НАСТАВА МАТЕМАТИКЕ
1996, XLI, 3–4, стр. 1–11

Др Веселин Перић

ОСНОВНА ТЕОРЕМА АЛГЕБРЕ

1. Увод

Као *Основна теорема алгебре* позната је сљедећа теорема:

Теорема 1.1. *Сваки полином* $f(X) \in \mathbf{C}[X]$ *степена* $n := \deg(f) \geqslant 1$ *има у пољу* $\mathbf{C}$ *комплексних бројева бар једну нулу* α.

Ако је $f(X) \in \mathbf{C}$, а $\bar{f}(X)$ полином који се добије из полинома $f(X)$ тако да му се конјугују коефицијенти, тада је $g(X) := f(X) \cdot \bar{f}(X) \in \mathbf{R}[X]$ полином са реалним коефицијентима и $\alpha \in \mathbf{C}$ је нула полинома $g(X)$ ако и само ако је α нула полинома $f(X)$ или полинома $\bar{f}(X)$, тј. α или $\bar{\alpha}$ нула полинома $f(X)$. Зато се Основна теорема алгебре може формулисати и у облику наредне теореме у којој се поставља привидно блажи захтјев.

Теорема 1.2. *Сваки полином* $f(X) \in \mathbf{R}[X]$ *степена* $n := \deg(f) \geqslant 1$ *има у пољу* $\mathbf{C}$ *бар једну нулу* α.

Добро је познато да је, за свако поље K, прстен полинома $K[X]$ *Еуклидов прстен* (в. нпр. [2], I дио, Примјер I, 4.1.), дакле и *прстен главних идеала* (Ibid. Пропозиција I, 4.1.), тј. да је сваки идеал тога прстена *главни идеал*. Одатле се лако закључује да је $K[X]$ уједно *Gauss-ов прстен* (ibid. Теорема I, 4.2.), тј. да вриједи:

Теорема 1.3. *Сваки полином* $f(X) \in K[X]$ *степена* $n := \deg(f) \geqslant 1$ *је производ несводљивих полинома, који су јединствени до поретка и константних фактора.*

У Gauss-овом прстену $K[X]$ сигурно су несводљиви сви линеарни полиноми, за које можемо узимати да су нормирани, тј. да имају облик $X - a$ $(a \in K)$. Но, у општем случају, несводљиви полиноми из $K[X]$, за које опет можемо узимати да су нормирани, не морају бити линеарни, већ могу имати степен већи од 1. Тако у случају $K = \mathbf{Q}$, за сваки природан број n и сваки прост број p, полином $X^n - p \in K[X]$ је несводљив. (В. нпр. [2], I дио, Лема I, 4.5.). Међутим, на основу теореме 1.2, несводљиви полином $f(X) \in \mathbf{R}[X]$ има у $\mathbf{C}$ бар једну нулу α, па је линеаран уколико $\alpha \in \mathbf{R}$, односно квадратан уколико $\alpha \notin \mathbf{R}$. Наиме, $\mathbf{R}[X]$ је Еуклидов прстен, па је у првом случају $f(X)$ дјељив полиномом $X - \alpha \in \mathbf{R}[X]$, а у другом полином $f(X) = \bar{f}(X)$ има у $\mathbf{C}$ и нулу $\bar{\alpha} \neq \alpha$, па је дјељив квадратним полиномом $(X - \alpha)(X - \bar{\alpha}) \in \mathbf{R}[X]$.

Тако из теореме 1.2. слиједи:

Теорема 1.4. *Сваки полином* $f(X) \in \mathbf{R}[X]$ *степена* $n := \deg(f) \geqslant 1$ *је производ несводљивих полинома из* $\mathbf{R}[X]$ *степена 1 или 2.*

Заправо је теорема 1.4. еквивалентна са теоремом 1.2, јер сваки полином $g(X) \in \mathbf{R}[X]$ степена 1 или 2 има сигурно бар једну нулу $\alpha \in \mathbf{C}$.

Ако је K потпоље поља L, каже се да је L *проширење поља* K. Проширење L поља K може се на природан начин схватити као векторски простор над пољем K. Димензија тога векторског простора означава се са $[L : K]$ и кад је ова коначна каже се да је L *коначно проширење поља* K. У том случају, за свако $\alpha \in L$, елененти α^j $(j = 0, 1, \dots, n := [L : K])$ су линеарно зависни над K, тј. постоји неконстантни полином $f(X) \in K[X]$ степена $\deg(f) \leqslant n$ чија је нула α. За елемент α неког проширења L поља К каже се да је *алгебарски елемент* над K, ако постоји ненулти полином $f(X) \in K[X]$ чија је нула α. Проширење L поља K зове се *алгебарско проширење* поља K уколико је сваки елемент $\alpha \in L$ алгебарски над K. За алгебарски елемент $\alpha \in L$ над K постоји нормирани полином $g(X) \in K[X]$ најнижег степена чија је нула α. Тај полином је јединствен и несводљив. Полином $g(X)$ зове се *минимални полином*, а $m := \deg(g)$ *степен алгебарског елемента* α у односу на K. Минимално потпоље $K[\alpha]$ поља L које садржи K и алгебарски елемент α је коначно проширење поља K са $[K[\alpha] : K] = m$ и састоји се од свих елемената облика $a_0\alpha^0 + \dots + a_{m-1}\alpha^{m-1}$. При томе се у пољу $K[\alpha]$ рачуна на природан начин, с тим што се уважава једнакост $g(\alpha) = 0$, дакле потпуно слично као у специјалном случају $K = \mathbf{R}$, $\alpha = i$ и $g(X) = X^2 + 1$.

У вези са овим наводимо без доказа сљедећу *Kronecker-ову теорему* (в. нпр. [2], II дио, теорема II, 1.7.):

Теорема 1.5. *За произвољно поље* K *и сваки (нормирани) несводљиви полином* $g(X) \in K[X]$ *постоји проширење* L *поља* K *које садржи бар једну нулу* α *полинома* $g(X)$.

Примијетимо да, у општем случају, поље $K[\alpha]$ које садржи нулу α полинома $g[X] \in K[X]$ не мора садржавати ниједну нулу неког другог (несводљивог) полинома $h(X) \in K[X]$, па није само по себи јасно зашто би поље $\mathbf{C} = \mathbf{R}[i]$ било изузетак.

Из теореме 1.5. и онога што је речено непосредно прије ње видимо да за произвољно поље K вриједи: *сваки несводљиви полином* $g(X) \in K[X]$ *је линеаран ако и само ако је свако алгебарско проширење* L *поља* K *тривијално, тј. једнако* K. Поље K које нема нетривијалних алгебарских проширења зове се *алгебарски затворено поље*. Према томе вриједи:

Теорема 1.6. *За свако поље* K *еквивалентни су сљедећи искази:*

1) Сваки полином $f(X) \in K[X]$ *има у* K *бар једну нулу;*

2) Сваки несводљиви полином $g(X) \in K[X]$ *је линеаран;*

3) Сваки полином $f(X) \in K[X]$ *степена* $n \geqslant 1$ *је производ линеарних полинома;*

4) Поље K *је алгебарски затворено.*

За свако проширење L поља K произвољан неконстантни полином $f(X) \in K[X]$ има у прстену $L[X]$ јединствен приказ у облику производа несводљивих полинома. У њему се појављује највише $n := \deg(f)$ линеарних полинома, па отуда полином $f(X)$ има у L највише $n := \deg(f)$ нула рачунајући за сваку од њих и њену вишеструкост. На основу теореме 1.5. може се лако доказати сљедећа теорема, која такођер припада Kronecker-у.

Теорема 1.7. *За свако поље* K *и сваки полином* $f(X) \in K[X]$ *степена* $n := \deg(f) \geqslant 1$ *постоји проширење* L *поља* K *које садржи свих* n *нула полинома* $f(X)$.

Минимално проширење L поља K из теореме 1.7. је коначно проширење поља K и зове се *поље разлагања* полинома $f(X)$ у односу на K.

Доказ теореме 1.7. може се скицирати овако. Разложимо $f(X)$ на несводљиве факторе у $K[X]$. Ако међу њима нема фактора степена > 1, можемо узети $L = K$. Ако је $f_1(X)$ несводљиви фактор полинома $f(X)$ у $K[X]$ степена > 1, онда одаберимо проширење $K_1 := K[\alpha_1]$ поља K које садржи нулу α_1 полинома $f_1(X)$, дакле и полинома $f(X)$. Ако се $f(X)$ у $K_1[X]$ разлаже на линеарне факторе можемо узети $L := K_1$. Иначе за несводљиви фактор $f_2(X)$ полинома $f(X)$ у $K_1[X]$ степена > 1 треба конструисати проширење $K_2 := K_1[\alpha_2]$ које садржи нулу α_2 полинома $f_2(X)$, дакле и полинома $f(X)$ итд.

2. Историјски осврт

Најприроднији пут да докажемо да реални полином $f(X) \in \mathbf{R}[X]$ у пољу $\mathbf{C}$ има бар једну нулу, тј. реална *алгебарска једначина* $f(X) = 0$ бар један коријен, је директна конструкција те нуле, односно тог коријена. За линеарни и квадратни полином та конструкција је једноставна и добро позната. Тај пут одабрао је Cardano за случај кубне једначине, а на тај начин (Ferrari-евом методом) ријешена је и биквадратна једначина. Покушаји да се на сличан начин „помоћу радикала“ ријеше и алгебарске једначине вишег степена запели су већ код једначина петог степена. То није нимало случајно, јер је N. H. Abel 1826. године доказао да се на тај начин не може ријешити *општа алгебарска једначина* степена $\geqslant 5$. Тај неочекивани резултат Abel-а добиће мало касније E. Galois у оквиру нове теорије која се данас зове његовим именом. (О томе в. нпр. [2], II дио).

Кад би се свака (реална) алгебараска једначина могла ријешити „помоћу радикала“, онда би се лако могло закључити да њена рјешења леже у пољу $\mathbf{C}$ комплексних бројева, а не како се то вјеровало све до Gauss-а, негдје у „ничијој земљи“, што бисмо данас рекли у неком проширењу поља $\mathbf{C}$.

Слиједећи књигу [1], навешћемо неке кључне датуме од прве мистичне појаве Основне теореме алгебре до њеног данашњег схватања као нечега природног и само по себи јасног.

2.1. Girard (1595–1632) и Descartes (1596–1650). Peter Roth (1608. године) изриче тврдњу да алгебарска једначина степена n има највише n коријена, а Vieta (1540-1603) наводи једначине степена n које заиста имају n коријена. Данас заборављени фламански математичар Albert Girard као први тврди да свака алгебарска једначина има n рјешења. Доказ ове тврдње Girard не наводи, већ га само илуструје на неким примјерима, између осталога на примјеру једначине

$X^4-4X+3=0$. Он међутим не тврди да рјешења имају увијек облик $a+b\sqrt{-1}$, $a, b \in \mathbf{R}$, па би се данашњим језиком могла исказати

2.1.1. Girard-ова теза. *За сваки полином $f(X) \in \mathbf{R}[X]$ степена n постоји проширење K поља $\mathbf{C}$ у коме $f(X)$ има n нула; поље K је евентуално нетривијално проширење поља $\mathbf{C}$.*

Descartes у својој књизи *La Geometrie* (1637. године) наводи став да је сваки полином са нулом α дјељив полиномом $X-\alpha$. Вјерује се да је тај став знао већ и Thomas Harriot (1560?–1621), који је 1585. премјеравао колонију Virginia и тако био први математичар који је живио у Сјеверној Америци. Иначе се овај став зове и Bezoút-ова теорема.

2.2. Leibnitz (1646–1716). У вези са разлагањем рационалне функције на парцијалне разломке ради њене интеграције, Leibnitz се бави питањем да ли се сваки полином $f(X) \in \mathbf{R}[X]$ може приказати као производ реалних полинома степена 1 и 2. Он не само да не вјерује да је тако нешто увијек могуће, него чак погрешно тврди да у разлагању

$$x^4+a^4=\left(x+a\sqrt{i}\right)\left(x-a\sqrt{i}\right)\left(x+a\sqrt{-i}\right)\left(x-a\sqrt{-i}\right)$$

производ никоја два линеарна фактора на десној страни не може бити реалан (квадратни) полином. Изгледа да му при томе није пало напамет да су $\sqrt{i}$ и $\sqrt{-i}$ комплексни бројеви, наиме

$$\sqrt{i}=\frac{1}{2}\sqrt{2}(1+i), \sqrt{-i}=\frac{1}{2}\sqrt{2}(1-i),$$

јер би иначе сигурно видио да је

$$x^4+a^4=\left(x^2+a\sqrt{2}x+a^2\right)\left(x^2-a\sqrt{2}x+a^2\right).$$

2.3. Euler (1707–1783). У једном писму Nikolaus Bernoulli-ју од 1. 11. 1742. године формулише Euler теорему 1.3. за коју је, како смо видјели, Leibnitz мислио да није тачна. За наводни контрапримјер Bernoulli-ја, полином $X^4-4X^3+2X^2+4X+4$ са комплексним нулама

$$x_{1,2}=1 \pm \sqrt{2+i\sqrt{3}}, \quad x_{3,4}=1 \pm \sqrt{2-i\sqrt{3}},$$

доказује Euler да су $(X-x_1)(X-x_3)$ и $(X-x_2)(X-x_4)$ реални полиноми

$$X^2-(2+a)X+1+\sqrt{7}+a \quad \text{и} \quad X^2-(2-a)X+1+\sqrt{7}-a$$

при чему је $a=\sqrt{4+2\sqrt{7}}$.

Осим тога, у једном писму Goldbach-у од 15. 12. 1742. године, Euler понавља своју тврдњу у облику теореме 1.3. и каже да ту тврдњу није потпуно доказао. У том писму он додаје да се имагинарни коријени реалног полинома могу у паровима тако груписати да се након множења припадних корјених фактора добију реални квадратни полиноми. То нам је данас савршено јасно, али тада Goldbach у то није вјеровао и нуди Euler-у полином $X^4+72X-20$ као контрапримјер, али Euler овај полином одмах факторизира.

За полиноме степена $\geqslant 6$ Еулер строго доказује теорему 1.3. Године 1749. проматра општи случај. Његова идеја састоји се у томе да реални нормирани полином $f(X)$ степена $2m := 2^n \geqslant 4$ разлаже у производ $f_1(X) \cdot f_2(X)$ двају нормираних реалних полинома степена $m := 2^{n-1}$. Проматрање само полинома оваквог степена не представља ограничење, јер се сваки ненулти реални полином множењем са aX^d за подесно a и d може довести на посматрани облик. Не представља ограничење ни Euler-ова претпоставка да је

$$f(X) = X^{2m} + a_{2m-2}X^{2m-2} + \cdots + a_0$$

и, у вези са тим

$$f_1(X) = X^m + uX^{m-1} + b_{m-2}X^{m-2} + \cdots + b_0 \quad \text{и}$$
$$f_2(X) = X^m - uX^{m-1} + c_{m-2}X^{m-2} + \cdots + c_0,$$

јер се смјеном $X \mapsto X - a$ за подесно $a \in \mathbf{R}$ може постићи $a_{2m-1} = 0$, па отуда $b_{m-1} + c_{m-1} = a_{m-1} = 0$. Коефицијенти u, a_j, b_k одређују се методом неодређених коефицијената. Euler тврди да се из добијених једнакости које повезују коефицијенте a_i са коефицијентима u, b_j, c_k коефицијенти b_j, c_k добијају као рационалне функције коефицијената a_i и коефицијента u, те да се елиминацијом коефицијената b_j, c_k добија реална нормирана алгебарска једначина степена $\binom{2m}{m}$ са негативним слободним чланом. Посљедња једначина, на основу теореме о међувриједностима, за коју Euler очигледно зна, има сигурно бар један реални коријен. Аргументи Euler-а који се односе на неодређене коефицијенте остају, међутим, недовољно образложени, јер он свој доказ за општи случај само скицира, а сав рачун у вези са њим проводи експлицитно само за специјалан случај $2m = 4$. Зато је према, Euler-овом доказу теореме 1.3, на који је своје примједбе имао и Gauss, остало одређено неповјерење.

Euler своје тврђење формулише и у комплексном облику, тврдећи да *ако алгебарска једначина има и имагинарних коријена, онда су они обавезно облика $a+ib$, при чему су a, b реални бројеви.* То наравно слиједи из теореме 1.3. Мала необичност ове тврдње за данашњег читаоца долази отуда што је појам имагинарног имао такођер своју мистичну фазу, кад није било јасно је ли све имагинарно баш горе наведеног облика.

2.4. D'Alembert (1717–1783). Нешто прије Euler-а учинио је 1746. Jean le Rond d'Alembert први озбиљнији покушај да докаже основну теорему алгебре. Отуда се ова теорема у француској литератури назива његовим именом. Његова идеја састојала се у нешто прикривеном покушају да се минимизира апсолутна вриједност полиномијалне функције $f(X)$. У ту сврху d'Alembert користи сљедећи помоћни став који не доказује:

2.4.1. *За сваки пар (b, c) комплексних бројева са $f(b) = c$ постоји природан број q и у околини тачке c конвергентни ред*

$$h(w) = b + \sum_{\nu=1}^{\infty} c_\nu (w-c)^{\frac{\nu}{q}},$$

тако да за све бројеве w блиске броју c вриједи $f(h(w)) = w$.

Тај помоћни став доказао је Pusieux тек 1851. године (и то уз имплицитно коришћење основне теореме алгебре!).

D'Alembert полази од реалних бројева b, c са $f(b) = c$ и у случају да је $c \neq 0$ налази комплексне бројеве z_1, w_1 са $f(z_1) = w_1$ и $|w_1| < |c|$. Понављање поступка даје све мање апсолутне вриједности полиномне функције $f(x)$ и уз примјену аргументације која се оснива на компактности и d'Alembert-у није могла бити блиска, водило би до нуле полинома $f(X)$.

Пропусте у d'Alembert-овом доказу, условљене временом, извргао је критици Gauss, иако је видовито примијетио да се на истим основама може изградити потпуно строги доказ основне теореме алгебре. Како ћемо видјети, то ће и урадити Argand 1814. године.

Радовима d'Alembert-а и Euler-а пробило се увјерење да свака алгебарска једначина степена $n \geqslant 1$ са комплексним коефицијентима има у пољу $\mathbf{C}$ n коријена.

2.5. Lagrange (1736–1813) и Laplace (1749–1827). Већ 1772. године изразио је Louis Lagrange своје неповјерење према Euler-овом доказу. Lagrange чини нови покушај да докаже факторизацију $f(X) = f_1(X) \cdot f_2(X)$ којом се бавио Euler. Захваљујући властитим резултатима о пермутацијама коријена дате једначине, успијева му да попуни празнине у Euler-овом доказу, истина не сасвим, јер будући да није знао за теорему 1.6, морао се ослањати на фиктивне, платонске коријене.

Године 1795. Laplace приступа доказу основне теореме алгебре на посве нов начин, служећи се као и Lagrange платонским коријенима једначине. Видјећемо како се тај пропуст у Laplace-овом доказу може релативно лако исправити, да би се добио један од најједноставнијих потпуно коректних доказа Основне теореме алгебре.

2.6. Gauss (1777–1855). Октобра 1797. Gauss је најавио, а 1799. објавио свој први доказ основне теореме алгебре, који са данашњег становишта није строг, али је ипак на основу тога доказа in absentia промовисан на Универзитету Helmstedt код J. F. Pfaff-а (1765–1825). Рад у коме је овај доказ објавио Gauss започиње критиком претходних доказа d'Alembert-а и Euler-а, скупа са Laplace-ом водећих математичара онога времена. Особито им приговара што се ослањају на фиктивне нуле полинома и раде са њима као да су стварне; тако Euler своју претпоставку о полиному $f(X)$ који разлаже изриче као претпоставку да је сума његових нула $-a_{2m-1} = 0$. И Laplace-ов доказ, за који тада није још знао, критикује Gauss касније 1815. године, приговарајући му исти недостатак.

Приговори Gauss-а изгубиће на снази тек након што се сазнало за могућност конструкције поља разлагања за сваки полином $f(X)$ над произвољним пољем K. Од тада се приступи Euler-а и Lagrange-а, односно Laplace-а, како је Adolf Kneser примијетио већ 1888. године, сматрају потпуним и коректним доказима основне теореме алгебре. Штавише, Frobenius 1907. године, поводом 200. годишњице рођења Leonhard Euler-а истиче да Euler даје највише алгебарски доказ, који почива на чињеници да свака реална алгебарска једначина непарног степена има бар један реалан коријен. Он сматра неправедним што се Основна теорема алгебре не зове Euler-овим, него Gauss-овим именом, који је на њен доказ ставио само задњи потез.

Ново у Gauss-овом доказу из 1799. је то што он не покушава да израчуна, него да докаже егзистенцију коријена алгебарске једначине. Поред овог доказа, Gauss је дао још три, од којих је посљедњи објавио 1849. године, у години златног јубилеума свог доктората.

Први доказ је тополошке природе и са данашњег становишта има битних пропуста. У том доказу Gauss полази од евидентне чињенице да за комплексну нулу $z_0 = x_0 + iy_0$ реалног полинома $f(Z) = u(X, Y) + iv(X, Y)$ тачка (x_0, y_0) представља пресјек реалних алгебарских кривих $u(X, Y) = 0$ и $v(X, Y) = 0$. Gauss-ов доказ да се ове реалне криве морају сјећи унутар круга $|z| = r$ за довољно велико r није довољно прецизан. Критику и допуну овог Gauss-овог доказа дао је A. Ostrowski тек 1920. године. Он примјећује да је Gauss-ов доказ вођен испод нивоа строгости и прецизности показане у претходној критици доказа Euler-а и Lagrange-а и то не само зато што је изложен у геометријском руху, него и зато што се у њему користе особине алгебарских кривих које нису доказане ни у самој дисертацији, нити у претходној литератури.

Ипак се на основу овог доказа основна теорема алгебре приписује Gauss-у и то не само у њемачкој литератури.

Други Gauss-ов доказ из 1816. године је врло алгебарски. Из анализе се користи једино чињеница да сваки реални полином непарног степена има бар једну нулу. Он полази од основне алгебарске идеје Euler-а уз једно поједностављење које је 1759. године предложио de Foncenex и умјесто недопустивих фиктивних нула користи сасвим допустиве варијабле. Овај Gauss-ов доказ апсолутно је коректан и по данашњим мјерилима.

Исте године дао је Gauss и свој трећи, тополошки доказ. У њему се помоћу двоструких интеграла пребројавају обиласци тачке $f(z)$ око тачке 0 када тачка z пролази затвореном кривом око тачке 0. Основна идеја овог доказа налази се данас у доказима који користе теорију функција и укључују интеграл $\dfrac{1}{2\pi i}\displaystyle\int \dfrac{f'(z)}{f(z)}\,dz$ (Rouché-ов став).

2.6. Argand (1768–1822) и Cauchy (1789–1857). Сигурно најједноставнији доказ основне теореме алгебре објавио је R. Argand 1814. године. Argand, који је идеје свог доказа скицирао још 1806. године, на неочекиван начин поједностављује основну d'Alembert-ову идеју. Он користи општи став о егзистенцији минимума непрекидне функције и тако долази до сасвим новог доказа. Како, међутим, Argand не каже ништа о егзистенсији минимума, његов елементарни доказ није у прво вријеме прихватан. A. Cauchy је дао 1820. године у суштини исти доказ, али у нешто приступачнијој форми. Тиме је значајно допринио да се уствари прошири Argand-ова идеја. Ни Cauchy не образлаже сасвим да $|f(z)|$ поприма најмању вриједност; то је било могуће тек након што се формирао општи појам инфимума. Занимљиво је да у својој познатој књизи *Cours d'Analyse* основној теореми алгебре Cauchy посвећује читаву једну главу, а да при томе уопште не спомиње Argand-а.

У 19. вијеку Argand-ов доказ улази у уџбеничку литературу. У новије вријеме, у односу на доказе који користе теорију функција (нпр. Liouville-ову теорему), Argand-ов доказ пада полако у заборав, иако се може наћи и у неким познатим уџбеницима прве половине овог вијека.

3. Два строга доказа основне теореме алгебре

У свим доказима до 1849. године, укључујући Cauchy-ев, Abel-ов и Jacobi-ев, који су се у међувремену појавили, посматрају се само реални полиноми. Тек у свом четвртом доказу Gauss допушта произвољне комплексне полиноме. Како смо већ истакли, то ипак не представља никакво уопштење.

Ми ћемо овдје изложити два доказа основне теореме алгебре у облику који задовољава данашње захтјеве коректности и прецизности.

3.1. Доказ према Argand-у. У овом доказу користе се сљедеће чињенице:

1) *Сваки комлексни полином је непрекидна функција* $\mathbf{C} \to \mathbf{R}$;

2) *Свака непрекидна функција* $f : K \to \mathbf{R}$ *на компакту* $K \subseteq \mathbf{C}$ *поприма свој минимум;*

3) *Сваки комплексан број има квадратни коријен у* $\mathbf{C}$.

Изјаве 1) и 2) су основне чињенице добро познате из Анализе.

Изјава 3) лако се доказује на основу чињенице да је *сваки позитивни реалан број квадрат реалног броја (и да поље* $\mathbf{R}$ *има карактеристику* 0). (В. нпр. [2], II дио, Додатак I, Лема 1.3.). На основу 3) доказаћемо одмах да вриједи:

3′) *Сваки комплексан број има, за сваки природан број* n, n*-те коријене у* $\mathbf{C}$.

За доказ се служимо индукцијом у односу на n и при томе користимо још из Анализе добро познату чињеницу:

4) *Сваки реалан полином непарног степена има у* $\mathbf{R}$ *бар једну нулу.*

Тврдња 3′) тривијална је за $n = 1$, а према 3) она је тачна за $n = 2$. Нека је сада $n = 2m$, $m > 1$. За произвољно задани комплексан број c, према 3), постоји $\eta \in \mathbf{C}$, $\eta^2 = c$. Како је $m < n$, по претпоставци индукције, постоји $\xi \in \mathbf{C}$, $\xi^m = \eta$. Зато $\xi^n = c$, тј. тврдња 3′) вриједи за све парне бројеве n.

Нека је сада n непаран број. Због 4) можемо узети да $c \notin \mathbf{R}$, $|c| = 1$. На основу 3) постоји $d \in \mathbf{C}$, $d^2 = c$. Но, тада $d\bar{d} = 1$. Проматрајмо полином

$$f(X) := i[\bar{d}(X+i)^n - d(X-i)^n] = i(\bar{d}-d)X^n + \text{чланови нижег степена.}$$

Полином $f(X)$ због $d \notin \mathbf{R}$ има непаран степен n. Осим тога, $\bar{f}(X) = f(X)$, тј. полином $f(X)$ има реалне коефицијенте. Зато према 4), постоји бар једна реална нула a тога полинома. То значи

$$\bar{d}(a+i)^n = d(a-i)^n, \quad \text{тј.} \quad \left(\frac{a+i}{a-i}\right)^n = \frac{d}{\bar{d}} = d^2 = c.$$

Први корак у овом доказу Основне теореме алгебре је

3.1.1. (Cauchy-ева теорема о минимуму). *За сваки полином* $f(Z) = a_0 + a_1 Z + \cdots + a_n Z^n \in \mathbf{C}[Z]$ постоји $c \in \mathbf{C}$, *за које вриједи* $|f(c)| = \inf |f(\mathbf{C})|$.

Доказ. Можемо узети да је $a_n \neq 0$ и $n \geqslant 1$. Доказаћемо прво сљедећи исказ:

3.1.2. *Постоји* $r \in \mathbf{R}$ *тако да вриједи* $|f(z)| > |f(0)|$ *за све* $z \in \mathbf{C}$, $|z| > r$.

За $z \neq 0$ вриједи $|f(z)| = |z|^n |a_n + g(z^{-1})|$, при чему је $g(W) := a_{n-1}W + \cdots + a_0 W^n \in \mathbf{C}[W]$. Како је g непрекидно у тачки 0, постоји $\delta > 0$, тако да вриједи $|g(w)| \geqslant \frac{1}{2}|a_n|$, уколико $|w| < \delta$. Према томе, $|f(z)| \geqslant |z|^n(|a_n| - |g(z^{-1}|) \geqslant \frac{1}{2}|a_n||z|^n$, ако $|z| > \delta^{-1}$. Сад је довољно одабрати $r > \delta^{-1}$ тако да вриједи $|a_n|r^n > 2|a_0|$.

Након ове припреме доказ става 3.1.1. лако се изводи. Како је, скупа са $f(z)$, непрекидна и функција $|f(z)|$, поприма функција $|f(z)|$ на компактном кругу $K := \{\, z \in \mathbf{C} \,:\, |z| \geqslant r \,\}$ свој минимум на основу исказа 2). Постоји, значи, $c \in K$ са $|f(c)| = \inf |f(K)|$. Но, према 3.1.2, $|f(c)| \geqslant |f(0)| \geqslant \inf |f(\mathbf{C} \setminus K)|$, па $|f(c)| = \inf |f(\mathbf{C})|$.

Други корак у Argand-овом доказу је

3.1.3. (Argand-ова неједнакост). *Нека је* $f(Z) \in \mathbf{C}[Z]$ *неконстантни полином. Тада за свако* $c \in \mathbf{C}$ *са* $f(c) \neq 0$ *постоји* $c' \in \mathbf{C}$ *са* $|f(c')| < |f(c)|$.

У доказу неједнакости 3.1.3. одлучну улогу игра сљедећа помоћна тврдња:

3.1.4. *Нека је* k *природан број* $\geqslant 1$ *и нека је*

$$h(Z) := 1 + bZ^k + Z^k g(Z) \text{ за неко } b \in \mathbf{C}, b \neq 0 \text{ и неко } g(Z) \in \mathbf{C}[Z], g(0) \neq 0.$$

Тада постоји $u \in \mathbf{C}$ *са* $|h(u)| < 1$.

Одаберимо k-ти коријен $d \in \mathbf{C}$ броја $-1/b$. Тада $bd^k = -1$, па за свако реално t, $0 < t \leqslant 1$ вриједи

$$|h(dt)| \leqslant |1 - t^k| + |d^k t^k g(dt)| = 1 - t^k + t^k |d^k g(dt)|.$$

Но, полином $g(Z)$ непрекидан је у тачки нула, па због $g(0) = 0$, постоји δ, $0 < \delta < 1$, тако да вриједи $|d^k(g(dt)| < \frac{1}{2}$ за свако t, $0 < t < \delta$. За свако такво t имамо $|g(dt)| \leqslant 1 - t^k + \frac{1}{2}t^k < 1$.

Сад се неједнакост 3.1.3. лако доказује. Скупа са $f(Z)$ неконстантан је и полином $h(Z) := \dfrac{f(c+Z)}{f(c)} \in \mathbf{C}[Z]$. Осим тога вриједи

$$h(Z) = 1 + b_k Z^k + b_{k+1} Z^{k+1} + \cdots + b_n Z^n,\ b_k \neq 0, 1 \leqslant k \leqslant n.$$

Ако сада ставимо $g(Z) := b_{k+1}Z + \cdots + b_n Z^{n-k}$ имаћемо $h(Z) = 1 + b_k Z^k + Z^k g(Z)$, $g(0) = 0$. Зато на основу 3.1.4. постоји $u \in \mathbf{C}$, $|h(u)| < 1$. За $c' := c + u$ вриједи, дакле, $|f(c')| = |h(u)||f(c)| < |f(c)|$

Основна теорема алгебре слиједи непосредно из 3.1.1. и 3.1.2. Према 3.1.1. постоји $c \in \mathbf{C}$, $|f(c)| \leqslant |f(z)|$ за свако $z \in \mathbf{C}$. Према 3.1.2. не може бити $|f(c))| > 0$. То значи, c је нула полинома $f(Z)$.

3.2. Доказ према Laplace-у. За овај доказ, поред 4), користимо сљедеће чињенице:

3″) *Сваки квадратни полином* $f(Z) \in \mathbf{C}[Z]$ *разлаже се на линеарне факторе у* $\mathbf{C}[Z]$.

5) *За сваки неконстантни реални полином* $f(X)$ *постоји проширење* L *поља* $\mathbf{C}$ *над којим се* $f(X)$ *разлаже на линеарне факторе.*

6) *Нека је* L *проширење поља* $\mathbf{R}$, $\xi_1, \dots \xi_n \in L$, *а*

$$\eta_k := \sum_{1 \leqslant \nu_1 < \dots < \nu_k \leqslant n} \xi_{\nu_1} \cdot \ldots \cdot \xi_{\nu_k}$$

елементарне симетричне функције у $\xi_1, \dots, \xi_n$. *Тада је*

$$\prod_{\nu=1}^{n} (X - \xi_\nu) = X^n - \eta_1 X^{n-1} + \eta_2 X^{n-2} - \dots + (-1)^n \eta_n.$$

Осим тога сваки симетрични полином у $\xi_1, \dots, \xi_n$ *са реалним коефицијентима је полином у* $\eta_1, \dots, \eta_n$ *са реалним коефицијентима.*

Исказ 3$''$) еквивалентан је очигледно са 3), а исказ 5) слиједи из Теореме 1.6. за $K = \mathbf{C}$. Исказ 6) вриједи не само за поље $\mathbf{R}$, него и за свако поље K карактеристике 0 и лако се добија у оквиру Теорије Galois-а (в. нпр. [2], II дио, Теорема III, 3.5.). Но, постоје и једноставни директни докази овог исказа. Зато га овдје нећемо доказивати.

Доказаћемо сада да сваки реални нормирани полином $f(X)$ степена $n \geqslant 1$, који ћемо из удобности написати у облику

$$f(X) = X^n - b_1 X^{n-1} + \dots + (-1)^n b_n,$$

има бар једну нулу $c \in \mathbf{C}$.

Доказ се проводи индукцијом у односу на број $k \in \mathbf{N}$ за који вриједи $n = 2^k q$, q непаран број. За $k = 0$ тврдња је тачна на основу 4). Нека је $k > 0$ и тврдња тачна за $k - 1$.

Према 5) постоји проширење L поља $\mathbf{C}$ над којим се $f(X)$ разлаже на линеарне факторе:

$$f(X) = (X - \xi_1)(X - \xi_2) \cdot \ldots \cdot (X - \xi_n).$$

Главна идеја Laplace-а је да се сада проматра полином

$$g_t(X) = \prod_{1 \leqslant \mu < \nu \leqslant n} (X - \xi_\mu - \xi_\nu - t\xi_\mu \xi_\nu)$$

за сваки реалан број t.

Коефицијенти полинома $g_t(X)$ су симетрични реални полиноми у $\xi_1, \dots \xi_n$, дакле, на основу 6), реални полиноми у елементарним симетричним функцијама $b_1, \dots, b_n$, што значи реални бројеви. Осим тога, полином $f_t(X)$ има степен $\binom{n}{2} = \dfrac{n(n-1)}{2} = 2^{k-1} q(2^k q - 1)$ и зато по претпоставци индукције бар једна од његових нула лежи у $\mathbf{C}$. Према томе, сваком реалном броју t одговара пар индекса (μ, ν) за које вриједи $\xi_\mu + \xi_\nu + t\xi_\mu \xi_\nu \in \mathbf{C}$, $1 \leqslant \mu < \nu \leqslant n$. Будући да бројева $t \in \mathbf{R}$ има бесконачно много, а оваквих парова (μ, ν) само коначно много, постоје реални бројеви r, s, $r \neq s$ којима припада исти пар $(\varkappa, \lambda)$, тј. за које вриједи

$$\xi_\varkappa + \xi_\lambda + r\xi_\varkappa \xi_\lambda \in \mathbf{C}, \quad \xi_\varkappa + \xi_\lambda + s\xi_\varkappa \xi_\lambda \in \mathbf{C}.$$

Одатле одмах слиједи $u := \xi_\varkappa \cdot \xi_\lambda \in \mathbf{C}$, $v := \xi_\varkappa + \xi_\lambda \in \mathbf{C}$. То значи да су $\xi_\varkappa$ и ξ_λ нуле квадратног полинома $X^2 - vX + u \in \mathbf{C}[X]$. Отуда, на основу 3″), $\xi_\varkappa,\ \xi_\lambda \in \mathbf{C}$.

Примијетимо да је Lagrange 1797/98. године у вези са Laplace-овим доказом примијетио да му као доказу ништа не недостаје, али да се стварно извођење свих рачуна чини немогућим.

Додајмо на крају још и напомену да се без битних измјена претходни доказ може пренијети на свако поље K карактеристике 0 умјесто поља $\mathbf{R}$ односно $K[i]$ умјесто $\mathbf{C} = \mathbf{R}[i]$. На тај начин може се уопштити један други сличан доказ основне теореме алгебре, у коме се користи нешто више чињеница из Теорије Galois-а (в. [2], II дио, Додатак I, Теорема 1.1.) и који није нипошто једноставнији од овдје изложеног доказа заснованог на Laplace-овој идеји.

ЛИТЕРАТУРА

[1] H.-D. Ebbinghaus et al.: *Zahlen*, 3. Auflage, Springer-Verlag, Berlin Heidelberg, 1992, pp. xiv+33.

[2] V. Perić: *Algebra*, I dio, 3. izdanje, Svjetlost Sarajevo, 1991, pp. 422; II dio, 2. izdanje, Svjetlost Sarajevo, 1989, pp. 196.