МАТЕМАТИЧКА ГИМНАЗИЈА

МАТУРСКИ РАД

из АНАЛИЗЕ С АЛГЕБРОМ

Докази немогућности неких геометријских конструкција

Ментор: др Соња Чукић
Ученик: Урош Малеш, IVд

Београд, јун 2020

Садржај

1 Предговор

Изучавање геометрије и простора око себе, код човечанства датира још од Старих Грка и Римљана. Познате су нам од тада многе теореме из геометрије, као што су Питагорина или Талесова теорема, које и дан данас имају огромну примену у математици, физици, инжењерству, без којих се ове науке не би могле ни приближно развити, као што су се развиле до данас и што се и даље развијају.

Међутим, поред великих доприноса данашњој науци, Стари Грци и Римљани су научницима задавали главобоље, питањима која су постављали (а која су била нерешена све до 19. века). Они у то време нису имали моћне математичке алате, те одређене проблеме нису могли да реше. Развитком математике (пројективне геометрије, теорије поља, група...), данас, решења тих проблема се комотно могу предавати на часу у каснијим разредима средње школе.

У овом раду бавићемо се конкретно проблемом **конструкција.** На располагању имамо лењир (који не може да мери дужину дужи) и шестар. Стари Грци су се бавили конструкцијама и решавали проблеме бисекције дужи, угла, конструкцијом троугла... Међутим, класа проблема конструкција које су они поставили остали су нерешени више од 2000 година. По мом мишљењу, лепота проблема које ћемо навести лежи у једноставности њихове формулације, која иза себе крије решење на које се чекало хиљадама година и које је захтевало увођење нових, наизглед неповезаних, грана математике.

У овом раду, доказаћемо да су следеће геометријске конфигурације неконструктибилне:

- Трисекција угла с лењиром и шестаром
- Дуплирање запремине коцке. Ако нам је дата ивица једне коцке, конструисати ивицу коцке 2 пута веће запремине од почетне коцке.
- Нормала из дате тачке на дату праву, користећи само лењир

Прво ћемо доказати прва два тврђења заједно, а затим и последње, одвојено. За прва два, биће нам потребне дефиниције поља (и операције унутар њега) а што се другог тиче биће нам потребан појам пројективне трансформације.

2 Дефиниције везане за поље

2.1 Основне дефиниције

Поље $(F, +, \cdot)$ је скуп F са операцијама $+, \cdot$ на њему, које испуњавају:

- Затвореност у односу на F: $\forall a, b \in F$ имамо $a + b \in F$ i $a \cdot b \in F$.
- Асоцијативност: $\forall a, b, c \in F$ имамо $(a + b) + c = a + (b + c)$ и $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.
- Комутативност: $\forall a, b \in F$ имамо $a + b = b + a$ и $a \cdot b = b \cdot a$.
- Постојање неутрала за $+$ и $\cdot$ (у ознаци 0 и 1, редом): $\forall a \in F$ имамо $a + 0 = a$ и $a \cdot 1 = a$.
- Инверз за $+$: $\forall a \in F$ постоји $-a \in F$ тако да $a + (-a) = 0$.
- Инверз за $\cdot$: $\forall a \in F$ постоји $a^{-1} \in F$ тако да $a \cdot a^{-1} = 1$.
- Дистрибутивност $\cdot$ према $+$: $\forall a, b, c \in F$ имамо $(a + b) \cdot c = a \cdot c + b \cdot c$.

Неки примери поља били би $(\mathbf{R}, +, \cdot), (\mathbf{C}, +, \cdot)$...
Сама дефиниција поља, нам не значи много. Као што смо код скупова дефинисали функције и бијекције, тако ћемо код поља исто дефинисати неку врсту бијекције, међутим овај пут генерализовану.

Дефинисаћемо **аутоморфизам.** Видећемо да, поред тога што је бијекција, он захтева и да се структура поља не мења. Видећемо сада у самој дефиницији шта то значи.

2.2 Аутоморфизам

Аутоморфизам поља $(F, +, \cdot)$ је бијекција $\sigma : F \to F$ таква да

$$\forall a, b \in F \quad \sigma(a + b) = \sigma(a) + \sigma(b) \quad \sigma(a \cdot b) = \sigma(a) \cdot \sigma(b).$$

Пример аутоморфизма би била операција конјугације на пољу $(\mathbf{C}, +, \cdot)$.

Сад ћемо увести појам **квадратног раширења** поља (напомињем, не улазим у мотивацију иза увођења ових појмова нити неку вишу сврху, већ их само напомињем јер су неопходни за доказ прва 2 задатка).

2.3 Квадратно раширење поља

Посматрајмо поље $(F, +, \cdot)$ и $F \subset R$. Кажемо да је поље $(L, +, \cdot)$ његово квадратно раширење ако су му сви елементи облика $a + b \cdot \sqrt{c}, \forall a, b \in F$ и фиксирано $c \geq 0$ из F. Пише се $L = F(\sqrt{c})$.

Напомена Веома је важно доказати да овако дефинисан скуп L заједно с операцијама $+, \cdot$ заиста чини поље. Међутим, доказ је тривијалан, било би потребно само проћи кроз основне дефиниције поља и проверити да ли важе за њега.

Сада ћемо дефинисати један од кључних појмова за наш доказ. Шта би се десило када бисмо посматрали квадратно раширење квадратног раширења неког поља? А затим квадратно раширење тог квадратног раширења? Добили бисмо **итеративно квадратно раширење.**

2.4 Итеративно квадратно раширење

Кажемо да је поље $(L, +, \cdot)$ итеративно квадратно раширење поља $(F, +, \cdot)$ ако постоји низ поља $F = L_0, L_1, ..., L_{k-1}, L_k = L$ тако да је L_i квадратно раширење од L_{i-1} за све $i = 1, ..., k$.

То су све дефиниције везане за поље које су нам потребне у доказу. Драги читаоци, ко би рекао да ће овако нешто наизглед алгебарски и насумично, заправо конкретно помоћи у проблему трисекције угла...

Међутим, управо следећи корак је да геометријски проблем пребацимо у језик алгебре, где смо много моћнији. Следи алгебризација нашег проблема.

3 Алгебризација проблема конструкције

Прва ствар коју ћемо урадити је формализација проблем конструкције. Одредићемо све кораке које можемо извршити у оквиру ње. Дакле:

Почевши од коначног скупа тачака P, скупа линија L и скупа кругова C можемо извршити следеће операције

- Можемо додати линију у скуп L која пролази кроз две тачке из P. (1)
- Можемо додати круг у скуп C чији је центар у тачки из скупа P и који садржи тачку из скупа P. (2)
- Можемо додати тачку у скуп P која је пресек два елемнта из скупа L или C или пак пресек елемената из C и L. (3)

Без умањења општости, сматраћемо да је почетна конфигурација $P = \{(0,0),(0,1)\}$ и да су L, C празни скупови (дакле, почињемо од две тачке).

Дакле, пребацујемо се у Декартов координатни систем и посматрамо шта се дешава са координатама тачака када су на њих примењене операције (1), (2) и (3).

Такође, посматрамо које бројеве можемо добити у координатама након примене ових операција и сходно томе, дефинишемо следеће.

За број α ћемо рећи да је **конструктибилан** ако можемо из почетне конфигурације, применом наведених операција, добити тачку $(\alpha, 0)$.

Сада ћемо извршити алгебарску класификацију конструктибилних бројева (тј. потпуно ћемо их описати).

Самим тим, следи нам прво од два кључна доказа теореме, јер смо овим тврђењем напустили геометрију и скроз се пребацили у алгебру.

Тврђење 1 *Број α је конструктибилан ако и само ако припада неком итеративном квадратном раширењу поља* $\mathbf{Q}$.

Доказ. Доказујемо оба смера независно. Докажимо прво да, ако је α конструктибилан, онда он припада итеративном квадратном раширењу поља $\mathbf{Q}$.
Испитајмо шта се дешава када применимо редом кораке 1,2,3.

Корак (1). Полазећи од две тачке (a,b) и (c,d) конструишемо линију чија је једначина

$$(d-b)(x-a)-(c-a)(y-b)=0,$$

тј

$$(d-b)x-(c-a)y-ad+bc=0.$$

Корак (2). Полазећи од две тачке (a,b) и (c,d) конструишемо круг са центром у првој тачки који садржи другу тачку. Једначина круга је

$$(x-a)^2+(y-b)^2=(c-a)^2+(d-b)^2.$$

Корак (3). Полазећи од праве $ax+by=c$ и круга $(x-p)^2+(y-q)^2=r^2$ тражимо њихов пресек. Слично и за пресек два круга или две праве. У ове калкулације нећемо улазити, јер су доста комликоване, међутим, битно је само схватити следећу суштину.

Пошто нас занимају конструктибилни бројеви, у ове једначине ћемо убацити да је $y = 0$. Свака једначина постаје једначина степена највише 2 по промењљивој x са коефицијентима из истог поља F као и почетне тачке. Одавде следи, по формули решења квадратне једначине, да x припада пољу $F(\sqrt{a})$ за неко a из F.

Међутим, због начина избора наше почетне конфигурације, одавде следи да x припада неком итеративном квадратном раширењу од поља $\mathbf{Q}$.

Дакле, доказали смо да, ако је α конструктибилан, онда он припада итеративном квадратном раширењу поља $\mathbf{Q}$. Сада ћемо доказити други смер, односно да ако α припада итеративном квадратном раширењу поља $\mathbf{Q}$ онда је он конструктибилан.

За ово је довољно показати да је скуп конструктибилних бројева затворен у односу на $+, \cdot$ и да је затворен у односу на кореновање (овако ћемо видети да, почев од почетне конфигурације, можемо покрити сва итеративна квадратна раширења од $\mathbf{Q}$, а претходан смер нам каже да ништа ван итеративних квадратних раширења $\mathbf{Q}$ не може бити конструктибилан број).

- Затвореност у односу на сабирање. Уколико имамо конструисане тачке $(a, 0)$ i $(b, 0)$ (без умањења општости, $a < b$) желимо да конструишемо $(a + b, 0)$.
  Посматрајмо два круга, први круг са центром у $(a, 0)$ који садржи b и исти такав круг са центром у $(b, 0)$ (који садржи $(a, 0)$). Ова два круга се секу у тачкама $(\frac{a+b}{2}, c)$ i $(\frac{a+b}{2}, -c)$, а пресек x осе са правом кроз ове две тачке нам даје тачку $(\frac{a+b}{2}, 0)$. Сада конструишемо круг са центром у тој тачки који садржи тачку $(0, 0)$ и други пресек са x осом нам даје тачку $(a + b, 0)$.

- Затвореност у односу на одузимање. Треба само од тачке $(a, 0)$ $(a \neq 0)$ конструисати тачку $(-a, 0)$, а онда даље вршимо сабирање. Ово постижемо тако што ту тачку добијамо као други пресек са x осом круга у центру $(0, 0)$ који пролази кроз $(a, 0)$.

- Затвореност у односу на множење. Посматрајмо тачке $(a, 0), (0, 1), (0, b)$ и из тачке $(0, b)$ уочимо паралелу правој која пролази кроз $(a, 0)$ и $(0, 1)$. Из Талесове теореме добија да ова парелела сече x осу у тачки $(ab, 0)$.

- Затвореност у односу на дељење. Слично претходном, само што ћемо повући паралелу из тачке $(0, 1)$ паралелну са правом која пролази кроз $(a, 0)$ и $(0, b)$.

- Затвореност у односу на кореновање. Полазећи од тачке $(a, 0)$ $(a \geq 0)$ конструишемо тачке $(0, a)$ и $(0, \frac{a-1}{2})$. Тачке $(\sqrt{a}, 0)$ и $(-\sqrt{a}, 0)$ добијамо као пресек круга са центром у $(0, \frac{a-1}{2})$ који пролази кроз $(0, a)$ и x осе
  Q.E.D

Приметићемо сада да је проблем трисекције угла заправо еквивалентан томе да је број $\cos\frac{\pi}{9}$ конструктибилан, а проблем дуплирања коцке томе да је број $2^{\frac{1}{3}}$ конструктибилан.

Дакле, по претходном тврђењу, довољно је доказати да ова два броја нису ни у једном итеративном квадратном раширењу поља $\mathbf{Q}$. Ово је сада наш проблем.

4 Нуле полинома са коефицијентима у итеративном квадратном раширењу датог поља F

Очигледно, наш преформулисани проблем захтева дубљу анализу бројева у итеративном квадратном раширењу датог поља F.

Означимо са $L = F(\sqrt{c})$ за c из F.

Посматраћемо пресликавање σ поља L дефинисано као

$$\forall a, b \in F \ \sigma(a + b\sqrt{c}) = a - b\sqrt{c}$$

Очигледно важи

$$\sigma(\sigma(a + b\sqrt{c})) = a + b\sqrt{c}$$

и одавде следи да је σ бијекција на скупу L. Лако се проверава да σ задовољава и

$$\sigma(a + b) = \sigma(a) + \sigma(b), \sigma(a \cdot b) = \sigma(a) \cdot \sigma(b), \forall a, b \in L$$

те је σ аутоморфизам поља L такав да су му једине фиксне тачке елементи поља F. Овакво пресликавање зове се мапа конјугације.

Тврђење 2 *Нека је $\sigma : L \to L$ аутоморфизам и нека је $F \subset L$ поље чији су елементи фиксирани аутоморфизмом σ. Онда за сваки полином $P \in F[x]$ и свако $\alpha \in L$ важи*

$$P(\sigma(\alpha)) = \sigma(P(\alpha)).$$

Доказ. Приметимо да важи

$$\sigma(\sum a) = \sum \sigma(a)$$

и исто тако

$$\sigma(\prod a) = \prod \sigma(a)$$

па одавде добијамо

$$\sigma(P(\alpha)) = \sigma(a_n\alpha^n + ... + a_1\alpha + a_0) = \sigma(a_n\alpha^n) + ... + \sigma(a_1\alpha) + \sigma(a_0)$$

$$= a_n\sigma(\alpha)^n + ... + a_1\sigma(\alpha) + a_0 = P(\sigma(\alpha))$$

Q.E.D

Последица. Због $\sigma(0) = 0$ јер $0 \in F$ добијамо да, ако је $P(\alpha) = 0$, онда је и $P(\sigma(\alpha)) = 0$.

Сада нам следи и друго кључно тврђење у овом доказу (прво је било тврђење о класификацији конструктибилних бројева).

Тврђење 3 *Нека је $L = F(\sqrt{c})$ и нека је дат полином трећег степена $P \in F[x]$. Уколико P има корен у L онда има и корен у F.*

Доказ. Нека је, без умањења општости,

$$P(x) = x^3 + ax^2 + bx + c$$

за неке $a, b, c \in F$. Нека је σ мапа конјугације поља L и претпоставимо да је $P(\alpha) = 0$ и $\alpha \in L$ и $\alpha \notin F$. Онда је и $\beta = \sigma(\alpha)$ корен полинома P (по последици тврђења 2) који је различит од α (јер мапа конјугације фиксира елемент ако и само ако је из F).
Уколико $\beta \in F$ завршили смо, тако да претпоставимо да $\beta \notin F$.

Очито,

$$P(x) = (x - \alpha)(x - \beta)Q(x),$$

где је $Q(x)$ моничан тј.

$$Q(x) = x - \gamma.$$

Сада из Вијетових формула добијамо

$$\alpha + \beta + \gamma = -a,$$

тј.

$$\gamma = -a - \alpha - \beta.$$

Дакле $\gamma \in L$ и добијамо

$$\sigma(\gamma) = \sigma(-a - \alpha - \beta) = -a - \sigma(\alpha) - \sigma(\beta)$$

$$= -a - \alpha - \beta = \gamma.$$

Дакле, $\sigma(\gamma) = \gamma$ tj $\gamma \in F$. **Q.E.D**

Последица. Приметимо, одавде следи да ако полином трећег степена $P \in F[x]$ има корен у неком итеративном квадратном раширењу од F онда мора имати и корен у F.

Дакле, уколико полином $P \in Q[x]$ трећег степена има конструктибилан корен онда има и корен у $\mathbf{Q}$.

Другим речима, за сваки од бројева $2^{\frac{1}{3}}$ и $\cos\frac{\pi}{9}$ ћемо пронаћи одговарајући полином трећег степена чији су они корени, а који нема рационалних нула.

5 Проналажење одговарајућих полинома трећег степена

- Доказ за немогућност трисекције. Доказујемо да је $\alpha = \cos\frac{\pi}{9}$ није конструктибилан. Имамо

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

  Посматрајмо дакле полином

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

  Уколико је α конструктибилан онда P мора имати рационалну нулу (јер му је α нула), што није случај. Контрадикција, α није конструктибилан, дакле трисекцију је немогуће извршити.

- Докажимо да $2^{\frac{1}{3}}$ није конструктибилан. Уколико јесте, посматрајмо полином

  $$P(x) = x^3 - 2.$$

  Ако је $2^{\frac{1}{3}}$ конструктибилан онда овај полином мора имати рационалну нулу, што свакако није случај, контрадикција.

6 Закључак за овај начин доказивања

Дакле, иако ова метода решава одређени број конструкција, она није довољно добра да би решила све конструкције. На пример, једна од конструкција за коју не можемо доказати да је немогућа на овај начин је **квадратура круга.**

Зашто? Зато што је $\sqrt{\pi}$ трансцендентан број, тј. не можемо наћи полином трећег степена $P \in Q[x]$ чија је он нула, па не можемо применити овај метод.

У наредним поглављима, бавићемо се доказом немогућности конструкције нормале из дате тачке на дату праву, коришћењем само лењира (који не може да мери дужине дужи).

Као што смо у претходном проблему морали дефинисати поље, аутоморфизме, итеративна квадратна раширења, тако ћемо у следећем проблему морати прецизно да испитамо афине трансформације.

7 Афине трансформације

7.1 Дефиниција и два тврђења

Афине трансформације Еуклидске равни су оне трансформације које можемо представити на следећи начин:

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} x \\ y \end{pmatrix} \cdot \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} + \begin{pmatrix} b_1 \\ b_2 \end{pmatrix},$$

где је (x, y) почетна тачка, а (x', y') тачка у коју се она слика афином трансформацијом.

Имамо следећа тврђења:

- Афине трансформације сликају тачку у тачку (по дефиницији пресликавања). Притом, у питању је бијективно пресликавање (такође јасно из дефиниције).
- Афине трансформације чувају колинеарност тачака. Ако имамо 3 тачке $(x_1, y_1), (x_2, y_2), (x_3, y_3)$ које су колинеарне, онда су и њихове слике колинеарне. Ово се лако доказује проверавајући критеријум колинеарности 3 тачке тј. да важи

  $$\frac{y_1' - y_3'}{x_1' - x_3'} = \frac{y_2' - y_3'}{x_2' - x_3'}, x_1' \neq x_3', x_2' \neq x_3'$$

  (међутим приметимо да ако важи $x_1' = x_3'$ и $x_2' = x_3'$ тачке јесу колинеарне (као специјалан случај) у супротном не) и уколико већ важи овај услов за почетне три тачке.

7.2 Примери афиних трансформација

Неки примери, нама познатих афиних трансформација:

- Ротација за угао θ

  $$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} x \\ y \end{pmatrix} \cdot \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} + \begin{pmatrix} 0 \\ 0 \end{pmatrix}$$

- Транслација за вектор (b_1, b_2)

  $$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} x \\ y \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \begin{pmatrix} b_1 \\ b_2 \end{pmatrix}$$

- Осна рефлексија тачке око дате праве. Уколико права има смер вектора (l_x, l_y) пресликавање је

  $$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} x \\ y \end{pmatrix} \cdot \frac{1}{\sqrt{l_x^2 + l_y^2}} \begin{pmatrix} l_x^2 - l_y^2 & 2l_xl_y \\ 2l_xl_y & l_y^2 - l_x^2 \end{pmatrix} + \begin{pmatrix} 0 \\ 0 \end{pmatrix}$$

7.3 Примена на наш проблем

Операције које можемо извршити само са лењиром су следеће:

- Доцртавање произвољне тачке у равни.
- Цртање праве кроз 2 тачке одабране тачке.
- Доцртавање тачке пресека 2 одабране праве.

Претпоставимо да је конструкција могућа, тј да за дату тачку P и праву l могуће конструисати праву g која испуњава тражене услове.

Дакле, постоји функција f која као аргументе узима почетну тачку и праву и даје нам тражену праву и она се може описати као низ горе наведених потеза.

Кључна ствар за приметити је да су могуће операције инваријанте у односу на било коју афину трансформацију, па је и цела функција f, инваријанта у односу на афине трансформације.
Јасније речено, ако је π афина трансформација онда важи

$$f(\pi(P), \pi(l)) = \pi(f(P, l)).$$

Због дефиниције функције f имамо

$$f(\pi(P), \pi(l)) \perp \pi(l).$$

Комбинујући ово са горњом једнакошћу директно следи

$$\pi(f(P, l)) \perp \pi(l).$$

Овде би требало да се запитамо и да почнемо да назиремо контрадикцију...

Шта ако бисмо имали афину трансформацију која не чува прав угао између правих? Ако бисмо нашли такву афину трансформацију, онда узмемо да она буде наша трансформација π па директно следи контрадикција.

Посматрајмо афину трансформацију

$$\beta : (x, y) \mapsto (x, x + y)$$

и тачке $A(0, 0), B(1, 0), C(0, 1)$. Приметимо, слике тачака су $A'(0, 0), B'(1, 1), C'(0, 1)$.
Али важило је $BA \perp BC$, међутим не важи $B'A' \perp B'C'$ и сада можемо узети да је $\pi = \beta$ и долазимо до контрадикције.

Q.E.D

8 Закључак

Свако ко се икада бавио математиком чуо је за трисекцију угла, па и ја. Лично, привлачила ме је чињеница да постоји доказ да нешто **не можемо** конструисати, шта год покушали, па сам одлучио да свој матурски посветим тој теми. У првом делу рада је детаљно изнесен доказ те немогућности, користећи се алгебарским методама (другим, нпр. геометријским методама, није могуће доказати ово) и увођењем не толико познатог појма, итеративних квадратних раширења.

У другом делу рада, занесен идејом да можемо доказати да је нешто фундаментално немогуће да урадимо, одлучио сам да представим још један доказ немогућности конструкције, овај пут где је доказ више геометријске природе.

Желео бих да се пре свега захвалим свом ментору др Соњи Чукић, на веома детаљном и посвећеном прегледању мог рада и указивањем на многобројне, мени тешко уочљиве, грешке.

Такође, захвалио бих се и свим професорима Математичке гимназије који су ми предавали и додатно побудили моје интересовање за природне науке.

Литература

[1] Darij Grinberg *https://artofproblemsolving.com/community/c6h65245p386612*

[2] Wikipedia *https://en.wikipedia.org/wiki/Transformationmatrix*

[3] Wikipedia *https://en.wikipedia.org/wiki/Affinetransformation*

[4] Wojtek Wawrów *Impossibility of Geometric Constructions*