Klasične konstrukcije i teorija polja

Matija Kazalicki

Duplikacija kocke, trisekcija kuta i kvadratura kruga su klasični konstrukcijski problemi koje su matematičari bezuspješno pokušavali riješiti još od vremena antičke grčke pa sve do devetnaestog stoljeća. Pierre Wantzel je 1837. koristeći metode teorije polja dokazao da duplikacija kocke i trisekcija kuta nisu moguće. Za kvadraturu kruga je trebalo pričekati 1882. kada je Lindemann dokazao transcendentnost broja π.

U ovom predavanju izložiti ćemo ideje iz teorije polja potrebne za razumijevanje ovih klasičnih rezultata. Glavna referenca je knjiga Iana Stewarta Galois theory [1].

1 Teorija polja

U ovom odjeljku proučavmo potpolja polja kompleksnih brojeva $\mathbb{C}$. Krenimo sa definicijom.

Definicija 1.1. *Neka je $K \subset L$ potpolje polja L. Kažemo da je L proširenje od K. Lako se provjeri da je uz prirodne operacije L vektorski prostor nad K. Ako je dimenzija tog vektorskog prostora konačna kažemo da je L konačno proširenje od K stupnja $[L : K] := \dim_K L$. Konačna proširenja od $\mathbb{Q}$ nazivamo polja algebarskih brojeva.*

Primjer. Polje $\mathbb{Q}(i) = \{a + bi : a, b \in \mathbb{Q}\}$ je proširenje od $\mathbb{Q}$ stupnja 2.

Općenito, ako je $K \subset \mathbb{C}$ polje i $X \subset \mathbb{C}$ bilo koji skup, sa $K(X)$ označavamo najmanje polje koje sadrži K i X. Možemo ga konstruirati kao presjek svih polja koje sadrže K i X (taj presjek je neprazan jer se $\mathbb{C}$ nalazi u njemu).

Neka je $\alpha \in \mathbb{C}$ bilo koji algebarski broj i $P(x) = a_0 + a_1 x + \ldots + x^n \in \mathbb{Q}[x]$ njegov minimalni polinom (tj. polinom minimalnog stupnja s racionalnim koeficijentima koji ga poništava). Proširenje od $\mathbb{Q}$ s jednim elementom α zovemo jednostavno proširenje. Sljedeća propozicija opisuje jednostavna proširenja.

Proposition 1.2. *Vrijedi da je* $\mathbb{Q}(\alpha) = \{b_0 + b_1\alpha + \ldots + b_{n-1}\alpha^{n-1} : b_i \in \mathbb{Q}\}$*, odnosno* $\mathbb{Q}(\alpha)$ *je proširenje od* $\mathbb{Q}$ *stupnja* n*.*

Dokaz. Skup $\{1, \alpha, \ldots, \alpha^{n-1}\}$ je linearno nezavisan nad $\mathbb{Q}$ (inače $P(x)$ ne bi bio minimalni polinom od α) pa je dovoljno provjeriti da je skup $\{b_0 + b_1\alpha + \ldots + b_{n-1}\alpha^{n-1} : b_i \in \mathbb{Q}\}$ polje (s prirodnim operacijama). Skup je očito zatvoren na zbrajanje i množenje (uočimo da α^n možemo zapisati kao $-a_0 - a_1\alpha - \ldots a_{n-1}\alpha^{n-1}$) pa treba jedino provjeriti zatvorenost na inverz.

Neka je $\beta \in \{b_0 + b_1\alpha + \ldots + b_{n-1}\alpha^{n-1} : b_i \in \mathbb{Q}\}$ proizvoljan. Tada su elementi $\{1, \beta, \beta^2, \ldots, \beta^n\}$ linearno zavisni nad $\mathbb{Q}$ pa postoje $c_i \in \mathbb{Q}$ takvi da je $c_0 + c_1\beta + \cdots + c_n\beta^n = 0$. Ako je $c_0 \neq 0$ tvrdnja slijedi dijeljenjem jednakosti sa $c_0\beta$. Inače jednakost podijelimo s $c_{k-1}\beta^k$ gdje je c_{k-1} prvi element niza $(c_i)_i$ različit od nule. $\square$

Proposition 1.3. *Neka je* $F \subset K \subset L$ *toranj konačnih proširenja. Tada vrijedi*

$$[L : F] = [L : K][K : F].$$

Dokaz. Neka je $\{l_1, \ldots, l_r\}$ baza za L/K i $\{k_1, \ldots, k_s\}$ baza za K/F. Dovoljno je dokazati da je $S = \{l_i k_j : 1 \leq i \leq r, 1 \leq j \leq s\}$ baza za L/F.

Skup je linearno nezavisan nad F, jer da nije skup $\{l_1, \ldots, l_r\}$ bi bio linearno zavisan nad K. Neka je $\gamma \in L$ proizvoljan. Tada postoje $d_i \in K$ takvi da je $\beta = \sum_{i=1}^{r} d_i l_i$. Svaki d_i se može zapisati kao linearna kombinacija elemenata k_j s koeficijentima iz F. Uvrštavanjem slijedi da se β može prikazati kao linerna kombinacija elemenata iz S s koeficijentima iz F, što pokazuje da je S baza za L/F. $\square$

Trebat će nam još jedna standardna definicija.

Definicija 1.4. *Kompozicija polja K i L, polje KL, je najmanje polje koje sadrži oba polja (tj. $KL = K(L)$).*

2 Konstrukcije ravnalom i šestarom

Zbog lakše primjene teorije polja na probleme konstrukcija, identificirat ćemo Euklidsku ravninu $\mathbb{R}^2$ s poljem $\mathbb{C}$.

Za $z_1, z_2 \in \mathbb{C}$ i $r \in \mathbb{R}$, označimo sa $L(z_1, z_2)$ pravac kroz z_1 i z_2, odnosno sa $C(z_1, r)$ kružnicu sa središtem u z_1 radijusa r. Sljedeća definicija formalizira pojam konstrukcije ravnalom i šestarom.

Definicija 2.1. *Za svaki $n \in \mathbb{N}$ označimo sa $\mathcal{P}_n$, $\mathcal{L}_n$ i $\mathcal{C}_n$ točke, pravce i kružnice konstruktibilne u n koraka koje definiramo rekurzivno sa*

$$\mathcal{P}_0 = \{0, 1\}, \mathcal{L}_0 = \emptyset, \mathcal{C}_0 = \emptyset,$$

$$\mathcal{L}_{n+1} = \{L(z_1, z_2) : z_1, z_2 \in \mathcal{P}_n\},$$
$$\mathcal{C}_{n+1} = \{C(z_1, |z_2 - z_3|) : z_1, z_2, z_3 \in \mathcal{P}_n\},$$

$$\begin{aligned} \mathcal{P}_{n+1} &= \{z \in \mathbb{C} : z \text{ } z \textit{ je presjek različitih pravaca iz } \mathcal{L}_{n+1} \} \cup \\ &= \{z \in \mathbb{C} : z \text{ } z \textit{ je presjek pravca iz } \mathcal{L}_{n+1} \textit{ i kružnice iz } \mathcal{C}_{n+1} \} \cup \\ &= \{z \in \mathbb{C} : z \text{ } z \textit{ je presjek dvije različite kružnice iz } \mathcal{C}_{n+1} \} \end{aligned}$$

Primjer. $\mathcal{P}_1 = \{-1, 0, 1, 2, \frac{1 + \pm i\sqrt{3}}{2}\}$.

Definicija 2.2. *Za točku $z \in \mathbb{C}$ kažemo da je konstruktibilna ako i samo ako je $z \in \mathcal{P}_n$ za neki $n \in \mathbb{N}$.*

Definicija 2.3. *Pitagorejsko zatvorenje $\mathbb{Q}^{py}$ od $\mathbb{Q}$ je najmanje potpolje K od $\mathbb{C}$ sa svojstvom:*

$$z \in K \implies \pm\sqrt{z} \in K. \tag{2.1}$$

Napomena. $\mathbb{Q}^{py}$ se može definirati kao presjek svih polja K sa svojstvom (2.1).

Sljedaća propozicija opisuje strukturu polja $\mathbb{Q}^{py}$.

Proposition 2.4. *Neka je $\alpha \in \mathbb{Q}^{py}$. Tada postoji toranj*

$$\mathbb{Q} = L_0 \subset \text{Ł}_1 \subset \ldots \subset L_n,$$

takav da je $\alpha \in L_n$ i $[L_{j+1}, L_j] = 2$ za sve j.

Dokaz. Reći ćemo da je polje algebarskih brojeva $L \subset \mathbb{C}$ 2-rješivo (pripazite, ovo nije standardna definicija) ako postoji toranj

$$\mathbb{Q} = L_0 \subset \text{Ł}_1 \subset \ldots \subset L_n = L,$$

gdje je $[L_{j+1}, L_j] = 2$ za sve j.

Označimo sa F uniju svih 2-rješivih polja. Dokazat ćemo da je F polje i da zadovoljava svojstvo (2.1). Tada tvrdnja slijedi jer iz minimalnosti od $\mathbb{Q}^{py}$ slijedi da je $\mathbb{Q}^{py} \subset F$.

Neka su $\alpha, \beta \in F$. Tada postoje 2-rješiva polja M i N takva da je $\alpha \in M$ i $\beta \in N$. Neka su $\mathbb{Q} = M_0 \subset M_1 \subset M_2 \subset \ldots \subset M_r = M$ i $\mathbb{Q} = N_0 \subset N_1 \subset N_2 \subset \ldots \subset N_s = N$ pripadni tornjevi. Tada je i njihova kompozicija MN 2-rješivo polje jer toranj

$$\mathbb{Q} = M_0 \subset M_1 \subset \ldots \subset M_r \subset M_r N_1 \subset M_r N_2 \subset \ldots \subset M_r N_s = MN$$

zadovoljava definiciju 2-rješivosti nakon što iz njega izbacimo polja koja se ponavljaju (vidi Zadatak 1).

Slijedi da je $MN \subset F$ pa su $\alpha + \beta, \alpha\beta$ i α^{-1} elementi od F, odnosno F je polje.

Za dokaz svojstva (2.1), neka je $\alpha \in F$. Tada postoji 2-rješivo polje G takvo da je $\alpha \in G$. Polje $G(\sqrt{\alpha})$ je također 2-rješivo pa je $\pm\sqrt{\alpha} \in F$, odnosno svojstvo (2.1) je zadovoljeno. $\square$

Zadatak 1. Neka su F_1, F_2 i F_3 polja algebarskih brojeva za koje je $[F_1 : F_2] = 2$. Tada je $[F_3 F_1 : F_3 F_2] = 1$ ili 2.

Teorem 2.5. *Točka $z \in \mathbb{C}$ je konstruktibilna ako i samo ako je $z \in \mathbb{Q}^{py}$. Ekvivalentno*

$$\cup_{n=0}^{\infty} \mathcal{P}_n = \mathbb{Q}^{py}.$$

Dokaz. Dokazat ćemo da je $\mathcal{P}_n \subset \mathbb{Q}^{py}$ za svaki prirodan broj n. Dokaz druge implikacije možete pogledati u [1, odjeljak 7.2].

Tvrdnju dokazujemo indukcijom po n. Očito je $\mathcal{P}_0 = \{0, 1\} \subset \mathbb{Q}^{py}$. Pretpostavimo $\mathcal{P}_n \subset \mathbb{Q}^{py}$. Neka je $z \in \mathcal{P}_{n+1}$. Dokažimo da je $z \in \mathbb{Q}^{py}$. Iz induktivne definicije skupa $\mathcal{P}_{n+1}$ slijedi da imamo tri slučaja: z je presjek dva pravca, pravca i kružnice ili presjek dvije kružnice. Mi ćemo dokazati treći slučaj (prva dva se dokazuju na sličan način).

Pretpostavimo $z \in C(z_1, |z_2 - z_3|) \cap C(z_4, |z_5 - z_6|)$ gdje su $z_i \in \mathcal{P}_n \subset \mathbb{Q}^{py}$. Neka je $r = |z_2 - z_3|$ i $s = |z_5 - z_6|$.

Tada postoje $\theta, \phi \in \mathbb{R}$ takvi da je

$$z = z_1 + re^{i\theta} \qquad \text{i} \qquad z = z_2 + se^{i\phi}.$$

Konjugiranjem ta dva izraza i množenjem dobivamo

$$(z - z_1)(\bar{z} - \bar{z_1}) = r^2,$$

$$(z - z_4)(\bar{z} - \bar{z_4}) = s^2.$$

Eliminacijom $\bar{z} = \frac{r^2}{z-z_1} + \bar{z_1}$ iz prve jednakosti i uvrštavanjem u drugu dobivamo kvadratnu jednadžbu u z s koeficijentima iz $\mathbb{Q}^{py}$. Rješavanjem te jednadžbe slijedi $z \in \mathbb{Q}^{py}$ (ovdje koristimo svojstvo (2.1) polja $\mathbb{Q}^{py}$). □

Teorem 2.6. *Broj $\alpha \in \mathbb{C}$ je element od $\mathbb{Q}^{py}$ ako i samo ako postoji toranj proširenja*

$$\mathbb{Q} = K_0 \subset K_1 \subset \ldots \subset K_n = \mathbb{Q}(\alpha),$$

takav da je $[K_{j+1} : K_j] = 2$ za sve $j = 0, \ldots, n-1$.

Dokaz. Pretpostavimo da takav toranj postoji. Dokazat ćemo indukcijom da $K_j \subset \mathbb{Q}^{py}$. Jasno, $K_0 \subset \mathbb{Q}^{py}$. Neka je K_{j+1} proširenje od K_j stupnja dva. Tada je $K_{j+1} = K_j(\beta)$ gdje je β bilo koji element iz K_{j+1} koji se ne nalazi u K_j. Minimalni polinom od β je stupnja 2. Rješavanjem te kvadratne jednadžbe slijedi da je $\beta \in \mathbb{Q}^{py}$, odnosno $K_{j+1} \subset \mathbb{Q}^{py}$.

Pretpostavimo da je $\alpha \in \mathbb{Q}^{py}$. Iz Propozicije 2.4 slijedi da postoji toranj

$$\mathbb{Q} = L_0 \subset L_1 \subset L_2 \subset \ldots \subset L_n,$$

takav da je $[L_{j+1} : L_j] = 2$ za sve j i da L_n sadrži α (pa onda i $\mathbb{Q}(\alpha)$). Definirajmo $M_j = L_j \cap \mathbb{Q}(\alpha)$. Lako se vidi da je $[M_{j+1} : M_j] = 1$ ili 2 za sve j (dokažite!). Ako iz tornja $(M_j)_j$ izbacimo polja koja se ponavljaju (polja M_{j+1} za koje je $[M_{j+1} : M_j] = 1$), dobit ćemo toranj sa traženim svojstvom (jer je $M_n = \mathbb{Q}(\alpha)$). □

Iz prethodnog teorema direktno slijedi nužan uvjet konstruktibilnosti koji ćemo koristiti kod dokazivanja nemogućnosti klasičnih konstrukcija.

Teorem 2.7. *Ako je $\alpha \in \mathbb{C}$ konstruktibilan, onda je $[\mathbb{Q}(\alpha) : Q]$ potencija broja dva.*

3 Primjena na klasične konstrukcije

U ovom odjeljku ćemo pomoću teorije koju smo do sada razvili riješiti (negativno) četiri klasična konstrukcijska problema: duplikaciju kocke, trisekciju kuta, kvadraturu kruga i konstrukciju pravilnog sedmerokuta.

Duplikacija kocke je problem konstrukcije kocke koja ima dvostruko veći volumen nego zadana kocka (za koju možemo pretpostaviti da ima stranicu duljine 1).

Teorem 3.1. *Kocka se ne može duplicirati šestarom i ravnalom.*

Dokaz. Duplikacija kocke je ekvivalentna konstrukciji broja $\alpha = \sqrt[3]{2}$. Kako je minimalni polinom od α jednak $x^3 - 2$, slijedi da je $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$, što nije potencija od 2 pa se α prema prethodnom teoremu ne može konstruirati. □

Trisekcija kuta je problem dijeljenja danog kuta na tri jednaka dijela.

Teorem 3.2. *Postoji kut koji se ne može podijeliti na tri jednaka dijela pomoću ravnala i šestara.*

Dokaz. Dokazat ćemo da se kut $2\pi/3$ ne može podijeliti na tri jednaka dijela. Znamo da je $\omega = e^{2\pi i/3} = \cos(2\pi/3) + i\sin(2\pi/3) \in \mathbb{Q}^{py}$ (jer je kut $2\pi/3$ konstruktibilan). Pretpostavimo da takva konstrukcija postoji. Tada je $\zeta = e^{2\pi i/9} \in \mathbb{Q}^{py}$ pa je i $\alpha = \zeta + \zeta^{-1} \in \mathbb{Q}^{py}$, odnosno stupanj minimalnog polinoma od α je potencija od 2. Računamo, iz $\omega^2+\omega+1 = 0$ slijedi $\zeta^6 + \zeta^3 + 1 = 0$, tj. $\zeta^3 + \zeta^{-3} = -1$. Vrijedi

$$\alpha^3 = (\zeta + \zeta^{-1})^3 = \zeta^3 + 3\zeta + 3\zeta^{-1} + \zeta^{-3} = 3\alpha - 1,$$

pa je minimalni polinom od α jednak x^3-3x+1 (polinom je ireducibilan). Kako stupanje od α nije potencija od 2, dobili smo kontradikciju. $\square$

Kvadratura kruga je problem konstrukcije kvadrata čija je površina jednaka površini danog (jediničnog) kruga.

Teorem 3.3. *Kvadratura kruga nije moguća sa ravnalom i šestarom.*

Dokaz. Ova konstrukcija je ekvivalentna konstrukciji broja $\sqrt{\pi}$. Ako je $\sqrt{\pi}$ konstruktibilan, onda je i π konstruktibilan pa je po Teoremu 2.7 stupanj proširenja $[\mathbb{Q}(\pi) : \mathbb{Q}]$ potencija od 2. Posebno slijedi da je π algebarski broj što je u kontradikciji sa Lindemannovim teoremom prema kojem je π transcendentalan broj. $\square$

Teorem 3.4. *Pravilni sedmerokut se ne može konstruirati ravnalom i šestarom.*

Dokaz. Konstrukcija pravilong sedmerokuta je ekvivalentna konstrukciji središnjeg kuta $2\pi/7$, odnosno konstruktibilnosti broja $\zeta_7 = e^{2\pi i/7} = \cos 2\pi/7 + i \sin 2\pi/7$. Polinom $P(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$ je ireducibilan nad $\mathbb{Q}$ i poništava ζ_7. Slijedi da je $P(x)$ minimalni polinom od ζ_7, odnosno $[\mathbb{Q}(\zeta_7) : \mathbb{Q}] = 6$. Kako 6 nije potencija broja dva, ζ_7 nije konstruktibilan. $\square$

Zadatak 2. Dokažite da je polinom $x^6+x^5+x^4+x^3+x^2+x+1$ ireducibilan nad $\mathbb{Q}$. (Hint: koristite Eisensteinov kriterij.)

Literatura

[1] I. STEWART, *Galois Theory*, Fourth Edition, Chapman and Hall/CRC (2015)