v nadtělese $\mathbb{C}$.*

V roce 1749 se pokusil o důkaz v obecném případě. Myšlenka spočívala v rozložení monického polynomu stupně $2^n \geq 4$ na součin dvou monických polynomů $P_1 P_2$ stupně $m := 2^{n-1}$. Pokud by to bylo možné, opakováním prodcedury by obecný případ zredukoval na již dokázané. Za zmínku stojí, že v důkazu použil trik známý od dob Cardana a použil větu o střední hodnotě. Pro více informací vizte [5]. Ve skutečnosti však tento postup dopodrobna diskutoval pouze pro $m = 2$ a obecný případ nebyl uspokojivý (jak později kritizoval Gauss).

Lagrange (1736–1813), Laplace (1749–1827). Lagrange v roce 1772 kritizoval Eulerův důkaz. Zároveň se mu podařilo některé kritizované body opravit a postavit na rigorózní základ a tak z většiny opravil Eulerův důkaz. Ale stále předpokládál, že kořeny „někde“ existují, na základě čehož potom rozhodoval, do jakého tělesa patří. Jinými slovy, ve své době nevěděli o Větě 3.

V roce 1795 se Laplace pokusil o svůj nezávislý důkaz Základní věty. Ve svém důkazu používá pojem diskriminantu polynomu a stejně jako jeho předchůdci předpokládá, že kořeny polynomu existují. Vizte [5, str. 120] pro „extrémně elegantní důkaz“ (dle slov autora reference) založený na výsledku z teorie symetrických funkcí (dokázaném Newtonem roku 1673). Důkaz byl dlouhou dobu zapomenut.

Gauss (1777–1855). V roce 1799 publikoval Gauss ve své doktorské práci důkaz Základní věty, za kterou obdržel doktorát. Důkaz však nesplňuje novodobé požadavky na rigoróznost. Práce dvacetidvouletého studenta začíná rozsáhlou kritikou dosavadních výsledků zejména Eulera a Lagrange — hlavní výtkou je předpoklad existence kořene, která je třeba dokázat (může se stát, že kořeny neexistují). Ve své práci si nebyl vědom důkazu Lagrange. Později kritizoval jeho práci stejným způsobem jako předchozí.

Dokonce i Gauss si ve své disertaci myslel, že existuje netriviální hierarchie imaginárních veličina (tzv. *stíny stínů*). Koncem 18. století se však paradigma změnilo a byla formulována následující myšlenka, která si žádala důkaz: „Ukažte, že každá imaginární veličina má tvar $a + b\sqrt{-1}$“. V moderním jazyce, těleso $\mathbb{C}$ je algebraicky uzavřené.

Gauss podal celkem čtyři, či osm důkazů Základní věty, v závislosti na jemnosti dělení co už je a co není nový důkaz. První důkaz (z roku 1799) je topologický a myšlenka stojí na charakterizaci kořenů poolynomu f jako průsečíků dvou algebraických křivek $(\Re f)(z) = 0$ a $(\Im f)(z) = 0$, důkaz však není bez pochyb. Moderními metodami a propracovanými argumenty je možné jádro důkazu o algebraických křivkách opodstatnit, to ale Gauss neudělal.

Druhý důkaz (z roku 1816) je téměř čistě algebraický, založený na důkazu Eulera a využívá Sylowovy věty. Jediný analytický vstup do důkazu je „každý reálný polynom lichého stupně má reálný kořen“, který je důsledek věty o střední hodnotě. Druhý důkaz nenechává prostor ani pro moderní pochybovače. S polynomem zachází jako s prvkem $f \in \mathbb{C}[x]$, kde x je jednoduše neurčitý formální výraz, který nemá žádnou konkrétní hodnotu a dalo by se říci, že v důkazu konstruuje rozkladové nadtěleso reálných čísel, o kterém ukáže, že to jsou čísla komplexní.

Třetí důkaz ze stejného roku staví na identifikaci nul funkce pomocí komplexního křivkového integrálu. Komplexní polynom je holomorfní na $\mathbb{C}$ a tak nemá žádné póly.

Věta 6 (Princip argumentu)**.** *Nechť $f : \Omega \to \mathbb{C}$ je holomorfní funkce. Potom*

$$Z - P = \frac{1}{2\pi i} \oint_\gamma \frac{f'(z)}{f(z)} dz, \tag{2}$$

kde Z, resp. P, je počet nul, resp. pólů, funkce f uvnitř uzavřené měřitelné křivky.

Do roku 1849 byly všechny důkazy vedeny pro reálné polynomy. Toho roku Gauss poskytl první důkaz Základní věty pro komplexní polynomy. Z moderního pohledu se však nejedná o zásadní příspěvek, neboť Základní věta pro reálné a komplexní polynomy je ekvivalentní. Skutečně, nechť $f \in \mathbb{C}[z]$. Potom $g(z) := \overline{f(\overline{z})} f(z)$ je reálný polynom. Pokud $g(c) = 0$, potom c nebo $\overline{c}$ je kořen f. Tedy f má alespoň jeden komplexní kořen, což dokazuje Základní větu pro komplexní polynomy.

Argand (1768—1822), Cauchy (1798—1857). Argand v roce 1814 publikoval důkaz, který se považuje za jeden z nejjednodušších důkazů Základní věty. Využívá poznatek, že $|f(z)|$ nabývá svého minima v $\mathbb{C}$ (pozor, nejedná se o kompakt). Cauchy o pár let později publikoval téměř stejný důkaz, kde navíc zevrubně komentoval na výše uvedeném poznatku a důkaz byl tak obecně přístupnější a známější.

3 Moderní důkazy

Má se za to, že kompletně algebraický důkaz Základní věty nemůže existovat, neboť reálná, potažmo komplexní, čísla jsou samy konstruktem zúplnění racionálních čísel a tedy nutně analýzy. Pro zájemce o „minimalitu“ použití analýzy můžeme odkázat na [2].

Za asi nejvíce algebraický způsob důkazu můžeme nazvat techniku využívají pojmu „reálného uzavřeného tělesa“, což je těleso F, které je úplně uspořádané, každý kladný prvek má druhou odmocninu a každý polynom lichého stupně má alespoň jeden kořen v F. Dá se ukázat, že každé reálné uzavřené těleso není algebraicky uzavřené, ale nadtěleso $F(\sqrt{-1}) = \{a + b\sqrt{-1} \mid a, b \in F\}$ už algebraicky uzavřené je. Analýza vstupuje až v okamžiku, kdy ukážeme, že reálná čísla jsou reálné uzavřené těleso pomocí základní analýzy. Přístup pomocí Galoisovy teorie je stejně tak účinný.

3.1 Pomocí komplexní analýzy

Standardní krátký nelementární důkaz je např. pomocí komplexní analýzy a teorie holomorfních funkcí.

Věta 7 (Liouvilleova věta)**.** *Nechť $f : \mathbb{C} \to \mathbb{C}$ je holomorfní a omezená na $\mathbb{C}$. Potom f je konstantní.*

Důkaz Základní věty. Nechť f je komplexní nekonstantní polynom a pro spor uvažujme, že pro všechny $z \in \mathbb{C}$ je $f(z) \neq 0$. Potom funkce $g(z) := \frac{1}{f(z)}$ je holomorfní a omezená (ze spojitosti f) na $\mathbb{C}$. Z toho plyne, že g je konstantní a tedy i f je konstantní. □

3.2 Algebraická topologie

Další kategorie důkazů jsou důkazy topologické. Uveďme příklad z algebriacké topologie, konkrétně fundamentální grupy [4].

Definice 8. Nechť X, Y jsou topologické prostory a f, g spojitá zobrazení $X \to Y$. Řekneme, že f je *homotopická* g, pokud existuje spojité zobrazení $H : X \times [0,1] \to Y$ tak, že $H(x,0) = f(x)$ a $H(x,1) = g(x)$. Značíme $f \simeq g$. Třídou homotopie f označujeme všechny křivky homotopické f, značíme $[f]$.

Definice 9. Fundamentální grupou $\pi_1(X, x_0)$ topologického prostoru X v bodě $x_0 \in X$ rozumíme množinu tříd homotopie smyček v bodě x_0, tedy

$$\pi_1(X, x_0) := \{[f] \mid f : [0,1] \to X \text{ spojitá}, \ f(0) = f(1) = x_0\}. \tag{3}$$

Fundamentální grupy ve stejné komponentě souvislosti si jsou izomorfní.

Věta 10. *$\pi_1(\mathbb{S}^1)$ je nekonečná cyklická grupa generovaná třídou homotopie smyčky $\omega \in \Omega(\mathbb{S}^1, (1,0))$, kde $\omega(t) = (\cos(2\pi t), \sin(2\pi t))$, tj. $\pi_1(\mathbb{S}^1) = \{[e^{2\pi i n t}] \mid n \in \mathbb{N}\}$.*

Důkaz Základní věty. Uvažujme bez újmy polynom $f(z) = z^n + a_1 z^{n-1} + \cdots + a_n$. Pro spor uvažujme, že f nemá kořen v $\mathbb{C}$. Pro všechny $r \geq 0$ tak můžeme sestrojit spojitou smyčku $\gamma_r : [0,1] \to \mathbb{C}$,

$$\gamma_r(t) := \frac{f\left(r \exp\left(2\pi i t\right)\right) / f(r)}{\left|f\left(r \exp\left(2\pi i t\right)\right) / f(r)\right|}, \tag{4}$$

která leží na jednotkové kružnici $\mathbb{S}^1 \subset \mathbb{C}$ s počátkem $\gamma_r(0) = 1 = \gamma_r(1)$. Spojitou změnou parametru r můžeme přejít ke konstantní křivce $\gamma_0(t) \equiv 1$ a tedy pro všechna $r \geq 0$ je $\gamma_r \simeq e$, kde e značí konstantní křivku v bodě 1. Homotopičnost křivek plyne z existence (pro libovolné $r \geq 0$) homotopie $H : [0,1] \times [0,1] \to \mathbb{S}^1$, $H(t,1) = \gamma_r(t)$, $H(t,0) = \gamma_0(t) \equiv 1$.

Nyní sestrojíme křivku γ_r^s tak, že $\gamma_r \simeq \gamma_r^s \simeq \exp(2\pi i n t)$. Z toho už by nutně vyplývalo, že $n = 0$ a tedy f je konstantní polynom. Definujme křivku předpisem

$$\gamma_r^s(t) := \frac{f_s\left(r \exp\left(2\pi i t\right)\right) / f_s(r)}{\left|f_s\left(r \exp\left(2\pi i t\right)\right) / f_s(r)\right|}, \quad f_s(z) := z^n + s\left(a_1 z^{n-1} + \cdots + a_n\right) \tag{5}$$

Ukážeme, že vlastnost platí pro $r > \kappa := \max\{1, |a_1| + |a_2| + \cdots + |a_n|\}$. Pro $|z| = r > \kappa$ dostáváme $|z^n| = |z||z^{n-1}| > (|a_1| + |a_2| + \cdots + |a_n|)|z^{n-1}| \geq (|a_1 z^{n-1}| + |a_2 z^{n-2}| + \cdots + |a_n|) \geq |a_1 z^{n-1} + a_2 z^{n-2} + \cdots + a_n|$ s použitím popořadě $\kappa > 1$, Cauchy-Schwartz nerovnosti a trojúhelníkové nerovnosti. Z toho dostáváme, že polynom $f_s(z)$ nemá pro $|z| > \kappa$ a $s \in [0,1]$ žádný kořen (poukažme na ostrou nerovnost). Křivka γ_r^s je tak dobře definovaná pro $r > \kappa$. Potom z definice platí $\gamma_r^1 = \gamma_r$ a $\gamma_r^0 = \exp(2\pi i n t)$. Ze spojitosti křivky v s dostáváme $e \simeq \gamma_r \simeq \gamma_r^s \simeq \exp(2\pi i n t)$. □

4 Další reference

Pro další reference vizte [3] pro obdobné tvrzení pro kvaterniony, [6] pro konstruktivistický pohled na důkaz Věty a [1] pro jeden z nekratších důkazů.

Reference

[1] Martin Aigner and Günter M Ziegler. Proofs from the book. *Berlin. Germany*, 1, 1999.

[2] Piotr Błaszczyk. A purely algebraic proof of the fundamental theorem of algebra. *Annales Universitatis Paedagogicae Cracoviensis— Studia ad Didacticam Mathematicae Pertinentia*, 8:7–23, 2016.

[3] Samuel Eilenberg and Ivan Niven. The "fundamental theorem of algebra" for quaternions. *Bulletin of the American Mathematical Society*, 50(4):246–248, 1944.

[4] Allen Hatcher. *Algebraic Topology*. Cambridge University Press, 2002.

[5] R Remmert. *The fundamental theorem of algebra, Chapter 4 in: "Numbers" (H. D. Ebbinghaus et al., eds.)*, volume 123. Springer Science & Business Media, 1991.

[6] Fred Richman. The fundamental theorem of algebra: a constructive development without choice. *Pacific Journal of Mathematics*, 196(1):213–230, 2000.