U čemu je snaga suvremene algebre?

Dr Ivan Tomašić

Queen Mary, University of London

SŠ Mate Blažina Labin 2014

Pitagorine trojke

Teorem

Postoje cijeli brojevi x, y i z koji zadovoljavaju:

$$x^2 + y^2 = z^2.$$

Dokaz.

Dovoljno je pogoditi jedno rješenje:

$$x = 3, \quad y = 4, \quad z = 5.$$

□

Može se pokazati i više, postoji beskonačno mnogo cjelobrojnih rješenja te jednadžbe, takozvane Pitagorine trojke.

Veliki Fermatov Teorem

Teorem

Za bilo koju potenciju $n \geq 3$,
ne postoje cijeli brojevi x, y i z koji zadovoljavaju:

$$x^n + y^n = z^n.$$

To je Veliki Fermatov Teorem, koji je Fermat postavio kao veliku zagonetku oko 1650, a dokazao ga je tek Andrew Wiles 1995.

Primijetimo: čak i ako na računalu provjerimo da za dani n nema cjelobrojnih rješenja do

$$-10^{100} \leq x, y, z \leq 10^{100},$$

to nam nije od velike koristi za opću tvrdnju:

kako znamo da ne postoji neko još veće rješenje?

Algebarske jednadžbe: linearni slučaj

Riješimo linearnu algebarsku jednadžbu:

$$3x + 4 = 0.$$

Rješenje je $x = -4/3$.
Što znači riješiti jednadžbu?
Trebamo naći sve brojeve koji zadovoljavaju jednadžbu kad ih uvrstimo za x.
Upozorenje: Čekaj malo–ne bismo li trebali precizirati skup (ili brojevni sustav) u kojem tražimo rješenje?

Algebarske jednadžbe: linearni slučaj

Promotrimo linearnu algebarsku jednadžbu:

$$3x + 4 = 0.$$

Postoje li rješenja u skupu cijelih brojeva

$$\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, 4, \ldots\}?$$

NE!
Postoje li rješenja u skupu racionalnih brojeva (razlomaka)?

$$\mathbb{Q} = \left\{ \frac{p}{q} : p, q \in \mathbb{Z}, \quad q \neq 0 \right\}?$$

Pa naravno, $\frac{-4}{3} \in \mathbb{Q}$.

Algebarske jednadžbe: linearni slučaj

Promotrimo opću linearnu algebarsku jednadžbu u nepoznanici x:

$$ax + b = 0,$$

gdje su $a, b \in \mathbb{Q}$, $a \neq 0$.
Ova jednadžba se može riješiti u $\mathbb{Q}$ i opće rješenje je

$$x = -b/a.$$

Da li se ovaj fenomen javlja samo u $\mathbb{Q}$? Koja svojstva zbrajanja i množenja u $\mathbb{Q}$ moramo iskoristiti da bi riješili linearnu jednadžbu?

Prvi susret s poljima brojeva

Koristimo jedino činjenicu da u $\mathbb{Q}$ možemo:

- zbrajati,
- oduzimati,
- množiti,
- dijeliti (s brojem različitim od 0),
- i, povrh toga, sve te operacije zadovoljavaju uobičajena pravila.

Algebarska struktura $(F, +, \cdot)$ u kojoj operacije $+$ i $\cdot$ zadovoljavaju ista svojstva se zove polje.
Linearne jednadžbe se mogu riješiti u bilo kojem polju F.

Primjeri polja

Zašto $\mathbb{Z}$ nije polje?
Naravno da u $\mathbb{Z}$ možemo zbrajati, oduzimati i množiti, ali ne možemo proizvoljno dijeliti.
Skup realnih brojeva $\mathbb{R}$ je polje. Imamo: $\mathbb{Q} \subseteq \mathbb{R}$.
Kasnije ćemo vidjeti više primjera.

Algebarske jednadžbe: kvadratni slučaj

Riješimo kvadratnu jednadžbu

$$x^2 - x - 6 = 0.$$

Povijesno, neke kvadratne jednadžbe su znali riješiti već i Babilonci, antički Grci, Indijci, a njihova rješenja su bila proceduralna, kroz recepte i naputke. Riješimo gornju jednadžbu nadopunjavanjem do punog kvadrata.

$$0 = x^2 - x - 6 = x^2 - 2 \cdot \frac{1}{2} x + \left(\frac{1}{2}\right)^2 - \left(\frac{1}{2}\right)^2 - 6 = \left(x - \frac{1}{2}\right)^2 - \frac{1 + 24}{4}.$$

Dakle, $\left(x - \frac{1}{2}\right)^2 = \frac{25}{4} = \left(\frac{5}{2}\right)^2$.
Imati ćemo dva rješenja, nazovimo ih x_1 i x_2, prvo u slučaju $x_1 - \frac{1}{2} = \frac{5}{2}$, a drugo za $x_2 - \frac{1}{2} = -\frac{5}{2}$. Prema tome, $x_1 = 3$ a $x_2 = -2$.

Algebarske jednadžbe: kvadratni slučaj

Prava je gnjavaža ponavljati ovaj recept svaki put kad želimo riješiti kvadratnu jednadžbu. Zar ne možemo naći formulu za rješenje opće kvadratne jednadžbe

$$ax^2 + bx + c = 0, \qquad a \neq 0?$$

Naravno da možemo, već je i vrapci na grani pjevaju:

$$x_{1,2} = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

Al-Khwarizmi

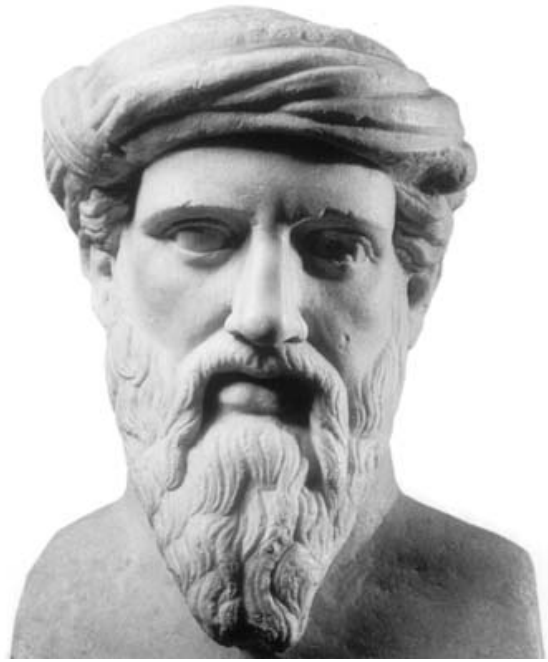
Prvi čovjek koji je zapisao nešto poput gornje formule bio je Muhammad ibn Musa al-Khwarizmi (c. 780–c. 850).

Riječ “algebra” se pojavljuje u naslovu njegove knjige *Hisab al-jabr w’al-muqabala*. Riječ *al-jabr* doslovno znači ‘balansiranje’, pri čemu se misli na prebacivanje negativne veličine na drugu stranu jednadžbe.
Iz imena Al-Khwarizmi je izvedena i riječ “algoritam”.

Kvadratne jednadžbe: razni problemi s brojevnim sustavima

Promotrimo jednadžbu

$$x^2 = 2.$$



Ima li rješenja u $\mathbb{Q}$?
Nema! Pitagora je dokazao da $\sqrt{2}$ nije racionalan broj.
Naravno, jednadžba se može riješiti u $\mathbb{R}$.
Rješenja su

$$x_{1,2} = \pm\sqrt{2}.$$

Kvadratne jednadžbe: razni problemi s brojevnim sustavima

Malo teže pitanje: promotrimo jednadžbu

$$x^2 = -1.$$

Ima li rješenja u $\mathbb{R}$?
Nema! Za svaki $x \in \mathbb{R}$, znamo da je $x^2 \geq 0$.
Što možemo učiniti?
Moramo proširiti realne brojeve dodavanjem imaginarne jedinice i koja zadovoljava $i^2 = -1$ i na taj način dobijemo kompleksne brojeve:

$$\mathbb{C} = \{a + bi : a, b \in \mathbb{R}\},$$

zajedno s operacijama:

$$\begin{aligned} (a+bi)+(c+di) &= (a+b)+(c+d)i \\ (a+bi)(c+di) &= (ac-bd)+(ad+bc)i. \end{aligned}$$

Rješenja gornje jednadžbe su:

$$x_{1,2} = \pm i.$$

Kompleksni brojevi kao polje

Kako dijelimo u $\mathbb{C}$? Ako $z = a + bi \neq 0$, dijeljenje sa z je u biti množenje sa

$$z^{-1} = \frac{a - bi}{a^2 + b^2}.$$

Provjerite da je $z \cdot z^{-1} = 1$!
$\mathbb{C}$ je polje i imamo

$$\mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}.$$

Rješavanje kvadratnih jednadžbi nad $\mathbb{C}$

Za bilo koje $a, b, c \in \mathbb{C}$, $a \neq 0$, jednadžba

$$ax^2 + bx + c = 0$$

se može riješiti u $\mathbb{C}$ formulom

$$x_{1,2} = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

$\mathbb{C}$ je algebarski zatvoreno polje

Nešto nevjerojatno se dogodi prelaskom na $\mathbb{C}$. To je algebarski zatvoreno polje u smislu da svaka algebarska (polinomijalna) jednadžba

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_2 x^2 + a_1 x + a_0 = 0,$$

za $a_n, a_{n-1}, \ldots, a_2, a_1, a_0 \in \mathbb{C}$, $a_n \neq 0$ ima rješenje u $\mathbb{C}$.
Štoviše, ako brojimo rješenja s točnim kratnostima, postoji točno n rješenja.
Ova tvrdnja se zove Osnovni Teorem Algebre.

Rješavanje algebarskih jednadžbi nad $\mathbb{C}$ općom formulom

Iako Osnovni Teorem Algebre garantira da svaka algebarska jednadžba stupnja $n > 0$ ima rješenje u $\mathbb{C}$, to ne znači da postoji eksplicitna opća formula koja rješava te jednadžbe u radikalima.
Osim $n = 2$ (za kvadratne jednadžbe smo dali formulu), postoje opće formule za $n = 3$ te $n = 4$,
ali može se dokazati za za $n \geq 5$ ne postoji opća formula–još ćemo se vratiti na ovu temu.

Kvadratna proširenja polja

Neka je F polje i $d \in F$ proizvoljni element (ako vam se čini lakše, razmišljajte o konkretnom primjeru kao $F = \mathbb{Q}$ ili $F = \mathbb{R}$). Kvadratno proširenje od F dobiveno dodavanjem $\sqrt{d}$ definiramo na sljedeći način. Kao skup,

$$F(\sqrt{d}) = \{a + b\sqrt{d} : a, b \in F\}.$$

Operacije se definiraju ovako:

$$\begin{aligned} (a + b\sqrt{d}) + (a' + b'\sqrt{d}) &= (a + a') + (b + b')\sqrt{d} \\ (a + b\sqrt{d})(a' + b'\sqrt{d}) &= (aa' + bb'd) + (ab' + ba')\sqrt{d}. \end{aligned}$$

Primijetimo da je uz te definicije $\mathbb{C}$ isto što i $\mathbb{R}(\sqrt{-1})$. To je poseban slučaj konstrukcije za $F = \mathbb{R}$ te $d = -1$.

Primjer kvadratnog proširenja polja

Izračunajmo sljedeće u $\mathbb{Q}(\sqrt{-5})$:

$$(1+\sqrt{-5})(1-\sqrt{-5}) = 1-\sqrt{-5}+\sqrt{-5}-(-5) = 6 = 2\cdot 3.$$

Za učenike koje zanima više: to pokazuje da u prstenu $\mathbb{Z}[\sqrt{-5}]$ nemamo jedinstveni rastav na proste faktore.

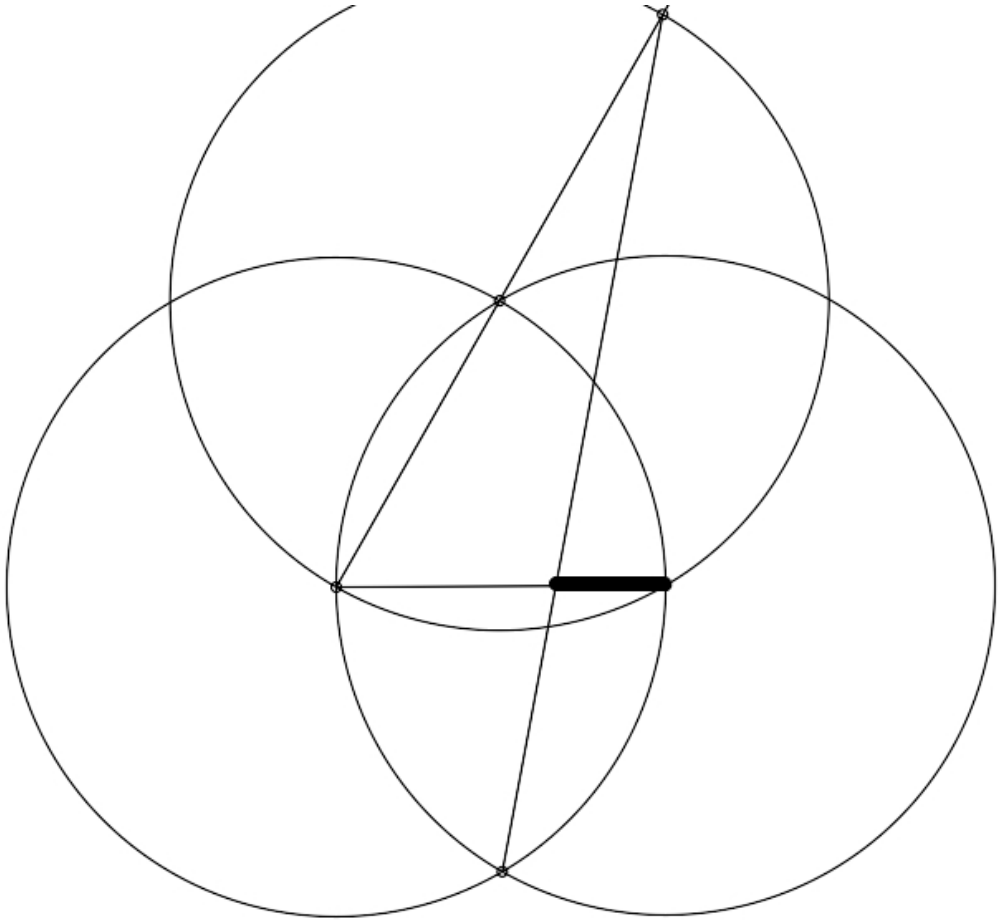
Grčka geometrija

Koristeći algebru koju smo upravo naučili, pokazati ćemo spektakularno razrješenje problema koji su za staro-grčke geometre ostali nerazjašnjeni misterij.
Od svih grana matematike, Grci su se najviše zanimali za geometriju. Najviše postignuće njihove matem-atike je Euklidova aksiomatska iz-gradnja geometrije u ravnini u nje-govom slavnim djelu Elementi.

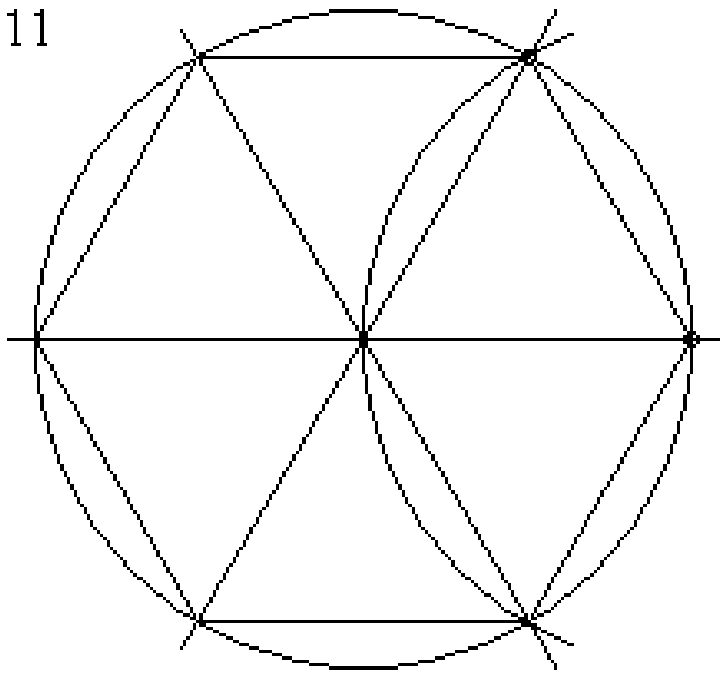
Konstrukcije ravnalom i šestarom

Jedan od glavnih ciljeva Grčke matematike je bio otkriti koji se geometrijski likovi mogu konstruirati isključivo ravnalom i šestarom.

Primjer: dioba dužine na tri jednaka dijela



Primjer: konstrukcija pravilnog šesterokuta



Neriješeni problemi antike

Grci nikako nisu mogli naći konstrukcije za tri problema:

- Kvadratura kruga: nacrtati kvadrat iste površine kao i zadani krug.
- Duplikacija kocke: nacrtati kocku čiji je volumen dvostruko veći od volumena zadane kocke.
- Trisekcija kuta: podijeliti zadani kut na tri jednaka dijela.

Naravno, činjenica da oni nisu mogli naći te konstrukcije ne znači sama po sebi da su te konstrukcije nemoguće–Grci su bili potpuno zbunjeni!

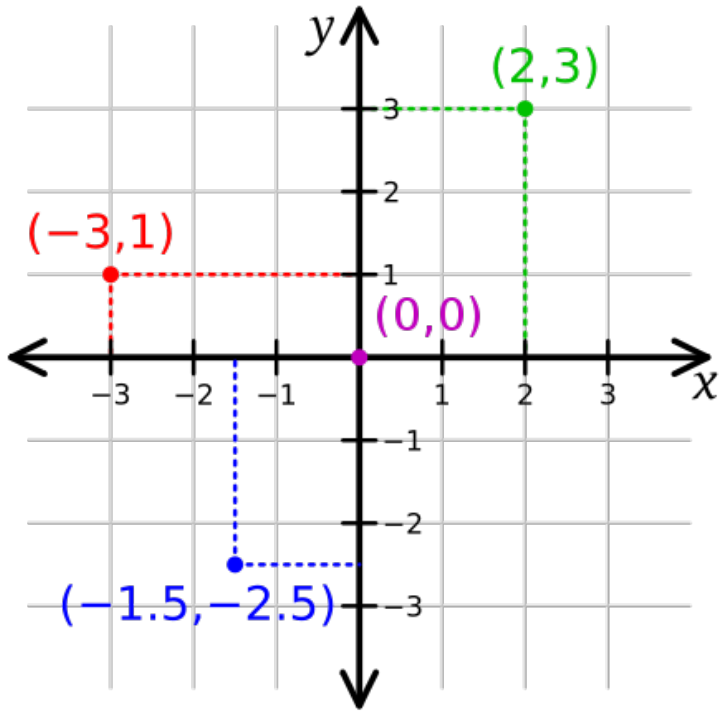
Razrješenje antičkih problema

Koristeći metode suvremene algebre, dokazati ćemo da se sve tri spomenute konstrukcije neizvedive. Naš će se dokaz temeljiti na sljedećim intelektualnim skokovima:

- Koordinatizacija.
- Prijevod problema u jezik teorije polja.
- Dokaz da su pridruženi problemi za polja nemogući.

Koordinatizacija

René Descartes je uveo koordinatni sustav u ravnini.



Koordinatno polje

Neka su zadane točke $P_1 = (x_1, y_1), \ldots, P_n = (x_n, y_n)$.
Koordinatno polje od $P_1, \ldots, P_n$ je polje $\mathbb{Q}(x_1, y_1, \ldots, x_n, y_n)$ koje se dobiva 'dodavanjem' svih koordinata danih točaka polju $\mathbb{Q}$.

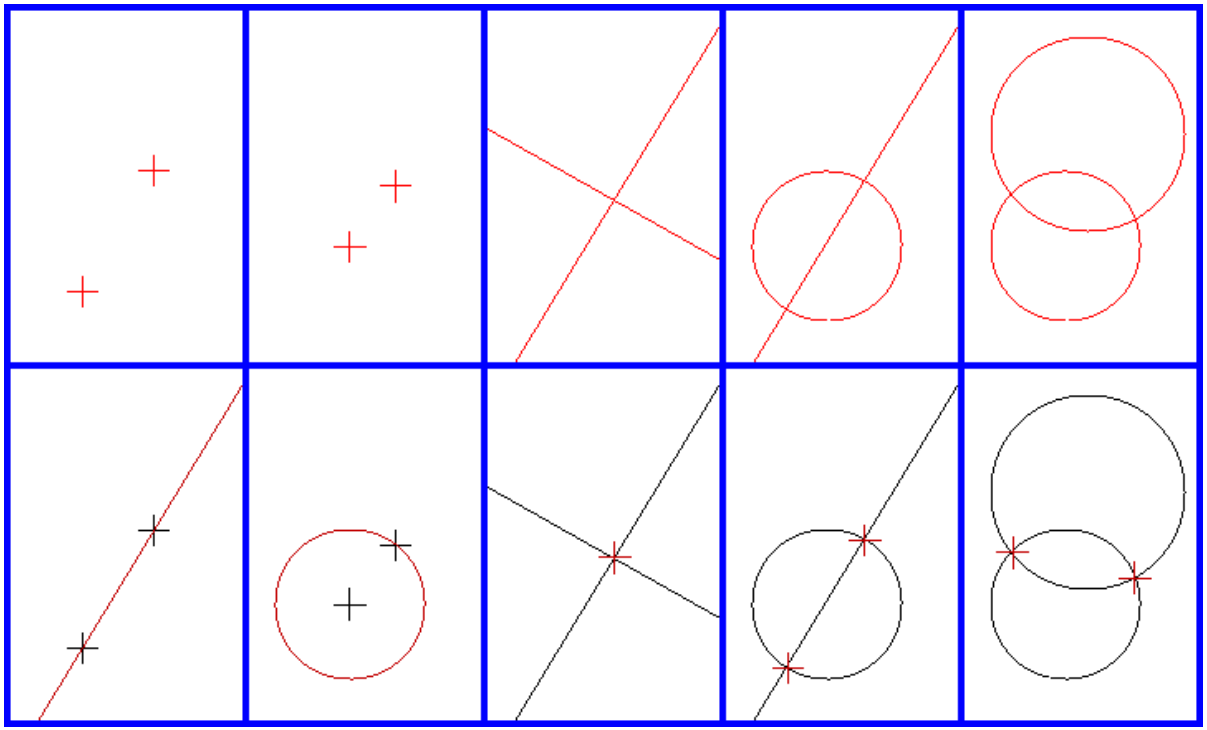
Teorem

Neka je F koordinatno polje točaka $P_1, \ldots, P_n$ i pretpostavimo da se točka P_{n+1} može konstruirati iz $P_1, \ldots, P_n$ koristeći neku od osnovnih konstrukcija ravnalom i šestarom.
Ako sa F' označimo koordinatno polje točaka $P_1, \ldots, P_n, P_{n+1}$, tada je F' kvadratno proširenje od F:

$$\text{postoji } d \in F \text{ takav da je } F' = F(\sqrt{d}).$$

Skica dokaza

Svaka konstrukcija ravnalom i šestarom se sastoji of pet osnovnih konstrukcija:



Bilo koji pravac kroz točke $P_1, \ldots, P_n$ ima jednadžbu oblika $ax + by + c = 0$ za neke $a, b, c \in F$, i bilo koja kružnica njima određena ima jednadžbu $x^2 + y^2 + ex + fy + g = 0$, za neke $e, f, g \in F$. Bilo koja točka P_{n+1} presjeka tih objekata ima koordinate koje su rješenja kvadratne jednadžbe nad F, a takva rješenja se nalaze u nekom kvadratnom proširenju of F.

Kvadratura kruga je nemoguća

Kad bi kvadratura kruga bila moguća, onda bi mogli konstruirati kvadrat iste površine kao i krug radijusa 1, a to je $1^2\pi = \pi$.
Dakle, bilo bi moguće konstruirati kvadrat stranice $\sqrt{\pi}$, što bi značilo da se $\sqrt{\pi}$ može dobiti slijedom kvadratnih proširenja od $\mathbb{Q}$.
Međutim, Lindemann ja 1882 dokazao da je π transcendentalan, što znači da uopće nije rješenje bilo koje algebarske jednadžbe nad $\mathbb{Q}$ pa je gore navedeno apsolutno nemoguće.

Duplikacija kocke je nemoguća

Prema našem Teoremu, svaki konstruktibilni omjer se može dobiti slijedom kvadratnih proširenja od $\mathbb{Q}$, pa mu je stupanj nad $\mathbb{Q}$ potencija od 2.
Da bi konstruirali kocku volumena 2, morali bi konstruirati omjer $\sqrt[3]{2}$, što je korijen ireducibilnog polinoma

$$x^3 - 2.$$

To znači da je x stupnja 3, što nije potencija broja 2, tako da je konstrukcija nemoguća.

Trisekcija općeg kuta je nemoguća

Prema Teoremu, svaki konstruktibilni omjer se može dobiti slijedom kvadratnih proširenja od $\mathbb{Q}$ pa mu je stupanj nad $\mathbb{Q}$ potencija od 2.
Da bi podijelili kut od 60° na tri jednaka dijela, morali bi moći konstruirati $x = \cos(20^\circ)$.
Poznata formula iz trigonometrije daje

$$\cos(3\alpha) = 4cos^3(\alpha) - 3\cos(\alpha),$$

pa vrijedi

$$4x^3 - 3x = \frac{1}{2}$$

i dobivamo da je x stupnja 3, što nije potencija od 2, pa je i ova konstrukcija nemoguća.

Galois-ova teorija

Metode teorije proširenja polja koje smo mi susreli su samo jedan sitni poseban slučaj opće teorije koju je razvio Évariste Galois.
Njegova teorija također pokazuje da ne postoji formula (u radikalima) za rješenje opće algebarske jednadžbe stupnja ≥ 5.

Suvremena algebra protiv klasične algebre

Što to dakle čini suvremenu algebru toliko moćnijom od klasične?

- Klasična algebra se bavi rješavanjem jednadžbi, često uz vrlo malo ‘kreativnog’ razmišljanja.
- Suvremena algebra proučava algebarske strukture i apstraktne algebarske pojmove.
- Grothendieck-ov princip: ‘Ne znam kako bih riješio ovaj konretan problem, idem probati riješiti puno općenitiji!’