Мр Сандра Косић-Јеремић

КОНСТРУКТИБИЛНИ БРОЈЕВИ

Увод

Конструктивни проблеми одувијек су били веома интересантни и омиљени у геометрији. Користећи само лењир и шестар може се извршити велики број конструкција, као на примјер: може се наћи симетрала дужи или угла, из тачке се може конструисати нормала на праву, могу се конструисати неки углови, нпр. $60°$, $30°$, многи правилни многоуглови итд. У свим тим конструкцијама лењир се користи искључиво као права ивица тј. као инструмент помоћу којег може да се конструише права линија, али којим се не мјере дужине. Постоје многи проблеми који не могу да се ријеше само употребом лењира и шестара, као што су три класична грчка проблема:

1. Дуплирање (удвостручење) коцке (наћи страницу коцке чија ће запремина бити два пута већа од запремине дате коцке);
2. Трисекција угла (наћи трећину датог угла само употребом лењира и шестара);
3. Квадратура круга (конструисати квадрат који има исту површину као дати круг).

   Овим проблемима касније је додат још један:

4. Конструкција правилног седмоугла.

За рјешавање ових проблема дозвољена је употреба само лењира и шестара. Многи математичари су се кроз вијекове бавили питањем рјешавања ових проблема. На крају се јавила сумња да ли је уопште могуће ријешити постављене проблеме. Наиме, математичари су добили нови проблем: *Како је могуће доказати да неки проблеми немају рјешења*? Тек након развоја модерне алгебре и теорије група, коју су започели Руфини, Абел и Галоа, доказано је да је да су ови проблеми неријешиви, односно да их је немогуће ријешити само употребом лењира и шестара.

За рјешавање ових проблема било је потребно увести појам конструктибилног броја. Сада ћемо навести неке основне појмове, дефиниције и теореме о проширењима поља који ће нам бити потребни за доказивање неких особина о конструктибилним бројевима и који ће нам послужити за доказивање немогућности рјешавања наведених проблема.

О проширењима поља

Нека је $(R, +, \cdot)$ комутативни прстен са јединичним елементом.

Дефиниција 1. За полином $p(x) \in R[x]$ ($R[x]$ – прстен полинома над R) ненултог степена n кажемо да је *несводљив (иредуцибилан)* над R, ако се $p(x)$ не може написати у облику производа два полинома чији су степени позитивни и мањи од n. У супротном кажемо да је полином $p(x)$ сводљив над R.

Полином првог степена је, по дефиницији, увијек несводљив над прстеном R. Над пољем рационалних бројева $\mathbf{Q}$ може бити несводљив полином ма којег степена. Над пољем реалних бројева несводљиви су само неки полиноми другог степена (и наравно полиноми првог степена који су увијек несводљиви). Над пољем комплексних бројева $\mathbf{C}$ једини несводљиви полиноми су полиноми првог степена. Другим ријечима, поље комплексних бројева је алгебарски затворено. Та хијерархија бројевних поља добијена је проширивањем полазног поља рационалних бројева до таквог поља у којем су једини несводљиви полиноми полиноми првог степена.

Дефиниција 2. *Проширење поља* F је свако поље E које садржи F као потпоље.

Поље E можемо сматрати векторским простором над пољем F. Ако је n димензија векторског простора E, онда кажемо да је E коначно проширење поља F. Коначан број n зове се степен проширења поља E и пишемо $(E : F) = n$. У том случају се сваки елемент $v \in E$ изражава као линеарна комбинација елемената базе који су у E и елемената поља F тј. $v = a_1x_1 + a_2x_2 + \cdots + a_nx_n$, $(a_i \in F)$. Ако је димензија векторског простора E над F бесконачна, онда је E бесконачно проширење поља F. Вриједи и сљедеће: ако је E проширење поља F и K проширење поља E, тада имамо проширење облика $F \subset E \subset K$. У случају проширења коначног степена важи сљедећа теорема (коју наводимо без доказа).

Теорема 1. *Нека су дата проширења* $F \subset E \subset K$. *Степен проширења* $(K : F)$ *је коначан ако и само ако су коначни степени проширења* $(K : E)$ *и* $(E : F)$. *У случају коначног проширења вриједи* $(K : F) = (K : E) \cdot (E : F)$.

Индукцијом се може доказати да ова једнакост важи и за случај коначно много коначних проширења. Наиме, за ланац коначних проширења $F \subset E_0 \subset E_1 \subset \cdots \subset E_{n-1} \subset E_n$ важи $(En : F) = \prod_{k=1}^{n} (E_k : E_{k-1})$.

У скупу природних бројева $\mathbf{N}$ није увијек изводиво одузимање, нпр. $2-4 = -2$ није природан број. Исто тако ни дијељење није увијек могуће. У једном проширењу тог скупа, у скупу цијелих бројева $\mathbf{Z}$ одузимање је увијек могуће, али не и дијељење, нпр. $2 : 3 = 2/3$, а то није цијели број. Сада скуп $\mathbf{Z}$ проширујемо и добијамо скуп $\mathbf{Q}$, скуп свих рационалних бројева, у којем је дијељење увијек могуће (уз изузетак дијељења нулом). У скупу $\mathbf{Q}$ није увијек могуће коријеновање. На примјер, квадратни коријени неких рационалних бројева нису рационални бројеви. Ту долазимо до појма ирационалности тј. ирационалних бројева. Проучавање ирационалних бројева започето је још у старој Грчкој и имало је велики значај и утицај на даљњи развој математике.

Разикујемо два типа ирационалних бројева: алгебарске и трансцендентне бројеве.

Дефиниција 3. Број $\alpha \in E$ је *алгебарски* над $\mathbf{Q}$ ако постоји полином $p(x) = a_0 + a_1x + \cdots + a_nx^n$ над $\mathbf{Q}$ позитивног степена такав да је број α нула полинома $p(x)$, односно коријен једначине $p(x) = 0$.

E је проширење (алгебарско проширење) поља $\mathbf{Q}$, ако је сваки елемент из E алгебарски над $\mathbf{Q}$. Ако такав полином не постоји, онда је број α трансцендентан над $\mathbf{Q}$. Примјери трансцендентних бројева су број π и база природног логаритма e. Трансцедентност броја e доказао је Ермит (Hermite) (1873. год), а броја π Линдеман (Lindemann) (1882. год).

Заправо, не постоји алгоритам који би утврдио да ли је дати број рационалан, алгебарски или трансцендентан. Сви рационални и ирационални бројеви заједно чине скуп реалних бројева $\mathbf{R}$.

Несводљиви полином $p(x)$, са коефицијентима из $\mathbf{Q}$, најмањег позитивног степена који анулира елеменат α и који има најстарији коефицијент (коефицијент уз x_n) једнак 1, зовемо минимални полином елемента α над $\mathbf{Q}$. Степен минималног полинома је степен алгебарског елемента α над $\mathbf{Q}$. За сваки алгебарски елемент постоји јединствен минимални полином који анулира тај елемент.

Примјери.

1. Сви рационални бројеви су алгебарски бројеви степена 1 над $\mathbf{Q}$, јер је свако $r \in \mathbf{Q}$ рјешење једначине $x - r = 0$.

2. Елемент $\sqrt{2}$ је алгебарски над $\mathbf{Q}$ степена 2, јер је коријен једначине $x^2 - 2 = 0$.

3. Елемент $\sqrt[3]{2}$ је алгебарски над $\mathbf{Q}$ степена 3 јер је то коријен (нула) једначине $x^3 - 2 = 0$.

4. Елемент $\sqrt{1 + \sqrt[3]{2}}$ има минимални полином степена 6, јер из $\alpha = \sqrt{1 + \sqrt[3]{2}}$ слиједи $1 + \sqrt[3]{2} = \alpha^2$, односно $\sqrt[3]{2} = \alpha^2 - 1$, а одавде кубирањем доијамо једначину шестог степена са рационалним коефицијентима $\alpha^6 - 3\alpha^4 + 3\alpha^2 - 3 = 0$. Дакле, полином $f(x) = x^6 - 3x^4 + 3x^2 - 3$ анулира елемент α и несводљив је, према Ајзенштајновом критеријуму[1], те је минимални за α.

Нека је E проширење поља F и S подскуп у E. Најмање потпоље у E које садржи $F \cup S$ је пресјек свих потпоља у E која садрже F и подскуп S. За такво потпоље кажемо да је генерисано са S над F и означавамо га са $F(S)$. Специјално, ако је $S = t$, онда ћемо поље генерисано са $F \cup \{t\}$ означавати са $F(t)$. Проширење $F(t)$ је поље које је генерисано елементима из F и елементом t. Јасно је да је $F(t) = F$ ако и само ако $t \in F$.

Ако је $F(t) = E$, онда кажемо да E просто проширење поља F. Ако је при томе t алгебарски елемент, онда кажемо да је E просто алгебарско проширење

[1] **Ајзенштајнов критеријум**. Полином $f(x) = a_0 + a_1x + \cdots + a_nx^n$ над прстеном цијелих бројева $\mathbf{Z}$, чији су сви коефицијенти сем a_n дјељиви неким простим бројем p и a_0 није дјељив са p^2, несводљив је над пољем рационалних бројева $\mathbf{Q}$

поља F. Ако је t трансцендентни елемент, онда је $E = F(t)$ просто трансцендентно проширење. Слично ћемо проширење поља које је генерисано пољем F и скупом елемената $S = \{t_1, \ldots, t_n\}$ означавати са $F(t_1, \ldots, t_n)$.

Сукцесивном примјеном више простих проширења може се добити проширење E поља F које садржи дате елементе $t_1, \ldots, t_n \in E$. Наиме, $F(t_1)$ је најмање поље које садржи F и елемент t_1. Сада проширимо поље $F(t_1)$ додавањем елемента t_2. Овај поступак можемо индуктивно наставити док не добијемо поље $F(t_1, \ldots, t_n)$ као проширење поља $F(t_1, \ldots, t_{n-1})$. Дакле имамо ланац проширења $F \subset F(t_1) \subset F(t_1, t_2) \subset \cdots \subset F(t_1, \ldots, t_n)$.

Појам проширења поља је, заправо, био иницран потребом да се за неки полином над датим пољем, у којем се не могу одредити све нуле тог полинома, одреди шире поље у којем је то могуће.

Теорема 2. (Еуклидов алгоритам за полиноме) *Ако су $f, g \in F[x]$ полиноми, тада постоје јединствени полиноми $q, r \in F[x]$ тако да је $f = g \cdot q + r$, при чему је $\mathrm{st}(r) < \mathrm{st}(g)$ или је $r = 0$.*

Теорема 3. *Ако је полином $p(x) = a_0 + a_1 x + \cdots + a_n x^n$ ($a_i \in F$) несводљив над F, а α је један његов корије у проширеном пољу E поља F, тада је $(E : F) = n$, тј. $(F(\alpha) : F) = n$.*

Доказ. Ако је α коријен полинома $p(x)$ и $p(x)$ је несводљив над F, тада α не може бити коријен ниједног ненула полинома из $F[x]$ степена мањег од n. Претпоставимо супротно, да постоји полином $q(x) \in F[x]$ најмањег степена чији је α коријен и претпоставимо да је $\mathrm{st}(q(x)) < n$. Тада је, на основу претходне теореме, $p = s \cdot q + r$, $s, r \in F[x]$ и $\mathrm{st}(r) < \mathrm{st}(q)$ или је $r = 0$. r не може бити 0, јер је p несводљив полином, па је $\mathrm{st}(r) < \mathrm{st}(q)$, одакле слиједи да је α коријен (нула) полинома $r(x)$, што је контрадикција са претпоставком да је q полином најмањег степена чији је коријен α.

Посматрајмо елементе $1, \alpha, \alpha^2, \ldots, \alpha^{n-1} \in F(\alpha)$. Они су линеарно независни, јер ако би нека нетривијална комбинација ових елемената над F била једнака нули, то би значило да је α коријен неког полинома из $F[x]$ степена мањег од n, а доказали смо да је то немогуће. Докажимо још да ови елементи генеришу $F(\alpha)$.

Како је $p(\alpha) = a_n \cdot \alpha^n + a_{n-1} \cdot \alpha^{n-1} + \cdots + a_1 \cdot \alpha + a_0 = 0$, одавде је $a_n \cdot \alpha^n = -a_{n-1} \cdot \alpha^{n-1} - \cdots - a_1 \cdot \alpha - a_0$, односно када подијелимо ову једначину коефицијентом a_n, добијамо $\alpha^n = -a_n^{-1} a_{n-1} \cdot \alpha^{n-1} - \cdots - a_n^{-1} a_1 \cdot \alpha - a_n^{-1} a_0$ па се за све $k \geqslant n$, α^k може приказати као линеарна комбинација елемената $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$. Дакле за све $b \in F(\alpha)$, $b = \sum_{0 \leqslant i < n} a_i \cdot \alpha^i$, $a_i \in F$, тј. сваки елемент b из $F(\alpha)$ се може изразити (приказати) као линеарна комбинација елемената $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$. ■

Можемо рећи да је скуп $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ база векторског простора $F(\alpha)$ над F, при чему је $n = \mathrm{st}(p)$.

Дефиниција 4. Нека је E проширење поља F. Кажемо да је E *поље разлагања* за полином $p(x)$ степена $n \geqslant 1$ над F ако се $p(x)$ разлаже у E на n

линеарних чинилаца $p(x) = c(x-a_1)(x-a_2)\cdots(x-a_n)$, $(c \in F,\ c \neq 0,\ a_i \in E)$ и не постоји поље између F и $E = F(a_1, a_2, \ldots, a_n)$ у којем се $p(x)$ разлаже на линеарне чиниоце.

Другим ријечима, поље разлагања полинома $p(x)$ степена n је најмање поље у којем тај полином има све нуле (n нула).

Примјери.

1. Доказати да је полином $p = x^2 + 1$ несводљив над пољем реалних бројева $\mathbf{R}$. Затим одредити проширење поља $\mathbf{R}$ у којем полином p има нуле.

Рјешење. Ако би полином x^2+1 био сводљив над $\mathbf{R}$, тада бисмо имали $x^2 + 1 = (ax + b) \cdot (cx + d) = acx^2 + (ad + bc)x + bd$ $(a, b, c, d \in \mathbf{R})$. Из посљедње једнакости изједначавањем одговарајућих коефицијената добијамо: $ac = 1$ и $ad + bc = 0$ и $bd = 1$. Елиминацијом се добија да је $(ad)^2 = -1$, што је немогуће за реалне бројеве a и d.

Поље реалних бројева $\mathbf{R}$ проширићемо пољем $\mathbf{R}(t)$ у којем су сви елементи облика $a + bt$ при чему је $t^2 + 1 = 0$ тј. $t^2 = -1$, а коефицијенти a и b су из $\mathbf{R}$. Дакле, проширење поља реалних бројева помоћу несводљивог полинома $p = x^2+1$ изоморфно је пољу комплексних бројева $\mathbf{C} = \{x + yi \mid x, y \in \mathbf{R}, i^2 = -1\}$.

2. Полином $p = x^2 - 3 \in \mathbf{Q}[x]$ је несводљив над пољем рационалних бројева $\mathbf{Q}$. Одредити најмање поље у којем полином $x^2 - 3$ има нуле.

Рјешење. Као што знамо, степен проширења биће 2. Поље $\mathbf{Q}$ проширићемо пољем $\mathbf{Q}(t) = \{a + bt \mid t^2 = 3, a, b \in \mathbf{Q}\}$, односно $\mathbf{Q}(\sqrt{3}) = \{a + b\sqrt{3} \mid a, b \in \mathbf{Q}\}$. Ако узмемо $x, y \in \mathbf{Q}(\sqrt{3})$ тако да је $x = a_0 + b_0\sqrt{3}$ и $y = a_1 + b_1\sqrt{3}$, биће:

$$\begin{aligned} x + y &= (a_0 + a_1) + (b_0 + b_1)\sqrt{3} \in \mathbf{Q}(\sqrt{3}), \\ x \cdot y &= a_0a_1 + 3b_0b_1 + (a_0b_1 + b_0a_1)\sqrt{3} \in \mathbf{Q}(\sqrt{3}), \\ \frac{x}{y} &= \frac{a_0 + b_0\sqrt{3}}{a_1 + b_1\sqrt{3}} = \frac{a_0a_1 - 3b_0b_1}{a_1^2 - 3b_1^2} + \frac{b_0a_1 - a_0b_1}{a_1^2 - 3b_1^2}\sqrt{3} = r + q\sqrt{3}, \end{aligned}$$

одакле видимо да и количник x/y такође припада пољу $\mathbf{Q}(\sqrt{3})$. Дакле, скуп $Q(\sqrt{3})$ је затворен за све аритметичке операције: сабирање, одузимање, множење и дијељење, па је $\mathbf{Q}(\sqrt{3})$ поље. То је најмање поље у којем полином p има нуле и сводљив је.

Проширење чији су елементи алгебарски степена 2 зове се *квадратно проширење*. Дакле, можемо рећи, поље E је квадратно проширење, ако је $(E : Q) = 2$. При томе ћемо још тражити, ради једноставности, да је $E \subset \mathbf{C}$ јер се лако показује да свако коначно проширење поља рационалних бројева $\mathbf{Q}$ има потпоље у $\mathbf{C}$ изоморфно са тим раширењем. Квадратна проширења су проста проширења, јер су генерисана једним коријеном неког над $\mathbf{Q}$ несводљивог квадратног полинома.

Конструктибилни бројеви

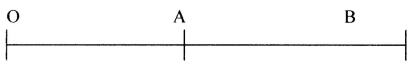
Кључ за што боље разумијевање геометријских проблема лежи у превођењу геометријских проблема на језик алгебре. Једноставности ради, претпоставићемо

да се тражи само једна дуж x. Геометријска конструкција се тада своди на рјешавање алгебарског проблема: наћи везу (једначину) између тражене величине x и датих величина $a, b, c, \ldots$. Затим треба наћи непознату величину x рјешавањем те једначине и на крају треба одредити да ли се то рјешење може добити поступком који одговара конструкцији помоћу лењира и шестара. Лењир не сматрамо инструментом за мјерење дужине. Он нам служи само за цртање правих линија и спајање тачака у равни.

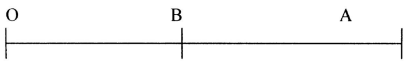
Претпоставићемо да је дат само један елемент који ћемо звати јединична дуж 1. Већ од раније знамо да увијек можемо конструисати било који ненегативан цијели број n: на произвољну праву почињући од неке фиксиране тачке O нанесемо јединичну дуж n пута.

Четири основне аритметичке операције одговарају елементарним геометријским конструкцијама. Наиме, тврдимо да вриједе сљедеће особине:

1) Ако су дате двије дужи са дужинама a и b (мјерене према датој јединичној дужи), тада је увијек могуће конструисати дуж дужине $a + b$. Нека је OA дуж дужине a и нека је AB дуж дужине b. Нацртајмо праву линију и означимо на њој растојања $OA = a$ и $AB = b$. Тада је $OB = a + b$ (сл. 1).



Сл. 1

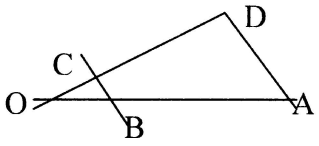


Сл. 2

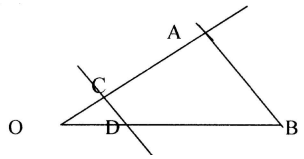
Слично се конструише и $a - b$ $(a > b)$, само што се прво конструише $OA = a$, па се $AB = b$ нанесе у супротном смеру од A, $OB = a - b$ (сл. 2).

Да бисмо конструисали $3a$, једноставно нанаесемо $a + a + a$. Слично можемо конструисати pa, гдје је p природан број.

2) $a/3$ можемо конструисати на сљедећи начин (сл. 3). Означимо $OA = a$ на једној правој и нацртајмо било коју другу праву кроз тачку O. На њој обиљежимо проивољну дуж $OC = c$ и конструишимо $OD = 3c$. Спојимо A и D и конструишемо кроз C праву паралелну правој AD која сијече OA у B. Троуглови OBC и OAD су слични, па према томе вриједи $OB : OA = OC : OD = 1 : 3$. Одавде је $OB = a/3$.



Сл. 3



Сл. 4

На сличан начин се може конструисати дуж a/q $(q \in \mathbf{N})$. Примјењујући овај поступак на дуж pa можемо конструисати ra, гдје је $r = p/q$ било који позитиван рационалан број.

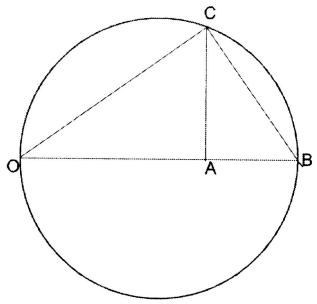
3) Да бисмо конструисали a/b, обиљежимо $OB = b$ и $OA = a$ на крацима било ког угла са врхом у тачки O, а на OB обиљежимо дуж $OD = 1$. Кроз D

конструишимо праву паралелну правој AB која сијече OA у тачки C. Тада ће OC имати дужину a/b (сл. 4). Опет из сличности троуглова OAB и OCD слиједи $OB : OD = OA : OC$, односно $b : 1 = a : OC$, одакле видимо да је $OC = a/b$.

4) За дате дужи a и b, могуће је конструисати ab. Опет као и до сада обиљежимо на крацима неког угла са врхом у тачки O дужи $OA = a$ и $OB = b$. На дужи OA обиљежимо јединичну дуж OC. Повуцимо праву кроз тачке C и B, а затим кроз A праву паралелну овој правој, која ће пресјећи други крак угла у некој тачки D. Тада је $OD = ab$. Доказ исправности конструкције опет слиједи из сличности троуглова OAD и OBC.

Дакле, полазећи од било којих датих дужи, које су мјерене бројевима $a, b, c, \ldots$, можемо узастопном примјеном ових једноставних конструкција одредити било коју величину која може да се изрази помоћу $a, b, c, \ldots$ на рационалан начин, тј. вишеструком примјеном сабирања, одузимања, множења и дијељења. Скуп величина које могу да се добију на тај начин образује бројно поље, тј. скуп бројева такав да примјена рационалних операција на два или више чланова тог скупа даје број који опет припада том скупу.

5) Једна конструкција која нас води ван добијеног поља јесте конструкција квадратног коријена дате дужи: ако је дата дуж a, дуж $\sqrt{a}$ може да се конструише само помоћу лењира и шестара као геометријска средина дужи a и 1. Опис конструкције: на правој линији одредимо дужи $OA = a$ и $AB = 1$. Нацртајмо кружницу чији је пречник дуж OB, тј. кружницу са центром у средишту дужи OB и полупречником $OB/2$, и конструишимо нормалу на OB из тачке A која сијече кружницу у тачки C. Дуж $AC = \sqrt{a}$. Доказ слиједи из сличности троуглова OAC и ABC.



Сл. 5

Дефиниција 5. Кажемо да је реалан број b конструктибилан ако је могуће лењиром и шестаром у коначно корака конструисати одсјечак дужине $|b|$.

Можемо закључити да су сви рационални бројеви и квадратни коријени ових бројева конструктибилни, као и било који број добијен из ових бројева узастопном примјеном претходно описаних конструкција. Дакле, почињући само од дате „јединичне“ дужи и користећи само лењир и шестар, можемо конструисати било који број из проширеног поља $\mathbf{Q}(\sqrt{m})$. У овом проширеном пољу бројеви су облика $a + b\sqrt{m}$ $(a, b \in \mathbf{Q})$. Можемо ићи и даље и искористити један од $\mathbf{Q}(\sqrt{m})$, рецимо $\mathbf{Q}(\sqrt{2})$, умјесто $\mathbf{Q}$. За различите m имаћемо поља $\mathbf{Q}(\sqrt{2}, \sqrt{m})$. На примјер, $\mathbf{Q}(\sqrt{2}, \sqrt{3})$ је проширење поља $\mathbf{Q}$, $\mathbf{Q}(\sqrt{2}, \sqrt{3}) = \{a + b\sqrt{3} \mid a, b \in \mathbf{Q}(\sqrt{2})\}$. Примијетимо да $3 \in \mathbf{Q}(\sqrt{2})$, док $\sqrt{3} \notin \mathbf{Q}(\sqrt{2})$. Да проширимо ово поље можемо изабрати било које његове елементе чији коријени не припадају овом пољу, нпр. $\sqrt{1 + \sqrt{2}}$ или $\sqrt{5 - 2\sqrt{2}}$ можемо искористити да проширимо поље $\mathbf{Q}(\sqrt{2})$.

Овај поступак се може наставити и даље, све док након n корака (n природан број) не добијемо поље које ћемо означити са $Q(\sqrt{m_1}, \sqrt{m_2}, \ldots, \sqrt{m_n})$, гдје су

m_i такви да $\sqrt{m_i} \notin Q(\sqrt{m_1}, \sqrt{m_2}, \ldots, \sqrt{m_{i-1}})$ $(i = 1, 2, \ldots, n)$. Можемо рећи да су сви бројеви из било ког поља добијеног на овај начин конструктибилни. Вриједи и обрнуто, било који конструктибилни број припада проширеном пољу $Q(\sqrt{m_1}, \sqrt{m_2}, \ldots, \sqrt{m_n})$.

Да докажемо ово, претпоставимо да поље K садржи само рационалне бројеве. Конструкција тачке у равни подразумијева конструкцију координата (a, b) те тачке. При томе је довољно знати конструисати дужи дужине $|a|$, односно $|b|$. Свака конструкција лењиром и шестаром подразумијева конструкције тачака пресјека. Тачка пресјека двије праве (једначина праве $ax + by + c = 0$) са коефицијентима из $K = \mathbf{Q}$ има координате које такође припадају пољу K. Да бисмо нашли тачке пресјека праве и кружнице или двије кружнице морамо ријешити квадратну једначину. Заиста, ако узмемо једначину праве $ax + by + c = 0$ и једначину кружнице $(x - p)^2 + (y - q)^2 = r^2$, гдје су коефицијенти $a, b, c, p, q, r \in K$, рјешавањем овог система једначина, добијамо x-координату пресјечне тачке кружнице и праве као рјешење квадратне једначине облика $Ax^2 + Bx + C = 0$ са коефицијентима $A, B, C \in K$. Ако коријени те квадратне једначине не припадају пољу K, можемо их искористити да проширимо поље K.

Укратко, нека постоји конструктибилан број α. Ово једноставно значи да је тај број одређен низом геометријских конструкција у којима користимо само лењир и шестар. Низ је коначан и у сваком кораку конструкције радимо нешто једноставно: цртамо праву линију или кружницу или тражимо пресјек двије праве линије. У првом кораку сви могући елементи имају координате (тачке) или коефицијенте (линије) које припадају $\mathbf{Q}$. Ово стање траје све док не покушамо да одредимо тачке пресјека праве са кружницом или кружнице са кружницом. Понекад ће те тачке пресјека имати координате у $K = \mathbf{Q}$. Међутим, ако координате тачке пресјека не припадају $K = \mathbf{Q}$, мораћемо проширити поље $\mathbf{Q}$ са $\mathbf{Q}(\sqrt{m_1})$, за неко m_1 такво да $\sqrt{m_1} \notin \mathbf{Q}$, а $m_1 \in \mathbf{Q}$. Сада ће K бити $K = Q(\sqrt{m_1})$.

Неколико корака опет можемо остати у пољу $K = Q(\sqrt{m_1})$. Али, ако конструкција захтијева од нас да опет нађемо тачке пресјека са кружницом, опет морамо проширити претходно поље неким m_2, $\sqrt{m_2} \notin \mathbf{Q}(\sqrt{m_1})$, па је сада $K = \mathbf{Q}(\sqrt{m_1}, \sqrt{m_2})$. Ово поље се, ако је потребно, проширује све док се не појави тражено α у току конструкције. Дакле, након неких n проширења (n је коначан природан број) добијамо поље $K = Q(\sqrt{m_1}, \sqrt{m_2}, \ldots, \sqrt{m_n})$ такво да $\alpha \in K$.

У претходном разматрању смо, заправо, доказали сљедећу важну теорему о конструктибилним бројевима.

Теорема 4. *Скуп конструктибилних реалних бројева K је поље, које је проширење поља рационалних бројева $\mathbf{Q}$, при чему је степен проширења $(K : Q) = 2^n$ (n ненегативан цијели број).*

Доказ. Нека су a и b два конструктибилна реална броја. Тада користећи лењир и шестар можемо конструисати одсјечке дужине $|a| + |b|$, $|a| - |b|$, $|a| \cdot |b|$ и $|a|/|b|$, тј. K је поље. Други дио доказа је садржан у претходном разматрању.

Користећи коначно корака у конструкцији можемо сукцесивно добити сљеде-

ћи ланац проширења:

$$\mathbf{Q} \subset \mathbf{Q}(\sqrt{m_1}) \subset \mathbf{Q}(\sqrt{m_1}, \sqrt{m_2}) \subset \cdots \subset Q(\sqrt{m_1}, \sqrt{m_2}, \ldots, \sqrt{m_n}) = K.$$

При томе је свако сљедеће проширење у односу на претходно степена 2 (јер су то све квадратна проширења) па на основу теореме 1 имамо $(K : Q) = 2^n$. ■

Закључак. Конструктибилни бројеви су они до којих се може доћи након коначног низа квадратних проширења поља $\mathbf{Q}$ (број проширења је неки коначан број n), тј. они који се налазе у пољу $K = Q(\sqrt{m_1}, \sqrt{m_2}, \ldots, \sqrt{m_n})$.

Примјене

Као примјену претходне теореме показаћемо најпре да није могуће произвољан угао подијелити на 3 једнака дијела користећи само лењир и шестар (**проблем трисекције угла**).

Доказ. Означимо трећину неког угла са α. Примјеном адиционе теореме имамо да је $\cos 3\alpha = 4\cos^3\alpha - 3\cos\alpha$. Означимо $\cos\alpha = x$ и $\cos 3\alpha = a$ (a је дато). Тада добијамо једначину $4x^3 - 3x = a$, односно $4x^3 - 3x - a = 0$. Ако захтијевамо да полином $p(x) = 4x^3 - 3x - a$ има нуле у неком проширењу E поља рационалних бројева $\mathbf{Q}$, онда то проширење (у општем случају) за ма које a мора бити степена 3, $(E : Q) = 3$ (јер је $p(x)$ полином степена 3), па је на основу претходне теореме број $x = \cos\alpha$ немогуће конструисати само лењиром и шестаром. ■

Други познати старогрчки проблем, **проблем дуплирања коцке**, такође није могуће ријешити само лењиром и шестаром.

Доказ. Претпоставимо да се тражи ивица коцке чија запремина ће бити два пута већа од запремине коцке чија је ивица једнака 1. Овај проблем се своди на рјешавање једначине $x^3 = 2$. Полином $p(x) = x^3 - 2$ је несводљив над $\mathbf{Q}$, он има нулу у проширеном пољу $\mathbf{Q}(\sqrt[3]{2}) = \{a + b\sqrt[3]{2} + c\sqrt[3]{2^2} \mid a, b, c \in \mathbf{Q}\}$. Степен проширења овог поља у односу на $\mathbf{Q}$ је 3, што значи, на основу теореме 4, да та нула, односно рјешење једначине није конструктибилан број, па се не може конструисати коцка дупло веће запремине од запремине дате коцке користећи само лењир и шестар. ■

Лема 1. *Свако коначно проширење поља F је алгебарско.*

Доказ. Нека је E коначно проширење поља F степена n (n ненегативан цијели број) и нека $\alpha \in E$ ($\alpha \neq 0$). Тада су елементи $1, \alpha, \alpha^2, \ldots, \alpha^n$ линеарно зависни (има их $n+1$)[2], јер би иначе димензија проширења E била бесконачна. То значи да постоје елементи $a_i \in F$ који нису сви нула такви да је $a_0 + a_1\alpha + \cdots + a_n\alpha^n = 0$, одакле слиједи да постоји ненулти полином степена n који анулира елемент α. Дакле, α је алгебарски над F. Пошто је α произвољан из E, одавде слиједи да је E алгебарско проширење поља F. ■

[2] *Теорема 1.1.* Ако је V коначно-димензионални векторски простор над F, тада било које две базе векторског простора V над F имају исти број елемената и тај број је тачно $\dim_F(V)$. *Теорема 1.2.* Нека је V коначно-димензионални векторски простор над F такав да $\dim_F(V) = n$, n коначан број. Ако је $m > n$, тада су било којих m елемената из V линеарно зависни над F.

Сада ћемо доказати сљедеће важно тврђење које ћемо формулисати у облику теореме.

Теорема 5. *Сваки конструктибилни број је алгебарски.*

Другим ријечима, сваки конструктибилан број α је нула неког полинома n-тог степена са рационалним коефицијентима.

Доказ. Нека је α било који консруктибилан број. То значи да он припада неком проширењу $K = \mathbf{Q}(\sqrt{m_1}, \sqrt{m_2}, \ldots, \sqrt{m_k})$ за неки коначан број k (k ненегативан цијели број) и степен проширења поља K над $\mathbf{Q}$ је коначан број 2^k, па на основу претходно доказане леме K је такође и алгебарско проширење, што значи да је α алгебарски број. Пошто је α био произвољан конструктибилан број, закључујемо да су сви конструктибилни бројеви алгебарски. ■

Обрнуто не важи! Нису сви алгебарски бројеви конструктибилни. На примјер, коријени једначине трећег степена $x^3 - 2 = 0$ нису конструктибилни.

Пошто је скуп свих алгебарских бројева пребројив, као посљедицу претходног тврђења добијамо да је и скуп свих конструктибилних бројева такође пребројив.

Примјери. Показати да су дати конструктибилни бројеви алгебарски.

1. $x = \sqrt{2 + \sqrt{3}}$. Квадрирањем добијамо $x^2 = 2 + \sqrt{3}$, одакле је $x^2 - 2 = \sqrt{3}$ и $(x^2 - 2)^2 = 3$. Посљедња једначина је, уствари, $x^4 - 4x^2 + 1 = 0$. Дакле, дати број је коријен једначине четвртог степена са коефицијентима из $\mathbf{Q}$, па је дати број алгебарски.

Примијетимо да је дати број x из неког проширења $\mathbf{Q}(\sqrt{3}, \sqrt{2 + \sqrt{3}}) = \{a + b\sqrt{2 + \sqrt{3}} \mid a, b \in \mathbf{Q}(\sqrt{3})\}$. Ово проширење је степена 2^2 у односу на $\mathbf{Q}$, па смо морали два пута вршити квадрирање, односно добили смо једначину четвртог степена са рационалним коефицијентима.

2. На сличан начин се показује да је за $x = \sqrt{2 + \sqrt{2 + \sqrt{2}}}$, $x \in Q_3 = \mathbf{Q}(\sqrt{2}, \sqrt{2 + \sqrt{2}}, \sqrt{2 + \sqrt{2 + \sqrt{2}}})$. Степен проширења $(Q_3 : \mathbf{Q}) = 2^3$, па ће постојати једначина осмог степена која анулира елемент x.

Сада ћемо доказати још једну лему која ће нам бити потребна за доказивање немогућности рјешавања познатих старогрчких проблема које смо споменули на почетку.

Лема 2. *Ако кубна једначина $a_3x^3 + a_2x^2 + a_1x + a_0 = 0$ $(*)$ са рационалним коефицијентима нема рационалних коријена, тада ниједан од њених коријена није конструктибилан.*

Доказ. Претпоставимо да једначина $(*)$ нема рационалних коријена. Тада се у леми тврди да једначина нема конструктибилних коријена.

Претпоставимо супротно, да једначина $(*)$ има конструктибилан коријен α. Као што знамо из теореме 4, конструктибилан број $\alpha \in F_k = \mathbf{Q}(\sqrt{m_1}, \ldots, \sqrt{m_k})$, гдје је k најмањи број проширења поља $\mathbf{Q}$ који је потребан да бисмо конструисали α. Нека $\alpha = a + b\sqrt{m_k}$ $(a, b, m_k \in F_{k-1},\ \sqrt{m_k} \notin F_{k-1})$ задовољава једначину

$(*)$, тј. $P(\alpha)=0$, гдје је $P(x)=a_3x^3+a_2x^2+a_1x+a_0$. Сада ћемо доказати да ако је $\alpha=a+b\sqrt{m_k}$ рјешење кубне једначине $(*)$, тада је и $\alpha_1=a-b\sqrt{m_k}$ такође рјешење те једначине. Из $P(\alpha)=0$ увртавањем $\alpha=a+b\sqrt{m_k}$ добијамо да је

$$a_3(a+b\sqrt{m_k})^3+a_2(a+b\sqrt{m_k})^2+a_1(a+b\sqrt{m_k})+a_0=0.$$

Одавде након груписања добијамо

$$A+B\sqrt{m_k}=0,$$

гдје коефицијенти $A,B,m_k\in F_{k-1}$, па можемо сада писати $P(\alpha)=A+B\sqrt{m_k}$, тј. $P(a+b\sqrt{m_k})=A+B\sqrt{m_k}=0$. Посљедња једнакост је тачна ако и само ако је $A=0$ и $B=0$. Заиста, ако би било нпр. $B\neq 0$ имали бисмо $\sqrt{m_k}=-A/B$, а то је контрадикција са претпоставком да $\sqrt{m_k}\notin F_{k-1}$. Исто тако је $P(a-b\sqrt{m_k})=A-B\sqrt{m_k}=0$ (јер је $A=0$ и $B=0$). Дакле, ако је $a+b\sqrt{m_k}$ коријен једначине $P(x)=0$, тада је и $a-b\sqrt{m_k}$ коријен те једначине.

На основу Вијетових правила мора бити $x_1+x_2+x_3=-\dfrac{a_2}{a_3}$. Знамо да је $x_1=a+b\sqrt{m_k}$ и $x_2=a-b\sqrt{m_k}$. Увртавањем у посљедњу једначину видимо да мора вриједити $a+b\sqrt{m_k}+a-b\sqrt{m_k}+x_3=-\dfrac{a_2}{a_3}$. Одавде слиједи $x_3=-\dfrac{a_2}{a_3}-2a\in F_{k-1}$ (јер се коријен изгубио), што је контрадикција са претпоставком да је k најмањи број за који F_k садржи коријен једначине $(*)$. ■

Сада ћемо још једном доказати немогућност рјешавања проблема **дуплирања коцке**, али сада ћемо у доказу користити претходну лему.

Доказ. Опет ћемо претпоставити да се тражи ивица коцке дупло веће запремине од запремине коцке ивице 1. Овај геометријски проблем се своди на алгебарски проблем: наћи конструктибилно рјешење једначине $x^3-2=0$.

Нека је $x=p/q$ рационално рјешење једначине $x^3-2=0$, при чему су p,q међусобно прости цијели бројеви. Увртавањем у једначину добијамо једначину $p^3=2q^3$, а одавде видимо да је p паран број, тј. $p=2k$ $(k\in ZC)$. Уврстимо p у посљедњу једначину и добићемо $(2k)^3=2q^3$, односно $4k^3=q^3$, што значи да је q дјељив са 4, односно са 2, па је и q паран број, а то је контрадикција са претпоставком да су p и q међусобно прости.

Дакле, пошто једначина $x^3-2=0$ нема рационалних коријена, тада на основу претходне леме, ниједан од њених коријена није конструктибилан, па ова једначина нема конструктибилних рјешења тј. проблем дуплирања коцке се не може ријешити само лењиром и шестаром. ■

Проблем конструкције правилног седмоугла

Правилан троугао, четвороугао, петоугао и шестоугао је лако конструисати само лењиром и шестаром. Такође, сви многоуглови добијени из наведених дуплирањем броја страница такође су конструктибилни. Наиме, из правилног n-тоугла можемо добити правилан $2n$-тоугао половљењем лукова описаног круга, који се налазе изнад страница правилног n-тоугла.

1796. године је млади Гаус показао да је могуће конструисати правилни 17-угао. Као што је Гаус показао, 17-угао је био само посебан случај фамилије конструктибилних правилних многоуглова. Гаус је открио да се правилан p-тоугао

(p прост број) може конструисати ако и само ако је p прост Фермаов број, $p = 2^{2^n} + 1$. Први Фермаови бројеви 3, 5, 17, 257 и 65537 су прости. Међутим, 1732. године, Ојлер је открио да за $n = 5$, $F(n) = 2^{2^n} + 1$ није прост број. Касније се открило да су многи од тих Фермаових бројева сложени.

Али, правилан седмоугао (хептагон) није могуће конструисати само лењиром и шестаром. Проблем је наћи страницу s правилног седмоугла који је уписан у јединични круг. Најједноставнији начин да докажемо да овај проблем није могуће ријешити само лењиром и шестаром је коришћење комплексних бројева.

Знамо да су тјемена правилног седмоугла дата коријенима једначине

$$z^7 - 1 = 0, \tag{1}$$

гдје је $z = x + iy$ (x и y су координате тјемена седмоугла). Очигледно је један коријен ове једначине $z = 1$, па дијелећи једначину (1) са $z-1$ добијамо једначину

$$z^6 + z^5 + z^4 + z^3 + z^2 + z + 1 = 0. \tag{2}$$

Међу коријенима ове једначине је $z = \cos(2\pi/7) + i\sin(2\pi/7)$. Угао $2\pi/7$ је угао захваћен код центра круга страницом правилног седмоугла. Дијелећи једначину (2) са z^3 и уводећи смјену $x = z + \dfrac{1}{z}$, добијамо једначину

$$x^3 + x^2 - 2x - 1 = 0. \tag{3}$$

Сада треба само доказати да једначина (3) нема рационалних коријена, па на основу леме 2 нема ни конструктибилних коријена. Ако једначина (3) има рационалних коријена, ти коријени су уједно и цјелобројни и то дјелиоци броја 1. Увртавањем вриједности за x у једначину (3) видимо да ни -1 ни 1 нису рјешења ове једначине, па једначина (3) нема рационалних рјешења, одакле, на основу леме 2, закључујемо да нема ни конструктибилних рјешења. Дакле, број $x = z + \dfrac{1}{z} = 2\cos(2\pi/7)$ није конструктибилан, па једначина (2) нема конструктибилних рјешења, што значи да се страница седмоугла не може конструисати. ■

О проблему квадратуре круга

То је један од најпознатијих и најинтересантнијих старогрчких проблема. Овим проблемом су се бавили многи познати математичари, али он је остао нерије шен све до 19. вијека, када је Линдеман доказао трансцендентност броја π. А проблем гласи: *да ли је могуће конструисати квадрат исте површине као што је површина датог круга?*

Овај проблем се опет своди на алгебарски проблем: треба испитати да ли једнаачина $x^2 = r^2\pi$ (r је полупречник датог круга) има рационалних рјешења. Рјешење ове једначине је $x = r\sqrt{\pi}$, па се поставља питање да ли је број π коструктибилан.

Тек након Линдемановог доказа трансцендентности броја π (1882. год) постало је јасно да π није конструктибилан. Јер, како је π трансцендентан број, онда он није алгебарски (не постоји полином који анулира тај елемент), па није ни конструктибилан. Линдеманов доказ о трансцендентности броја π се, заправо,

ослања на Ермитов доказ о трансцендентности броја e. Међутим, ови докази су доста сложени, па их овдје нећемо наводити.

И тиме је коначно ријешен најстарији и најчувенији старогрчки проблем – проблем квадратуре круга.

ЛИТЕРАТУРА

1. В. Дашић, *Алгебра*, НИО Универзитетска ријеч, Титоград, 1987.
2. Р. Курант, Х. Робинс, *Шта је математика*, Београд, 1973.
3. Kac, Ulam, *Matematika i logika*, Školska knjiga, Zagreb, 1977.
4. S. Crvenković, I. Dolinka, R. Sz. Madarasz, *Odabrane teme opšte algebre*, Novi Sad, 1998.
5. T. W. Hungerford, *Algebra*, Holt, Rinehart & Winston, New York, Chicago, San Francisco, 1973.
6. V. Perić, *Algebra II*, IGKRO Svjetlost, OOUR Zavod za udžbenike, Sarajevo, 1980.
7. G. Birkhoff, S. MacLane, *A Survey of Modern Algebra*, Macmillan Publishing Co., New York, London, 1965.
8. М. Д. Стојаковић, *Теорија једначина*, Научна књига, Београд, 1973.
9. H. Dorrie, *100 Great Problems of Elementary Mathematics*, Dover Publications, New York, 1965.
10. I. Stewart, *Concepts of Modern Mathematics*, Dover, 1995.
11. М. Божић, *Преглед историје и филозофије математике*, Завод за уџбенике и наставна средства, Београд, 2002.

Природно-математички факултет Бања Лука, 78000 Бања Лука, Српска, БиХ, Младена Стојановића 2

E-mail: jeremic@bl.elta-kabel.com

ОБАВЕШТЕЊА

НОВО У ИЗДАЊУ ДРУШТВА МАТЕМАТИЧАРА СРБИЈЕ

У издању Друштва математичара Србије објављене су следеће нове књиге:

1. *Миодраг Петковић*: ЗАНИМЉИВИ МАТЕМАТИЧКИ ПРОБЛЕМИ ВЕЛИКИХ МАТЕМАТИЧАРА.
2. *Војислав Андрић*: МАТЕМАТИКА 3, збирка решених задатака за 3. разред основне школе, за ученике који желе и могу више, треће допуњено издање, Материјали за младе математичаре, св. 37.

„КЕНГУР БЕЗ ГРАНИЦА“

Овогодишње такмичење „Кенгур без граница“ одржаће се 19. марта 2009. године. Пријава такмичара могућа је преко сајта Друштва математичара Србије www.dms.org.rs.