LIETUVOS MATEMATIKOS RINKINYS
Lietuvos matematikų draugijos darbai, ser. B
63 tomas, 2022, 47–53
https://doi.org/10.15388/LMR.2022.29899

Pagrindinė algebros teorema

Juozas Juvencijus Mačys

Vilniaus universitetas, Duomenų mokslo ir skaitmeninių technologijų institutas
Akademijos 4, LT-08663 Vilnius
El. paštas: juozas.macys@mif.vu.lt

Įteiktas 2022 rugsėjo 14; publikuotas 2022 gruodžio 10

Santrauka. Straipsnyje mokytojai ir mokiniai supažindinami su pagrindine algebros teorema realiesiems polinomams ir jos įrodymu. Atskirai nagrinėjami mažųjų laipsnių polinomai. Aiškinama, kaip sprendžiamos trečiojo ir ketvirtojo laipsnio lygtys, pasiūlytas algoritmas kubinėms lygtims spręsti.

Raktiniai žodžiai: realieji polinomai; pagrindinė algebros teorema; polinomų skaidymas; kartotinio argumento sinusas ir kosinusas; kubinės lygtys; ketvirtojo laipsnio lygtys

Šio straipsnio tikslas – supažindinti mokytojus ir mokinius su pagrindine algebros teorema (PAT). Ji buvo suformuluota dar XVII amžiuje, bet griežtai įrodyta tik XX amžiaus pradžioje. Realiųjų skaičių srityje PAT skamba taip:

Teorema (PAT). *Kiekvieną n-tosios eilės polinomą su realiaisiais koeficientais*

$$f(x) = c_n x^n + c_{n-1}x^{n-1} + \cdots + c_2x^2 + c_1x + c_0 \quad (c_n \neq 0) \tag{1}$$

galima išskaidyti tiesiniais ir kvadratiniais realiaisiais polinomais.

Kadangi polinomo išskaidomumui neturi įtakos jo dalijimas iš $c_0 \neq 0$, tai galima laikyti, kad $c_n = 1$. Taip pat galima laikyti, kad $f(x) > 0$ visiems x – kitaip jis turės šaknį α, ir polinomą galima padalyti iš $x - \alpha$. Kadangi dabar $c_0 = f(0) > 0$, tai c_0 galima laikyti teigiamu. Tada galime atlikti keitimą $x = y\sqrt{c_0}$, ir padaliję iš c_0 gausime teigiamąjį polinomą

$$f(x) = x^n + c_{n-1}x^{n-1} + \cdots + c_2x^2 + c_1x + 1, \tag{2}$$

kurį dažniausiai neperspėdami ir turėsime galvoje. Beje, n čia galima laikyti lyginiu – nelyginio laipsnio polinomas įgyja tiek teigiamų, tiek neigiamų reikšmių.

PAT įrodymas. Užtenka įrodyti, kad (2) polinomas dalijasi iš kvadratinio trinario. Tada padalįję gausime $n-2$ laipsnio polinomą. Jis vėl dalysis iš tam tikro kvadratinio trinario. Kartodami šią procedūrą, (2) polinomą išskaidysime kvadratiniais trinariais.

Kadangi polinomas neturi šaknų, tai ir trinaris jų negali turėti, taigi tas trinaris teigiamas. Kiekvieną teigiamąjį trinarį galima užrašyti kaip

$$(x - r\cos\varphi)^2 + r^2\sin^2\varphi, \quad \varphi \neq k\pi. \tag{3}$$

Polinomas (2) dalijasi iš (3) trinario, jei polinomas

$$\begin{aligned} f(x + r\cos\varphi) &= \sum_{k=0}^{n} c_k (x + r\cos\varphi)^k \\ &= \sum_{k=0}^{n} c_k \left(r^k \cos^k\varphi + x\binom{k}{1} r^{k-1}\cos^{k-1}\varphi + x^2\binom{k}{2} r^{k-2}\cos^{k-2}\varphi + \cdots \right) \end{aligned} \tag{4}$$

dalijasi iš dvinario $x^2 + r^2\sin^2\varphi$, o tam užtenka, kad iš jo dalytųsi lyginė ir nelyginė (4) polinomo dalys. Lyginė (4) polinomo dalis

$$\sum_{k=0}^{n} c_k \left(r^k \cos^k\varphi + x^2\binom{k}{2} r^{k-2}\cos^{k-2}\varphi + x^4\binom{k}{4} r^{k-4}\cos^{k-4}\varphi + \cdots \right)$$

dalysis iš to dvinario, jeigu x^2 pakeitę į $-r^2\sin^2\varphi$ gausime nulį:

$$\sum_{k=0}^{n} c_k \left(r^k \cos^k\varphi - r^2\sin^2\varphi\binom{k}{2} r^{k-2}\cos^{k-2}\varphi + r^4\sin^4\varphi\binom{k}{4} r^{k-4}\cos^{k-4}\varphi - \cdots \right) = 0.$$

Panašiai (4) polinomo nelyginė dalis

$$x\sum_{k=0}^{n} c_k \left(\binom{k}{1} r^{k-1}\cos^{k-1}\varphi + x^2\binom{k}{3} r^{k-3}\cos^{k-3}\varphi + x^4\binom{k}{5} r^{k-5}\cos^{k-5}\varphi + \cdots \right)$$

dalysis iš to dvinario, jei x^2 po sumos ženklu pakeitę į $-r^2\sin^2\varphi$ gausime nulį:

$$\begin{aligned} \sum c_k \biggl(\binom{k}{1} r^{k-1}\cos^{k-1}\varphi &- r^2\sin^2\varphi\binom{k}{3} r^{k-3}\cos^{k-3}\varphi \\ &+ r^4\sin^4\varphi\binom{k}{5} r^{k-5}\cos^{k-5}\varphi - \cdots \biggr) = 0. \end{aligned}$$

Taigi (2) polinomas dalijasi iš (3) trinario, jeigu

$$\sum_{k=0}^{n} c_k r^k \left(\cos^k\varphi - \binom{k}{2}\sin^2\varphi\cos^{k-2}\varphi + \binom{k}{4}\sin^4\varphi\cos^{k-4}\varphi - \cdots \right) = 0, \tag{5}$$

$$\sum_{k=0}^{n} c_k r^{k-1} \left(\binom{k}{1}\cos^{k-1}\varphi - \binom{k}{3}\sin^2\varphi\cos^{k-3}\varphi + \binom{k}{5}\sin^4\varphi\cos^{k-5}\varphi - \cdots \right) = 0. \tag{6}$$

Dabar (5) formulės skliaustuose atpažįstame kartotinio argumento kosinusą:

$$\cos k\varphi = \cos^k \varphi - \binom{k}{2} \sin^2 \varphi \cos^{k-2} \varphi + \binom{k}{4} \sin^4 \varphi \cos^{k-4} \varphi - \cdots .$$

Padauginę (6) sąlygą iš $r \sin \varphi \neq 0$, gauname ekvivalenčią

$$\sum_{k=0}^{n} c_k r^k \left(\binom{k}{1} \sin \varphi \cos^{k-1} \varphi - \binom{k}{3} \sin^3 \varphi \cos^{k-3} \varphi + \binom{k}{5} \sin^5 \varphi \cos^{k-5} \varphi - \cdots \right),$$

ir skliaustuose atpažįstame kartotinio argumento sinusą:

$$\sin k\varphi = \binom{k}{1} \sin \varphi \cos^{k-1} \varphi - \binom{k}{3} \sin^3 \varphi \cos^{k-3} \varphi + \binom{k}{5} \sin^5 \varphi \cos^{k-5} \varphi - \cdots .$$

(Kartotinio argumento formules nesunku įrodyti standartiniu matematinės indukcijos metodu.) Tai reiškia, kad (2) polinomas dalijasi iš (3) kvadratinio trinario, jei tik išpildytos sąlygos:

$$U(r, \varphi) \doteq r^n \cos n\varphi + c_{n-1} r^{n-1} \cos(n-1)\varphi + \cdots + c_2 r^2 \cos 2\varphi + c_1 r \cos \varphi + 1 = 0, \tag{7}$$

$$V(r, \varphi) \doteq r^n \sin n\varphi + c_{n-1} r^{n-1} \sin(n-1)\varphi + \cdots + c_2 r^2 \sin 2\varphi + c_1 r \sin \varphi = 0. \tag{8}$$

Vadinasi, PAT bus įrodyta, kai parodysime, kad visada egzistuoja $r \in (0, \infty)$ ir $\varphi \in [0, 2\pi]$, tenkinantys (7) ir (8) sąlygas. Būtent tai yra įrodymo sunkioji dalis.

Tarkime priešingai, kad visada

$$U^2(r, \varphi) + V^2(r, \varphi) \neq 0.$$

Įsitikinkime, kad ši prielaida veda prie prieštaros, ir PAT bus įrodyta. Nagrinėkime funkcijas

$$X(r, \varphi) = U(r, \varphi) / \sqrt{U^2(r, \varphi) + V^2(r, \varphi)}, \qquad Y(r, \varphi) = V(r, \varphi) / \sqrt{U^2(r, \varphi) + V^2(r, \varphi)}.$$

Vaizduokime taškus (X, Y) Dekarto koordinačių sistemoje xOy. Kadangi

$$X^2(r, \varphi) + Y^2(r, \varphi) = 1,$$

tai visi taškai (X, Y) yra vienetinio apskritimo $x^2 + y^2 = 1$ taškai.

Kai r pastovus, o φ kinta nuo 0 iki 2π, tai taškas (X, Y) tolydžiai juda vienetiniu apskritimu. Intervalą $[0, 2\pi]$ galima taip padalyti į baigtinį skaičių pointervalių, kad kiekviename iš jų taškas (X, Y) judės prieš laikrodžio rodyklę (l.r.), arba pagal l.r. (žr. 1 pastabą toliau). Kai taškas pointervalyje juda prieš l.r., jo nueitą kelią (lygų atitinkamam vienetinio apskritimo lankui) laikykime teigiamu ir imkime su ženklu $+$. Kai taškas juda pagal l.r., jo nueitą kelią imkime su ženklu $-$.

Sudėję visus kelius, gauname suminį kelią $S(r)$. Kadangi taško kelias tolydus, prasideda ir baigiasi taške $(1, 0)$ (nes $U(r, 0) = 1$, $V(r, 0) = 0$, $\sqrt{U^2(r, 0) + V^2(r, 0)} = 1$, o dėl sin ir cos periodiškumo $X(r,0)=X(r,2\pi)=1$, $Y(r,0)=Y(r,2\pi)=0$), tai suminis kelias gali įgyti tik reikšmes iš aibės $\{2\pi k \mid k\in \boldsymbol{Z}\}$, t.y. teigiamus ir neigiamus apskritimo ilgio kartotinius (žr. 2 pastabą).

Kintant r nuo 0 iki $+\infty$, suminis kelias $S(r)$ kinta tolygiai (žr. 3 pastabą).

Kai $r=0$, tai $U\equiv 1$, $V\equiv 0$, ir kintant φ taškas (X,Y) nejuda, $S(0)=0$.

Kai $r\to 0$, tai $U\to 1$, $V\to 0$, todėl pakankamai mažiems r taškas (X,Y) grįžta į pradinę padėtį $(1,0)$, nepasiekęs, pvz., taško $(-1,0)$ ir neapėjęs viso apskritimo, taigi pakankamai mažiems r bus $S(r)=0$.

Kai $r\to\infty$, tai kiekvienam φ

$$\begin{aligned}
\lim X(r,\varphi) &= \lim\bigl(U(r,\varphi)/\sqrt{U^2(r,\varphi)+V^2(r,\varphi)}\bigr)\\
&= \lim\bigl(r^n\cos n\varphi/\sqrt{(r^n\cos n\varphi)^2+(r^n\sin n\varphi)^2}\,\bigr)\\
&= \lim\bigl(r^n\cos n\varphi/\sqrt{r^{2n}}\,\bigr)=\cos n\varphi,\\
\lim Y(r,\varphi) &= \lim\bigl(r^n\sin n\varphi/\sqrt{r^{2n}}\,\bigr)=\sin n\varphi.
\end{aligned}$$

Tai reiškia, kad pakankamai dideliems r taškas (X,Y) visą laiką lydi tašką $(\cos n\varphi$, $\sin n\varphi)$, ir jo kelias $S(r)$ kiek norint artimas to taško keliui $2n\pi$, vadinasi, lygus $2n\pi$.

Kadangi suminis kelias $S(r)$ tolydus, tai jis įgyja tik vieną reikšmę iš $\{2\pi k\}$. Bet jau įsitikinome, kad jis gali įgyti ir reikšmę 0, ir reikšmę $2\pi n$ (n – nagrinėjamojo polinomo laipsnis). Prieštara. Vadinasi, prielaida

$$U^2(r,\varphi)+V^2(r,\varphi)\neq 0$$

neteisinga, taigi egzistuoja r ir φ reikšmių pora, su kuria $U(r,\varphi)=0$ ir $V(r,\varphi)=0$. PAT įrodyta. $\square$

1 pastaba. Paaiškinsime, kodėl taškas (X,Y) judėdamas gali keisti kryptį tik baigtiniame (aprėžtame) taškų skaičiuje. Kiekviename ketvirtyje jis keičia kryptį kartu su Y ženklu. Bet Y yra trigonometrinis polinomas, $\cos k\varphi$ galima pakeisti $\cos\varphi$ polinomu, ir turėsime n-tojo laipsnio $\cos\varphi$ polinomą, kuris turi ne daugiau kaip n šaknų, o $\cos\varphi$ virsta nuliu tik dviejuose intervalo $[0,2\pi]$ taškuose. Taigi tokių krypties keitimo taškų skaičius aprėžtas.

2 pastaba. Kodėl suminis kelias lygus kuriai nors reikšmei iš aibės $\{2k\pi \mid k\in\boldsymbol{Z}\}$? Sudalykime φ kitimo intervalą $[0,2\pi]$ į minėtus monotoniškumo intervalus. Kol taškas juda ta pačia kryptimi, kelias aiškus. Kai taškas keičia judėjimo kryptį, monotoniškumo intervale vienos krypties kelią naikina atvirkščias kelias. Po to judėjimas tęsiasi, ir lieka tik vienos krypties keliai. Kadangi tas kelias tolydus, prasideda ir baigiasi taške $(1,0)$, tai jį sudaro 0, 1 ar keli apskritimai, ir jis lygus $2\pi k$, $k\in\boldsymbol{Z}$.

3 pastaba. Kad kelias $S(r)$ tolydžiai kinta r kintant nuo 0 iki $+\infty$, suvokti padeda fizikiniai sumetimai. Beje, apsirikti tolydumo samprotavimuose labai nesunku, ir tai pailiustruosime tokiu pavyzdžiu.

Kai $r>0$ fiksuotas, kreivė $(U(r,\varphi),V(r,\varphi))$, $\varphi\in[0,2\pi]$, tolydi ir uždara, nes sinusas ir kosinusas periodiški.

Kai r pakankamai didelis, tai U^2+V^2 aukščiausiosios eilės narys yra $r^{2n}\cos^2 n\varphi+r^{2n}\sin^2 n\varphi=r^{2n}$, todėl U^2+V^2 kiekvienam φ didesnis už 1. Vadinasi, tada kreivė (U,V) apgaubia vienetinį apskritimą, taigi taškas $(0,0)$ yra kreivės viduje. Kadangi

(7) laisvasis narys lygus 1, tai r pakankamai mažiems $U > \frac{1}{2}$, visa kreivė (U, V) yra į dešinę nuo ašies Oy, taigi taškas $(0, 0)$ yra kreivės išorėje. Todėl r mažėjant nuo begalybės iki nulio taškas $(0, 0)$ iš vidinio kreivės taško virsta išoriniu, ir tam tikru momentu atsiduria kreivėje.

Deja, šis samprotavimas nėra korektiškas. Iš tikrųjų, imkime kreivę, panašią į „tuščiąją" raidę $\mathbb{C}$, jos ertmėje patalpinkime tašką $(0, 0)$ ir glauskime jos galus, kol kreivė pasidarys panaši į „pustuštę" $\mathbb{O}$. Taškas $(0, 0)$ buvo kreivės išorėje, tapo vidiniu, bet pačioje kreivėje jis taip ir neatsidūrė.

Panašios klaidos neišvengta ir knygoje [1], nors šiaip šis sustiprintos matematikos vadovėlis parašytas puikiai ir apima daugybę įdomių temų, tinkamų fakultatyvams mokykloje.

Neapseinama be tolydumo ir kituose PAT įrodymuose. Todėl ypač netikėta, kad A. Novikas rado originalų būdą, padedantį įrodyme išvengti tolydumo argumentų. Pasirodo, griežtai įrodyti PAT galima nagrinėjant diskrečiuosius dydžius. Įrodymas bus pateiktas rengiamame spaudai straipsnyje.

PAT žemesniųjų laipsnių polinomams. Kaip matėme, bendruoju atveju PAT įrodymas techniškai sunkus. Aptarsime, kaip teorema įrodoma mažiesiems n.

Šeštojo ir aukštesnių laipsnių atveju PAT įrodymas nė kiek ne lengvesnis nei bendruoju atveju.

Penktojo laipsnio polinomas visada turi šaknį α (tik ne visada mokame ją rasti), todėl dalydami jį iš $x - \alpha$ gautume ketvirtojo laipsnio polinomą. Taigi viskas priklauso nuo PAT ketvirtajam laipsniui.

Ketvirtojo laipsnio polinomą visada galima išskaidyti į dviejų kvadratinių polinomų sandaugą – tam užtenka mokėti rasti bent vieną kubinio polinomo šaknį. Kubinį polinomą išskaidyti tikrai galima, nes jis visada turi šaknį. Vadinasi, trečiojo, ketvirtojo ir penktojo laipsnio polinomams PAT įrodyti nesunku.

Žinoma, PAT įrodo tik tiek, kad minėtus polinomus išskaidyti galima. Bet visai kitas klausimas, kaip tai padaryti. Yra įrodyta, kad konkrečiai išskaidyti penktojo ir aukštesnių laipsnių polinomus, apskritai šnekant, neįmanoma – tam nėra ir būti negali gatavų formulių. O štai trečiojo ir ketvirtojo laipsnio polinomus išskaidyti įmanoma, ir net mokykliškai.

Ketvirtojo laipsnio polinomą išskaidyti į du kvadratinius paprasta neapibrėžtųjų koeficientų metodu – tiesa, tam kartais prireiks rasti pagalbinės kubinės lygties sprendinį.

Kaip visa tai atliekama, smulkiai išdėstyta straipsnyje [2]. Čia tiktai pateiksime *algoritmą*, kuriuo galima rasti kubinio polinomo šaknis (žinoma, tam užtenka rasti bent vieną realiąją šaknį).

1 žingsnis. Jeigu kubinės lygties ($a \neq 0$!)

$$ax^3 + bx^2 + cx + d = 0 \tag{9}$$

koficientai racionalūs, tai nesunku rasti jos racionaliuosius sprendinius (jei tokių yra). Lygtį dauginame iš koeficientų vardiklių bendrojo mažiausiojo kartotinio. Dabar (9) lygties koeficientai sveiki. Dauginame lygtį iš a^2, ir keičiame $ax = y$.

Suprastinę gauname pavidalo

$$x^3 + ax^2 + bx + c = 0 \tag{10}$$

lygtį su sveikaisiais koeficientais. Jos racionalieji sprendiniai būtinai sveiki, juos randame patikrinę visus (teigiamus ir neigiamus) c daliklius. Jeigu radome bent vieną (10) lygties sprendinį α, ją išskaidome ir randame visus jos sprendinius, po to ir lygties (9) sprendinius.

2 žingsnis. Jeigu racionaliųjų sprendinių nėra, tai dalijame (9) lygtį iš a, ir gauname (10) pavidalo lygtį.

3 žingsnis. Atliekame keitinį $y = x - \frac{a}{3}$, – išnyksta nežinomojo kvadratas, ir gauname lygtį

$$x^3 + px + q = 0. \tag{11}$$

4 žingsnis. Keičiame kintamuosius, $x = y\sqrt[3]{\frac{2}{q}}$, gauname pavidalo

$$y^3 + ky + 2 = 0 \tag{12}$$

lygtį.

5′ žingsnis. Jei $k \geqslant -3$, tai atliekame keitimą $y = t - \frac{k}{3t}$:

$$\left(t - \frac{k}{3t}\right)^3 + k\left(t - \frac{k}{3t}\right) + 2 = 0,$$
$$t^3 - tk + \frac{k^2}{3t} - \frac{k^3}{27t^3} + kt - \frac{k^2}{3t} + 2 = 0,$$
$$t^3 - \frac{k^3}{27t^3} + 2 = 0,$$
$$t^6 + 2t^3 = \frac{k^3}{27},$$
$$\left(t^3 + 1\right)^2 = \frac{k^3}{27} + 1.$$

Iš čia randame t, o tada y. Lygtis (12) išspręsta.

5″ žingsnis. Jei $k < -3$, tai (12) lygtyje atliekame keitimą $y = \sqrt{-\frac{4k}{3}}\cos\varphi$:

$$\left(\sqrt{-\frac{4k}{3}}\right)^3 \cos^3\varphi + k\cos\varphi\sqrt{-\frac{4k}{3}} + 2 = 0,$$
$$4\cos^3\varphi - 3\cos\varphi = -\sqrt{-\frac{27}{k^3}}.$$

Bet $\cos 3\varphi = \cos(2\varphi + \varphi) = \cos 2\varphi\cos\varphi - \sin 2\varphi\sin\varphi = (2\cos^2\varphi - 1)\cos\varphi - 2\sin^2\varphi\cos\varphi = 2\cos^3\varphi - \cos\varphi - 2(1 - \cos^2\varphi)\cos\varphi = 4\cos^3\varphi - 3\cos\varphi$, todėl

$$\cos 3\varphi = -\sqrt{-\frac{27}{k^3}}.$$

Iš čia randame φ, o tada visas tris skirtingas $\cos\varphi$ (taigi ir y) reikšmes. Lygtis (12) išspręsta.

Literatūra

[1] S.B. Gaškov. *Sovremennaja elementarnaja algebra v zadačach i upražnenijach.* MCNMO, Moskva, 2006.

[2] J.J. Mačys. Elementary theory of cubics and quartics. *Liet. matem. rink. Proc. LMS, Ser A*, **58**:16–22, 2017.

SUMMARY

Fundamental theorem of algebra

J.J. Mačys

The purpose of the article is to familiarize teachers and students with the fundamental theorem of algebra for real polynomials and its proof. Polynomials of small degrees are considered separately. It is showed how equations of the third and fourth degree can be solved. An algorithm for solving cubic equations is proposed.

Keywords: real polynomials; fundamental theorem of algebra; decomposition of polynomials; sine and cosine of multiple argument; cubic equations; equations of the fourth degree