НАСТАВА МАТЕМАТИКЕ
LIII, 1–2 (2008), 13–22

Др Зоран Каделбург

АБЕЛОВА ТЕОРЕМА О АЛГЕБАРСКИМ ЈЕДНАЧИНАМА ВИШЕГ РЕДА

1. Увод

Међу најтежа тврђења у математици спадају она која тврде да се нешто не може урадити. Рецимо, „сви знамо“ да је немогуће помоћу лењира и шестара извршити квадратуру круга или трисекцију угла, али није превише оних који то знају и да докажу, или бар да укажу на идеју како се тај доказ спроводи. Има, наравно, и тврђења тог типа која се релативно лако доказују, обично свођењем на контрадикцију – о једном таквом чувеном доказу (Еуклидовом доказу да се не може наћи највећи прост број) било је говора у једном од прошлих бројева овог часописа. Такви докази онда спадају међу класичне математичке „бисере“ и често се цитирају, па и предају у школи.

Једно од чувених тврђења поменутог типа, које притом сигурно не спада у категорију очекиваних, а ни лако доказивих, јесте Абелова[1] теорема која тврди да за алгебарску једначину степена већег од четири не постоји формула која је решава у општем случају. Когод да први пут чује за такву чињеницу, вероватно се упита: „А зашто баш 4?“ Другим речима, како то да за 2, 3 и 4 такве формуле постоје, а за 5 и више не? Одговор није ни мало једноставан, но ипак је елементаран (тј. не користи „вишу математику“) и циљ овог чланка је да, углавном следећи књигу [1], изложи поменути Абелов доказ у нешто модификованом облику.

Пре навођења самог доказа, ево неколико историјских напомена.

Стари Грци нису имали алгебарску нотацију, па се за њих решавање алгебарских једначина није постављало. Наравно, решавали су проблеме који би се могли записати у облику линеарних једначина, па и неких квадратних, но средства за њихово експлицитно записивање нису имали. Практично (бар принципијелно) решавање квадратних једначина резултат је средњевековних арапских математичара.

Један од првих резултата ренесансне математике у Италији јесте решавање једначина трећег и четвртог степена. Ако занемаримо проблеме настале (у то време) некоришћењем негативних бројева, као и помало нејасну ситуацију око

[1] Niels Henrik Abel (1802–1829), норвешки математичар

комплексних, нађене су експлицитне формуле, сличне познатим формулама за решења квадратне једначине (наравно, нешто сложеније од њих).

Природно се поставило питање – а даље? После вероватно више покушаја да се нађу сличне формуле за једначину петог степена, изгледа да је италијански лекар (!) Руфини[2] био први који је скупио храброст да јавно искаже тврђење да је такав задатак неостварив. Храброст је била потребна и зато што је у то време међу математичарима била увелико прихваћена чињеница да свака алгебарска једначина (дакле, било ког степена) *има* решења (и то тачно онолико колики је њен степен) у скупу $\mathcal{C}$ комплексних бројева. Истина, строгог доказа још није било, али је и он уследио врло брзо (Гаус[3], 1799. године).

Руфини је покушао и да докаже своје тврђење у књизи „Општа теорија једначина" (Teoria generale delle equazioni) објављеној у Болоњи 1798. године. Његов доказ, међутим, није био потпун, па је слава коначног решења ипак припала младом норвешком математичару Абелу, који је свој доказ објавио у првом тому тада формираног часописа *Crelle's Journal für Mathematik*[4] 1826. године. Наслов чланка био је „Доказ немогућности алгебарског решавања једначина степена већег од четири" (Démonstration de l'imposibilité de la résolution algébraique des équations générales qui dépassent le quatrieme degré).

Доказ који наводимо користи нека каснија тврђења Кронекера[5], Гауса и самог Абела. Да бисмо мало скратили излагање, ограничићемо се случајем једначина чији је степен прост број већи или једнак 5.

2. Помоћни појмови и тврђења

Прецизираћемо најпре неке појмове које ћемо користити. Претпостављаћемо да је читаоцу познат појам *поља*, дакле алгебарске структуре у којој се могу неограничено изводити четири основне рачунске операције (наравно, сем дељења нулом). Најједноставније поље којим ћемо се бавити је поље $\mathcal{Q}$ рационалних бројева.

Ако је $\mathcal{P}$ произвољно потпоље поља $\mathcal{C}$ комплексних бројева, а α, β, γ, … неки елементи из $\mathcal{C} \setminus \mathcal{P}$, поље $\mathcal{P}' = \mathcal{P}[\alpha, \beta, \gamma, \dots]$ представљаће скуп свих рационалних функција од елемената α, β, γ, … , са коефицијентима из $\mathcal{P}$. Рецимо,

$$\mathcal{Q}[\sqrt{2}] = \{\, x + y\sqrt{2} \mid x, y \in \mathcal{Q} \,\}.$$

Функција $f(x)$, односно једначина $f(x) = 0$ у пољу $\mathcal{P}$ је функција, односно једначина, чији су коефицијенти елементи поља $\mathcal{P}$.

Полином

$$F(x) = Ax^n + Bx^{n-1} + \cdots, \quad \text{и одговарајућа једначина} \quad F(x) = 0$$

[2] Paolo Ruffini (1765–1822), италијански лекар и математичар

[3] Carl Friedrich Gauss (1777–1855), немачки математичар

[4] Крелеов часопис је један од најстаријих математичких часописа који без прекида и данас излази. Садашњи наслов му је *Journal für die reine und angewandte Mathematik.*

[5] Leopold Kronecker (1823–1891), немачки математичар

из поља $\mathcal{P}$ су *растављиви* у $\mathcal{P}$ ако се $F(x)$ може представити као производ полинома из $\mathcal{P}$ који су мањег степена. Уколико то није могуће, тај полином и једначина су *нерастављиви*. На пример, полином $x^2 - 10x + 7$ је нерастављив у $\mathcal{Q}$ али је растављив у $\mathcal{Q}[\sqrt{2}]$:

$$x^2 - 10x + 7 = (x - 5 - 3\sqrt{2})(x - 5 + 3\sqrt{2}).$$

Став 1 (Абел[6]). *Ако је p прост број, а број $C \in \mathcal{P}$ није p-ти степен броја из $\mathcal{P}$, тада је једначина*

$$x^p = C$$

нерастављива у пољу $\mathcal{P}$.

Доказ. Претпоставимо да је $x^p - C = 0$ растављива, тако да је

$$x^p - C = \varphi(x)\psi(x),$$

где су φ и ψ полиноми у $\mathcal{P}$ чији слободни чланови A и B су бројеви из $\mathcal{P}$. Ако је r неки корен једначине $x^p = C$, тада су и $r\varepsilon$, $r\varepsilon^2$, ... , $r\varepsilon^{p-1}$ такође њени корени, где је ε комплексни p-ти корен из јединице. Тада слободни чланови полинома φ и ψ (до на знак) износе $A = r^\mu \varepsilon^M$ и $B = r^\nu \varepsilon^N$. Како је $\mu + \nu = p$, бројеви μ и ν су узајамно прости, па постоје цели бројеви h и k такви да је $\mu h + \nu k = 1$. На тај начин за производ K степена A^h и B^k добијамо вредност $r\varepsilon^{hM+kN}$ и, дакле, вредност $K^p = r^p = C$ за p-ти степен броја $K \in \mathcal{P}$. То противречи претпоставци о броју C, чиме је став доказан. ■

Став 2 (Шенеман[7]). *Ако полином*

$$f(x) = C_0 + C_1 x + \cdots + C_{N-1} x^{N-1} + x^N$$

има целобројне коефицијенте који су сви дељиви простим бројем p, при чему C_0 није дељив са p^2, тада је $f(x)$ нерастављив над $\mathcal{Q}$.

Доказ. Претпоставимо да се f може представити као $f = \varphi\psi$, где је

$$\varphi = a_0 + a_1 x + \cdots + a_{m-1} x^{m-1} + x^m,$$
$$\psi = b_0 + b_1 x + \cdots + b_{n-1} x^{n-1} + x^n.$$

Према једном Гаусовом ставу, коефицијенти a и b морају бити цели бројеви. Множењем и упоређивањем добијамо да је

$$C_0 = a_0 b_0, \quad C_1 = a_0 b_1 + a_1 b_0, \quad C_2 = a_0 b_2 + a_1 b_1 + a_2 b_0, \quad \ldots$$

Знамо да $p \mid C_0$, а $p^2 \nmid C_0$. Зато је један од бројева a_0, b_0 дељив са p, а други није. Нека је, на пример, $p \mid a_0$ и $p \nmid b_0$. Из друге једнакости онда следи да $p \mid a_1$, затим из треће да $p \mid a_2$ итд. Најзад, добија се да $p \mid a_m = 1$, што је контрадикција. ■

[6] N. H. Abel, Œuvre complètes, vol. II, p. 196.

[7] Schoenemann, *Crelle's Journal*, **32**, 1846.

Теорема 1 (Абелова[8] теорема о нерастављивим полиномима). *Нека су* f *и* F *полиноми над* $\mathcal{P}$*, при чему је* f *нерастављив. Ако је један корен једначине* $f(x)=0$ *уједно корен једначине* $F(x)=0$*, тада су сви корени прве једначине уједно корени друге. Штавише,* $F(x)$ *је дељив са* $f(x)$ *без остатка, тј.*

$$F(x)=f(x)F_1(x),$$

где је $F_1(x)$ *такође полином над* $\mathcal{P}$*.*

Доказ. Применићемо Еуклидов алгоритам за налажење највећег заједничког делиоца полинома f и F. После одређеног броја дељења (у којима су сви коефицијенти полиноми над $\mathcal{P}$) долазимо до једнакости облика

$$F(x)=F_1(x)g(x),\qquad f(x)=f_1(x)g(x),$$

као и

$$V(x)F(x)+v(x)f(x)=g(x).$$

Нека је α корен једначине $f=0$ који је уједно корен једначине $F=0$. То значи да полиноми f и F имају бар један заједнички фактор $(x-\alpha)$, који је онда чинилац и полинома g (који је над $\mathcal{P}$). Како је f нерастављив, то је могуће једино у случају да је $f_1(x)\equiv 1$ и $f(x)=g(x)$, а тада је

$$F(x)=F_1(x)f(x),$$

што је и требало доказати. ■

Последица 1. *Ако је корен једначине* $f(x)=0$*, која је нерастављива над* $\mathcal{P}$*, уједно корен једначине* $F(x)=0$ *у* $\mathcal{P}$ *која је степена нижег од* f*, онда су сви коефицијенти полинома* F *једнаки нули.*

Последица 2. *Ако је* $f(x)=0$ *нерастављива једначина над* $\mathcal{P}$*, тада не постоји друга нерастављива једначина над* $\mathcal{P}$ *која има заједнички корен са* $f(x)=0$*.*

Најчешћи облик проширивања неког бројног поља $\mathcal{P}$ јесте када му прикључујемо корен нерастављиве једначине (над $\mathcal{P}$)

$$f(x)=x^n+a_1x^{n-1}+\cdots+a_n=0. \tag{1}$$

Тада важи

Став 3. *Сваки број из поља* $\mathcal{P}[\alpha]$*, где је* α *корен нерастављиве једначине* (1) *степена* n*, може се, и то на јединствен начин, приказати као полином* $(n-1)$*-ог степена од* α *са коефицијентима из поља* $\mathcal{P}$*.*

Доказ. Број $\zeta\in\mathcal{P}'=\mathcal{P}[\alpha]$ је дефинисан као резултат замене броја α у рационалну функцију над $\mathcal{P}$, тј. може се представити као $\zeta=\Phi(\alpha)/\Psi(\alpha)$, где су

[8] N. H. Abel, *Crelle's Journal*, **4**, 1829.

Φ и Ψ полиноми над $\mathcal{P}$. Како је $\alpha^n = -a_1\alpha^{n-1} - \cdots - a_n$, сваки степен броја α већи или једнак од n може се изразити преко степена $\alpha^{n-1}, \ldots, \alpha$, па можемо писати $\zeta = \varphi(\alpha)/\psi(\alpha)$, где су φ и ψ полиноми над $\mathcal{P}$ степена највише $n-1$.

Како $f(x)$ и $\psi(x)$ немају заједнички фактор, могу се наћи полиноми $u(x)$ и $v(x)$ над $\mathcal{P}$, такви да је $u(x)\psi(x) + v(x)f(x) = 1$. Ако у ову једнакост заменимо $x = \alpha$, како је $f(\alpha) = 0$, добијамо да је $u(\alpha)\psi(\alpha) = 1$, тј. $\zeta = \varphi(\alpha)u(\alpha)$. Ако израз на десној страни измножимо и још једном све степене броја α веће или једнаке од n изразимо преко степена највише $n-1$, добијамо да је

$$\zeta = c_0 + c_1\alpha + \cdots + c_{n-1}\alpha^{n-1},$$

где су $c_\nu \in \mathcal{P}$.

Јединственост овог представљања се лако доказује. ■

Размотримо сада нешто општију ситуацију када нерастављив полином над $\mathcal{P}$ простог степена p постаје растављив проширивањем поља кореном неког другог нерастављивог полинома.

Став 4. *Нерастављива једначина простог степена p у пољу $\mathcal{P}$ може постати раставља проширивањем поља $\mathcal{P}$ кореном неке друге нераставље једначине само ако је степен те друге једначине дељив са p.*

Доказ. Нека су $f(x) = 0$ и $g(x) = 0$ две нераставље једначине над пољем $\mathcal{P}$, при чему су им степени, редом, p и q (p је прост). Претпоставимо да f постаје раставља проширивањем поља $\mathcal{P}$ кореном α једначине $g(x) = 0$. Тада се f може представити као производ $f(x) = \varphi(x,\alpha)\psi(x,\alpha)$, где су полиноми φ и ψ, редом, степена m и n.

За неки рационалан број r, полином над $\mathcal{P}$

$$u(x) = f(r) - \varphi(r,x)\psi(r,x)$$

анулира се за $x = \alpha$. Према Абеловој теореми 1, полином $u(x)$ се анулира за *све* корене α, α', α'', … нераставље једначине $g(x) = 0$. Зато, на пример, једнакост

$$f(x) - \varphi(x,\alpha')\psi(x,\alpha') = 0$$

важи за свако *рационално* x, па она важи за све вредности од x. Дакле, имамо једнакост

$$f(x) = \varphi(x,\alpha')\psi(x,\alpha'),$$

и слично за све корене једначине $g(x) = 0$.

Из q једнакости

$$f(x) = \varphi(x,\alpha)\psi(x,\alpha), \quad f(x) = \varphi(x,\alpha')\psi(x,\alpha'), \quad \ldots$$

које тако добијамо, множењем следи

$$f(x)^q = \Phi(x)\Psi(x),$$

где су Φ и Ψ производи по q полинома $\varphi(x,\alpha)$, $\varphi(x,\alpha')$, ... , односно $\psi(x,\alpha)$, $\psi(x,\alpha')$, ... Како је сваки од тих производа симетрична функција корена једначине $g(x) = 0$, он се може изразити рационално преко коефицијената једначине $g(x) = 0$ (и преко x), па су $\Phi(x)$ и $\Psi(x)$ полиноми над $\mathcal{P}$.

Сваки од полинома $\Phi(x)$ и $\Psi(x)$ се анулира бар за један корен нерастављаве једначине $f(x) = 0$, па се они могу поделити са $f(x)$ без остатка. Како је f нерастављив, ниједан други делилац није могућ, па као резултат добијамо да је

$$\Phi(x) = f(x)^{\mu}, \quad \Psi(x) = f(x)^{\nu},$$

при чему је $\mu + \nu = q$. Поређењем степена левих и десних страна добијамо да је $mq = \mu p$ и $nq = \nu p$, одакле, како су m и n мањи од p, следи да $p \mid q$. ■

3. Алгебарски решиве једначине

Пређимо сада на формулацију и доказ основног тврђења. За једначину n-тог степена у пољу $\mathcal{P}$ рећи ћемо да је *алгебарски решива* ако се њено решење може изразити (сем помоћу четири рачунске радње) помоћу коначно много операција кореновања, извршених над коефицијентима дате једначине. Другим речима, ако се њен корен ω може одредити следећим поступцима:

1. Налажење a-тог корена $\alpha = \sqrt[a]{P}$ неког елемента из $\mathcal{P}$ (који није a-ти степен елемента из $\mathcal{P}$) и формирање проширења $\mathcal{A} = \mathcal{P}[\alpha]$.

2. Налажење b-тог корена $\beta = \sqrt[b]{A}$ неког елемента из $\mathcal{A}$ (који није b-ти степен елемента из $\mathcal{A}$) и формирање проширења $\mathcal{B} = \mathcal{A}[\beta] = \mathcal{P}[\alpha, \beta]$.

3. Налажење c-тог корена $\gamma = \sqrt[c]{B}$ неког елемента из $\mathcal{B}$ (који није c-ти степен елемента из $\mathcal{B}$) и формирање проширења $\mathcal{C} = \mathcal{B}[\gamma] = \mathcal{P}[\alpha, \beta, \gamma]$, и тако даље, док ова сукцесивна проширења не доведу до поља којем припада тражени корен ω и у којем полином f постаје растављав (с обзиром да поседује фактор $x - \omega$).

Овде се подразумева да су сви изложиоци корена a, b, c, ... прости бројеви. Ово очигледно не представља ограничење.

Да бисмо мало скратили излагање, ограничићемо се на једначине $f(x) = 0$ са рационалним коефицијентима, тако да је $\mathcal{P} = \mathcal{Q}$, уз претпоставку да је f нерастављив полином над $\mathcal{Q}$ степена n који је прост број.

Прво проширење ћемо извршити n-тим кореном из јединице

$$\alpha = \eta = \sqrt[n]{1} = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}.$$

Према ставу 4, ово проширење још увек не чини f растављавим, јер је η корен једначине $x^{n-1} + x^{n-2} + \cdots + x + 1 = 0$ чији је степен мањи од n.

Такође, са сваким проширењем неким кореном који још увек не чини f растављавим, извршићемо и проширење комплексним конјугатом тог корена. Ово некад може бити сувишно, али свакако неће ништа покварити.

Теорема 2 (Кронекер[9]). *Ако је $f(x) = 0$ алгебарски решива једначина чији степен је прост број и која је нерастављива над пољем $\mathcal{Q}$ рационалних бројева, онда она има или тачно један реалан корен или искључиво реалне корене.*

Доказ. Претпоставимо да је $\lambda = \sqrt[l]{K}$ корен помоћу којег добијамо проширење у којем је полином f растављив, дакле претпоставимо да је f још увек нерастављив у неком пољу $\mathcal{K}$ (коме припада број K), али постаје растављив у $\mathcal{L} = \mathcal{K}[\lambda]$:

$$f(x) = \varphi(x,\lambda)\psi(x,\lambda)\chi(x,\lambda)\cdots .$$

Овде су фактори φ, ψ, χ, … нерастављиви полиноми у $\mathcal{L}$ (али свакако нису полиноми у $\mathcal{K}$), чији коефицијенти су полиноми од λ у $\mathcal{K}$.

Како, према ставу 4, прост број n мора бити делилац простог броја l, то мора бити $l = n$.

Једначина $x^l = K$, која је нерастављива у $\mathcal{K}$ према Абеловом ставу 1, има l корена:

$$\lambda_0 = \lambda,\ \ \lambda_1 = \lambda\eta,\ \ \ldots,\ \ \lambda_\nu = \lambda\eta^\nu,\ \ \ldots,\ \ \lambda_{n-1} = \lambda\eta^{n-1}.$$

Како је $\varphi(x,\lambda)$ делилац полинома $f(x)$, онда $\varphi(x,\lambda_\nu)$ такође дели $f(x)$ (в. доказ става 4).

Докажимо да су свих n полинома $\varphi(x,\lambda_\nu)$ нерастављиви у $\mathcal{L}$. Заиста, као у доказу става 4, из $\varphi(x,\lambda_\nu) = u(x,\lambda_\nu)v(x,\lambda_\nu)$ би следило $\varphi(x,\lambda) = u(x,\lambda_\nu)v(x,\lambda)$, но та једнакост је немогућа јер је $\varphi(x,\lambda)$ нерастављив у $\mathcal{L}$.

Докажимо сада да су свих n полинома $\varphi(x,\lambda_\nu)$ различити међу собом. Претпоставимо, супротно, да је $\varphi(x,\lambda\eta^\mu) = \varphi(x,\lambda\eta^\nu)$. Као и пре, овде се λ може заменити са $\lambda\eta^{n-\mu}$, одакле следи

$$\varphi(x,\lambda) = \varphi(x,\lambda H),$$

где је H корен из јединице $\eta^{\nu-\mu}$. Овде се λ опет може заменити са λH, што даје

$$\varphi(x,\lambda H) = \varphi(x,\lambda H^2).$$

Настављањем овог поступка добија се

$$\varphi(x,\lambda) = \varphi(x,\lambda H) = \varphi(x,\lambda H^2) = \cdots ,$$

дакле и

$$\varphi(x,\lambda) = \frac{\varphi(x,\lambda) + \varphi(x,\lambda H) + \cdots + \varphi(x,\lambda H^{n-1})}{n}.$$

Десна страна ове једнакости, међутим, као симетрична функција n корена λ, λH, … једначине $x^n = K$, јесте полином од x над $\mathcal{K}$, тако да је $f(x)$ такође полином од x над $\mathcal{K}$. То се не слаже са претпоставкама учињеним о полиному $f(x)$.

Из доказаних чињеница следи да је $f(x)$ дељив производом $\Phi(x)$ n различитих фактора $\varphi(x,\lambda)$, $\varphi(x,\lambda\eta)$, … , $\varphi(x,\lambda\eta^{n-1})$ који су нерастављиви у $\mathcal{L}$,

$$f(x) = \Phi(x)U(x),$$

[9] L. Kronecker, *Monatsberichte der Berliner Akademie*, 1856.

где је Φ (као симетрична функција корена једначине $x^n = K$), па зато и U полином од x у $\mathcal{K}$. Како $f(x)$ није растављив у $\mathcal{K}$, U мора бити једнак 1, па је

$$f(x) = \Phi(x) = \varphi(x,\lambda)\varphi(x,\lambda\eta)\cdots\varphi(x,\lambda\eta^{n-1}).$$

Претпостављена растављивост полинома $f(x)$ у $\mathcal{L}$ мора бити растављивост на *линеарне* факторе. Дакле, ако су ω, ω_1, ... , ω_{n-1} корени полинома f и $x-\omega$, $x-\omega_1$, ... $x-\omega_{n-1}$ одговарајући линеарни фактори, онда је

$$x-\omega = \varphi(x,\lambda), \quad x-\omega_1 = \varphi(x,\lambda\eta), \quad \ldots, \quad x-\omega_{n-1} = \varphi(x,\lambda\eta^{n-1}),$$

па је зато

$$\begin{aligned}
\omega &= K_0 + K_1\lambda + K_2\lambda^2 + \cdots + K_{n-1}\lambda^{n-1},\\
\omega_1 &= K_0 + K_1\lambda_1 + K_2\lambda_1^2 + \cdots + K_{n-1}\lambda_1^{n-1},\\
&\vdots\\
\omega_{n-1} &= K_0 + K_1\lambda_{n-1} + K_2\lambda_{n-1}^2 + \cdots + K_{n-1}\lambda_{n-1}^{n-1},
\end{aligned}$$

где сви $K_\nu \in \mathcal{K}$.

Једначина $f(x) = 0$ је непарног степена (са реалним коефицијентима), па она има бар један реалан корен. Нека је то $\omega = K_0 + K_1\lambda + K_2\lambda^2 + \cdots + K_{n-1}\lambda^{n-1}$. Разликоваћемо даље следећа два могућа случаја.

1. *Основа K корена λ је реална.*
2. *Основа K је комплексна.*

Случај 1. Овде можемо да претпоставимо да је λ реалан, јер n-ти корени јединице припадају пољу $\mathcal{K}$. У том случају комплексни конјугат броја ω је

$$\bar{\omega} = \overline{K}_0 + \overline{K}_1\lambda + \cdots + \overline{K}_{n-1}\lambda^{n-1},$$

где сви $\overline{K}_\nu \in \mathcal{K}$. Из $\bar{\omega} = \omega$ следи да је

$$(\overline{K}_0 - K_0) + (\overline{K}_1 - K_1)\lambda + \cdots + (\overline{K}_{n-1} - K_{n-1})\lambda^{n-1} = 0,$$

а одатле према ставу 3 следи да је $\overline{K}_\nu = K_\nu$ за свако ν. Дакле, бројеви K_0, K_1, ... , K_{n-1} су такође реални.

Штавише,

$$\omega_\nu = K_0 + K_1\lambda_\nu + \cdots + K_{n-1}\lambda_\nu^{n-1}$$

и

$$\omega_{n-\nu} = K_0 + K_1\lambda_{n-\nu} + \cdots + K_{n-1}\lambda_{n-\nu}^{n-1}.$$

Међутим, како су бројеви $\lambda_\nu = \lambda\eta^\nu$ и $\lambda_{n-\nu} = \lambda\eta^{n-\nu} = \lambda\eta^{-\nu}$ комплексно конјуговани, следи да су ω_ν и $\omega_{n-\nu}$ такође комплексно конјуговани. Дакле, у случају 1 *једначина $f(x) = 0$ има један реалан корен и $(n-1)/2$ парова комплексно конјугованих корена* (ω_1 и ω_{n-1}, ω_2 и ω_{n-2} итд).

Случај 2. Сада, осим кореном $\lambda = \sqrt[n]{K}$, извршимо проширивање поља и комплексним конјугатом $\bar{\lambda} = \sqrt[n]{\overline{K}}$, што значи да је у проширење „ушла“ и реална вредност $\Lambda = \lambda\bar{\lambda}$.

Да је проширење бројем $\Lambda = \sqrt[n]{K\overline{K}}$ само по себи било довољно да учини $f(x)$ растављивим, то би значило да смо у ситуацији као у случају 1. Зато можемо да претпоставимо да је $f(x)$ још увек нерастављив у $\mathcal{K}[\Lambda]$ и не постаје растављив без додатног проширивања помоћу λ.

Из

$$\omega = K_0 + K_1\lambda + \cdots + K_{n-1}\lambda^{n-1}$$

следи да је

$$\begin{aligned}\bar{\omega} &= \overline{K}_0 + \overline{K}_1\bar{\lambda} + \cdots + \overline{K}_{n-1}\bar{\lambda}^{n-1}\\ &= \overline{K}_0 + \overline{K}_1\left(\frac{\Lambda}{\lambda}\right) + \cdots + \overline{K}_{n-1}\left(\frac{\Lambda}{\lambda}\right)^{n-1},\end{aligned}$$

а одатле, због $\bar{\omega} = \omega$, и да је

$$K_0 + K_1\lambda + \cdots + K_{n-1}\lambda^{n-1} = \overline{K}_0 + \overline{K}_1\left(\frac{\Lambda}{\lambda}\right) + \cdots + \overline{K}_{n-1}\left(\frac{\Lambda}{\lambda}\right)^{n-1}.$$

У последњој једнакости сви бројеви сем λ припадају пољу $\mathcal{K}(\Lambda)$ и, како је једначина $x^n = K$ (према Абеловом ставу 1) нерастављива у том пољу, можемо у тој једначини да λ заменимо произвољним кореном λ_ν једначине $x^n = K$.

Ако то учинимо и узмемо у обзир да је

$$\frac{\Lambda}{\lambda_\nu} = \frac{\Lambda}{\lambda\eta^\nu} = \frac{\bar{\lambda}}{\eta^\nu} = \bar{\lambda}\bar{\eta}^\nu = \overline{\lambda\eta^\nu} = \bar{\lambda}_\nu,$$

добијамо да је

$$K_0 + K_1\lambda_\nu + \cdots + K_{n-1}\lambda_\nu^{n-1} = \overline{K}_0 + \overline{K}_1\bar{\lambda}_\nu + \cdots + \overline{K}_{n-1}\bar{\lambda}_\nu^{n-1},$$

тј. $\omega_\nu = \bar{\omega}_\nu$. Дакле, *сви корени једначине $f(x) = 0$ су реални.*

Тиме је тврђење теореме доказано. ∎

Из доказане Кронекерове теореме 2 лако следи закључак који смо желели.

Последица 3 (Абел). *За сваки прост број p већи или једнак 5 постоји једначина степена p која није алгебарски решива.*

Доказ. Посматрајмо једначину

$$x^5 - ax - b = 0,$$

где су a и b природни бројеви дељиви простим бројем q, при чему b није дељив са q^2 и такви да је $4^4a^5 > 5^5b^4$. Према Шенемановом ставу 2, ова једначина је нерастављива. Примена стандардне технике тзв. Штурмовог[10] низа (в. нпр.

[10] Jacques Charles François Sturm (1803–1855), француски математичар

[2] или [3]) даје закључак да ова једначина има тачно 3 реална корена (и два комплексна). Дакле, она не задовољава услов који би следио из Кронекерове теореме када би била алгебарски решива.

Слично се конструише пример у случају $p = 7$ (услов је $6^6 a^7 > 7^7 b^6$), као и за било који други прост број $p \geqslant 5$. ■

ЛИТЕРАТУРА

1. H. Dörrie, *100 Great Problems of Elementary Mathematics*, Dover Publications, New York, 1965.
2. G. Kalajdžić, *Algebra. Osnovni pojmovi*, Matematički fakultet, Beograd, 1992.
3. I. R. Shafarevich, *Selected chapters from algebra. Chapter V: Real numbers and polynomials*, The Teaching of Mathematics, **IV**, 1, 1–34, Beograd 2001.

Математички факултет, Студентски трг 16, Београд

E-mail: `kadelbur@matf.bg.ac.yu`