Abel-Ruffinijev izrek

Avtorja: Jernej Grlj, Jasmina Pegan
Mentor: Rok Gregorič

1 Predstavitev

Dokazali smo Abel-Ruffinijev izrek, ki pravi, da niso vsi polinomi pete ali višje stopnje rešljivi v radikalih. Z drugimi besedami, ni mogoče najti formule za iskanje rešitev polinomov pete ali višje stopnje le z njihovimi koeficienti prek uporabe seštevanja, množenja, deljenja, potenciranja in korenjenja, kakršna je npr. znana formula

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

za kvadratno enačbo $ax^2 + bx + c = 0$. Izrek o nerešljivosti je formuliral Paolo Ruffini, Niels Henrik Abel pa je prvi podal popoln dokaz. Naš dokaz temelji na dokazu ruskega matematika Vladimirja Arnolda. Standardni sodobni pristop k Abel-Ruffinijevem izreku sicer temelji na Galoisovi teoriji.

2 Osnove

2.1 Permutacije

Definicija 1. *Permutacija* π je bijekcija množice $\{1, 2, \dots, n\}$ same nase. Množico vseh permutacij, ki jo označimo S_n, imenujemo simetrična grupa. *Produkt permutacij* π *in* σ je permutacija $\pi\sigma$, ki je definirana kot kompozitum $\sigma \circ \pi$.

Primer 1. *Transpozicija* (ab) za različni naravni števili a in b med 1 in n preslika a v b, b v a ter vse ostale elemente same vase. To je permutacija množice z n elementi.

Znano je, da je mogoče vsako permutacijo zapisati kot produkt transpozicij, vendar v splošnem ta zapis ni enoličen. Izkaže pa se, da je enolična parnost števila transpozicij, ki jih pri tem potrebujemo.

Definicija 2. *Soda permutacija* je produkt sodega števila transpozicij, množico vseh sodih permutacij v $\{1, 2, ..., n\}$ označimo z A_n. Imenujemo jo tudi *alternirajoča grupa.*

Glede na to, da je vsaka permutacija π, bijekcija, ima inverz, ki ga bomo označimo s π^{-1}.

Definicija 3. *Komutator* dveh permutacij π in σ je permutacija $\pi\sigma\pi^{-1}\sigma^{-1}$, ki jo označimo z $[\pi, \sigma]$.

Definicija 4. *Tri-cikel* (abc) slika po pravilu

$$\begin{aligned} a &\mapsto b, \\ b &\mapsto c, \\ c &\mapsto a, \end{aligned}$$

ostale elemente pa slika same vase.

Opazimo, da velja $(abc) = (ab)(ac)$. Na podoben način kot transpozicije in tricikle lahko definiramo poljubne n-cikle $(a_1 \dots a_n)$. Zanje podobno velja

$$(a_1a_2a_3 \dots a_n) = (a_1a_2)(a_1a_3)\cdots(a_1a_n),$$

torej je n-cikel soda permutacija natanko tedaj, ko je n liho število.

Trditev 1. Vsaka soda permutacija je produkt tri-ciklov.

Dokaz. Dovolj je pokazati, da lahko tako zapišemo produkte dveh transpozicij. Opazimo, da obstajata dve vrsti produktov transpozicij, ki nista trivialna (ne slikata vseh elementov samih vase). Te lahko zapišemo v obliki

$$(ab)(ac) = (abc),$$

$$(ab)(cd) = ((ab)(bc))((bc)(cd)) = (bac)(cbd),$$

kjer so a, b, c in d poljubna med seboj različna števila. $\square$

Trditev 2. Vsak element A_n za $n \geq 5$ je mogoče zapisati kot produkt komutatorjev elementov A_n.

Dokaz. Zadostno je, če pokažemo, da lahko s komutatorji ciklov lihe dolžine pridobimo vsak tri-cikel. To lahko storimo kot

$$[(abcde), (abc)] = (abcde)(abc)(edcba)(cba) = (bec).$$

Elemente b, e in c izberemo poljubno in lahko naredimo poljuben tri-cikel. $\square$

2.2 Koreni enote in večkratne ničle

Definicija 5. Koreni enote so kompleksna števila, ki zadoščajo enačbi $x^k = 1$. Za $\omega_k = e^{2\pi i \frac{2\pi}{k}}$, kjer je $e^{ix} = \cos x + i \sin x$, so koreni enote natanko potence ω_k, ω_k^2, $\ldots$ ω_k^{k-1}, $\omega_k^k = 1$.

Trditev 3. Imejmo enačbo $x^k = \alpha$. Za $\alpha \neq 0$ ima ta enačba k rešitev. Iz poljubne rešitve x_0 dobimo ostale rešitve s tem, da množimo x_0 s k-timi koreni enote.

Dokaz. Denimo, da je x_0 ena rešitev (brez dokaza privzemimo, da obstaja). Za vsak koren enote ω_k^n velja

$$(\omega_k^n x_0)^k = \omega_k^{n+k} x_0^k = \alpha,$$

torej je tudi $\omega_k^n x_0$ rešitev za vsak $n \in \{1, 2, \ldots, n\}$. Enačba $x^k = \alpha$ je polinomska stopnje k, zato ima največ k rešitev. Našli smo jih prav toliko. $\square$

Trditev 4. Polinom p s kompleksnimi koeficienti ima večkratno ničlo v točki x_0 natanko tedaj, ko je x_0 ničla polinoma p in njegovega odvoda p'.

Tega tu ne bomo dokazovali.

3 Dokaz

V tem članku se bomo ukvarjali s polinomi stopnje pet ali več. Predsem bomo obravnavali družino polinomov

$$p_a(x) = x^n - x + a,$$

kjer na komplekso število a gleamo kot na parameter.

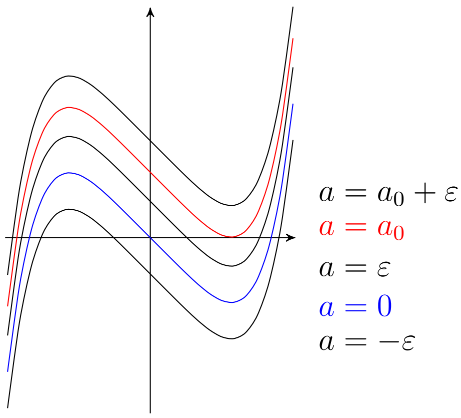
Trditev 5. Polinom $p_a(x)$ ima večkratno ničlo v točki b natanko tedaj, ko a zadošča enačbi $a^{n-1} = \frac{(n-1)^{n-1}}{n^n}$ in b zadošča enačbi $b^{n-1} = \frac{1}{n}$.

Dokaz. Trditev bomo dokazali s pomočjo trditve 4. Iz nje sledi, da večkratna ničla b reši enačbo $p_a'(b) = nb^{n-1} - 1 = 0$. Ker je b tudi ničla polinoma p_a, je $a = b - b^n = b(1 - b^{n-1})$ in iz prejšnje zveze dobimo $a^{n-1} = b^{n-1}(1 - b^{n-1})^{n-1} = \frac{1}{n}\left(1 - \frac{1}{n}\right)^{n-1} = \frac{(n-1)^{n-1}}{n^n}$. $\square$

3.1 Nevarne točke in zanke

Definicija 6. *Nevarne točke* so tiste točke $a \in \mathbb{C}$, v katerih ima polinom $p_a(x)$ večkratne ničle. Množico nevarnih točk označimo z D.

Elementi množice D so po trdtitvi 5 takšna kompleksna števila a, ki rešijo enačbo $a^{n-1} = \frac{(n-1)^{n-1}}{n^n}$. Posebej lahko uporabimo trditev 3, da to prepoznamo kot produkti realnega števila $a_0 = \sqrt[n-1]{\frac{(n-1)^{n-1}}{n^n}} = (n-1)n^{-\frac{n}{n-1}}$ z $(n-1)$-timi koreni enote, pripadajoče večkratne ničle pa kot produkte števila $b_0 = \frac{1}{\sqrt[n-1]{n}} = n^{-\frac{1}{n-1}}$



Slika 1: Grafi polinomov $p_a(x)$ za $-\varepsilon \leq x \leq a_0 + \varepsilon$. Z modro je obarvan $p_0(x)$, z rdečo pa $p_{a_0}(x)$.

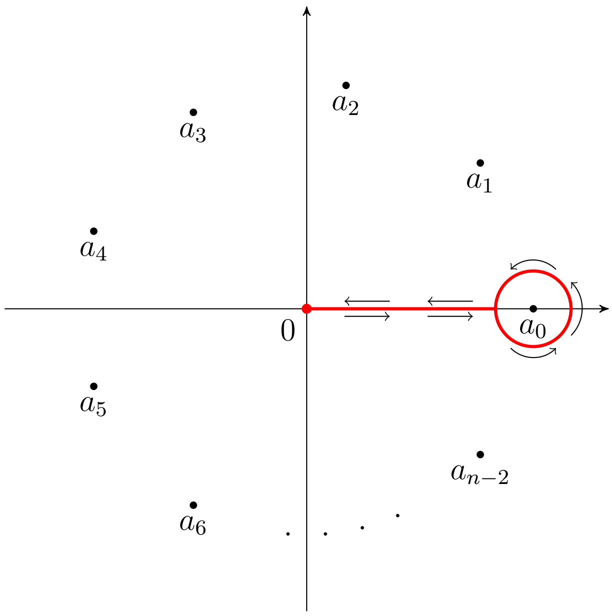
Definicija 7. Zanke so krivulje, ki se začnejo in končajo v isti točki. Množico vseh zank, ki ležijo v podprostoru $U \subseteq \mathbb{C}$ in potekajo skozi točko $x \in U$, označimo $\Omega_x(U)$.

Definicija 8. *Produkt zank* ℓ_1 in ℓ_2 je nova zanka, ki jo dobimo tako, da najprej prepotujemo ℓ_1 in nato ℓ_2. Produkt zank označimo z $\ell_1\ell_2$.

Definicija 9. *Inverz zanke* ℓ označimo z ℓ^{-1} in pomeni, da zanko prepotujemo v obratni smeri.

Definicija 10. *Komutator zank* ℓ_1 in ℓ_2 je zanka $\ell_1\,\ell_2\,\ell_1^{-1}\,\ell_2^{-1}$, ki jo označimo z $[\ell_1\ell_2]$.

V nadaljevanju se bomo omejili zgolj na zanke, ki se izogibajo točkam iz množice D in gredo skozi točko 0, tj. z elementi množice $\Omega_0(\mathbb{C} - D)$. Ko vrednost a potuje po poljubni taki zanki skozi točko 0, se s tem spreminjajo tudi ničle polinoma $p_a(x)$. Zanka se začne in konča v 0, torej ob spreminjanju a po njej ničle polinoma $p_0(x)$ pripotujejo nazaj v ničle istega polinoma. Pri tem si lahko nekatere med njimi izmenjajo lokacijo. Na ta način zanke skozi 0 inducirajo permutacije ničel polinoma $p_0(x)$. Permutacijo, pripadajočo zanki ℓ, označimo kot $\pi(\ell)$.



Slika 2: Zanka ℓ in nevarne točke $a_0, \ldots a_{n-2}$.

Imejmo tako zanko ℓ, ki se začne v točki 0, potuje po realni osi proti a_0, okoli a_0 napravi krog z zelo majhnim polmerom, ter se vrne po realni osi nazaj v 0.

Trditev 6. Ko a prepotuje zanko ℓ, se zamenjata ničli 0 in 1 polinoma p_0, ostale ničle pa se vrnejo vsaka nazaj vase.

Dokaz. Ničle polinoma p_0, ki niso 0 ali 1, se vrnejo vase. Oglejmo si zato, kaj se dogaja z 0 in 1. Dokler a potuje po relani osi od 0 proti a_0, se ničli 0 in 1 pomikata druga proti drugi in to proti pripadajoči večkratni točki b_0, ki leži med njima. Ko je a blizu a_0, sta ničli blizu b_0. Označimo $x = b_0 + \varepsilon$ za neko kompleksno število ε z zelo majhno absolutno vrednostjo. Ugotovimo, za katere vrednosti a je x rešitev enačbe $p_a(x) = 0$. V tem primeru mora biti

$$a = x - x^n = b_0 + \varepsilon - (b_0 + \varepsilon)^n$$

$$= b_0 + \varepsilon(1 - nb_0^{n-1}) - \binom{n}{2}\varepsilon^2 b_0^{n-2} - \ldots - \binom{n}{n-1}\varepsilon^{n-1} b_0 - b_0^n$$

torej po formulah $a_0 = b_0 - b_0^n$ in $1 - nb_0^{n-1} = 0$, ki obe sledita iz trditve 5, lahko ocenimo $a \approx a_0 - C\varepsilon^n$. Iz polarnega zapisa kompleksnih števil sledi, da se a vrti okoli a_0 dvakrat hitreje kot x okoli b_0, ko se a giblje po krožnici, ki je del zanke ℓ. Gibanje ničel 0 in 1 je torej takšno: najprej se iz obratnih smeri približujeta točki b_0, nato zakrožita okoli nje vsaka za pol kroga in pri tem izmenjata mesti, nakar se spet oddaljujeta proti 0 in 1 - le, da se pri tem zamenjata! $\square$

Iz dane trditve sledi, da lahko s spremembo a po neki zanki zamenjamo 0 s katerokoli drugo ničlo polinoma p_0. Vemo namreč, da so te oblike ω_{n-1}^k za $k = 1, \ldots, n-2$ in vidimo, da za kompleksno število x velja, da je rešitev enačbe $p_a(x) = 0$ natanko tedaj, ko je

$$(\omega_{n-1}^k x)^n - \omega_{n-1}^k x = \omega_{n-1}^k (x^n - x) = \omega_{n-1}^k a,$$

torej, ko je $\omega_{n-1}^k x$ ničla polinoma $p_{\omega_{n-1}^k a}(x) = 0$. Torej potovanje a po zanki, ki jo iz zanke ℓ dobimo z množenjem z ω_{n-1}^k, na ničle polinoma p_0 inducira permutacijo, ki zamnenja ničli 0 in ω_{n-1}^k med seboj, ostalih pa ne spremeni.

Trditev 7. Če označimo ničle polinoma p s števili od 1 do n, pri čemer n predstavlja izhodišče, lahko s permutacijami, ki jih inducirajo produkti zanke ℓ, pomnožene s koreni enote, konstruiramo vse elemente S_n.

Dokaz. Imamo vse transpozicije števila n z ostalimi števili. Dovolj je, če pokažemo, da lahko vsako transpozicijo dobimo kot produkt le-teh. Poglejmo si poljubno transpozicijo (ab), kjer velja $1 \leq a, b \leq n$. To transpozicijo lahko zapišemo kot produkt $(an)(bn)(an)$. $\square$

3.2 Reševanje polinomov v radikalih

Polinomska enačba

$$a_n x^n + a_{n-1} x^{n-1} + ... + a_1 x + a_0 = 0 \tag{1}$$

je rešljiva v radikalih, če je mogoče njene ničle izraziti na naslednji način: obstajajo nek $m \in \mathbb{N}$, polinomi p_i in števila $k_i \in \mathbb{N}$ za vse $i = 1, \ldots, m$, da za sistem enačb

$$\begin{aligned} x_1^{k_1} &= p_1(a_1, a_2, ..., a_n), \\ x_2^{k_2} &= p_2(a_1, a_2, ..., a_n, x_1), \\ &\vdots \\ x_m^{k_m} &= p_m(a_1, a_2, ..., a_m, x_1, x_2, ..., x_{m-1}), \end{aligned}$$

lahko vse rešitve (1) najdemo med vrednostmi za x_m.

Posebej se omejimo na polinome $p_a(x)$. Privzemimo, da je enačba $p_a(x) = 0$ rešljiva v radikalih, torej, da obstajajo polinomi $q_1, \ldots, q_m$ in eksponenetni $k_1, \ldots, k_m$, da za sistem enačb

$$x_1^{k_1} = q_1(a),$$

$$x_2^{k_2} = q_2(a, x_1),$$

$$\vdots$$

$$x_m^{k_m} = q_m(a, x_1, x_2, ..., x_{m-1}),$$

vrednosti spremenljivke x_k vsebujejo tudi vse ničle polinoma p_0.

3.3 Permutacije zank

Za nevarne točke proglasimo še vse a, ki rešijo enačbo $q_1(a) = 0$. Glej rešitve v radikalih. Prav tako take a, da bo $q_2(a, x_1) = 0$ za nek x_1. Tako nadaljujemo do q_n in povečamo množico D nevarnih točk. Kljub temu je nevarnih točk še vedno končno mnogo in vse zanke, ki jih obravnavamo, se jim morajo ogibati.

Trditev 8. Naj bo ℓ oblike $[\ell_1, \ell_2]$ za $\ell_1, \ell_2 \in \Omega_0(\mathbb{C} - D)$, potem permutacija, ki jo inducira zanka ℓ, označimo jo s $\pi(\ell)$, fiksira vse x_1, kjer se x_1 nanaša na rešitve v radikalih iz razdelka 3.2.

Dokaz. Fiksiramo en x_1, ki reši enabčo $x_1^{k_1} = q_1(a) \neq 0$. Ostale rešitve so

$$\omega_{k_1} x_1, \omega_{k_1}^2 x_1, ..., \omega_{k_1}^{k_1-1} x_1.$$

Permutacija $\pi(\ell_1)$ slika x_1 v $\omega_{k_1}^s x_1$. Potem slika $\omega_{k_1}^{k_1-1} x_1$ v $\omega_{k_1}^{s+k_1-1} x_1$. Permutacija $\pi(\ell_2)$ slika $\omega_{k_1}^{k_1-1} x_1$ v $\omega_{k_1}^{t+k_1-1} x_1$. Sledi, da je

$$\pi(\ell)(x_1) = \pi(\ell_1)\pi(\ell_2)\pi(\ell_1)^{-1}\pi(\ell_2)^{-1}(x_1) = \omega_k^{s+t-s-t} x_1 = x_1,$$

torej $\pi(l)$ slika x_1 v x_1. $\square$

Trditev 9. Naj bo $\ell = [\ell_1, \ell_2]$, kjer sta ℓ_1, ℓ_2 produkta komutatorjev. Potem $\pi(\ell)$ fiksira vse vrednosti x_2.

Dokaz je enak prejšnjemu, kjer upoštevamo, da je $x_2^{k_2} = q_2(a, x_1)$ in x_1 je fiksen pod $\pi(\ell_1)$ in $\pi(\ell_2)$. Ta dokaz lahko priredimo naprej vse do x_m, kjer nato $\pi(\ell)$ fiksira vse vrednosti x_m, če le je zanka ℓ produkt komutatorjev produkta komutatorjev itd. m-krat.

3.4 Dokaz Abel-Ruffinijevega izreka

Izrek 1 (Abel-Ruffini)**.** *Ni vsaka polinomska enačba stopnje* $n \geq 5$ *rešljiva v radikalih.*

Dokaz. Predpostavimo, da je $p_a(x) = x^n - x + a = 0$ rešljiva v radikalih za vsak a. To pomeni, da so vse rešitve vsebovane med različnimi možnimi vrednostmi za x_m. Imejmo sodo permutacijo n elementov, $n \geq 5$, imenujmo jo π. Permutacijo π lahko z m-kratno uporabo trditve 2 zapišemo kot produkt komutatorjev $\underbrace{\text{produkta komutatorjev ... produkta komutatorjev}}_{(n-1)\text{-krat}}$. Za vsako od notranjih permutacij π_i, tj. permutacij, ki nastopajo v najgloblje vgnezdenih komutatorjih, obstaja zanka $\ell_i \in \Omega_0(\mathbb{C} - D)$, da je $\pi(\ell_i) = \pi_i$. Po prejšnji trditvi sledi, da $\pi(\ell) = \pi$ trivialna permutacija (identiteta). Po drugi strani pa je bila π poljubna soda permutacija, kar ne more biti. S tem smo prišli do protislovja s predpostavko o rešljivosti enačb $x^n - x + a = 0$ v radikalih. $\square$

Literatura

[1] Dimitry Fuchs, Serge Tabachinkov *Mathematical Omnibus: Thirty Lectures on Classic Mathematics*[online.] [citirano 24. avgust 2015] Dostopno na spletnem naslovu: `http://http://www.math.psu.edu/tabachni/Books/taba.pdf`