УНИВЕРЗИТЕТ У БЕОГРАДУ

МАТЕМАТИЧКИ ФАКУЛТЕТ

Конструкције лењиром и шестаром

и њихова веза са алгебром

мастер рад

Ментор: Кандидат:
Проф. др Александар Липковски Даријана Давидовић, 1067/2018

Београд, август 2020.

Садржај

I УВОД. О КОНСТРУКЦИЈИ

Геометријске конструкције су део геометрије у равни који планиметријске задатке решава конструктивном методом. Оне су врло погодно средство упознавања са облицима у равни и њиховим особинама. У настави математике оне више него неки други задаци доприносе остварењу циљева наставе математике и развојних особина ученика: довитљивост, самосталност, смисао за ред, прецизност и уредност, оригиналност, систематичност, логичко и стваралачко мишљење; унапређују математичку писменост и концизност, развијају математичку интуицију и машту и др. Геометријске конструкције имају велики значај у техници јер, између осталог, нацртна геометрија у својој основи се базира на геометријским конструкцијама. Конструктивни задатак се састоји у томе да се конструише (нацрта) нека геометријска фигура одабраним допуштеним справама ако је дата нека друга фигура и извесни односи између дате и тражене фигуре. Било коју фигуру која задовољава у задатку постављене услове зовемо решењем задатка. Задатак може имати једно или више решења. Постоји велики број инструмената помоћу којих се могу изводити геометријске конструкције, а то су лењир, шестар, двострани лењир, лењир са подеоцима, угломер, кривуљар, елипсограф, конац и други. Кроз историју су многи математичари покушавали решити геометријске проблеме користећи само лењир и шестар. Ово ограничавање потиче од старогрчких математичара, нарочито за време Платонове Академије, и сматра се најелегантнијим решењем.

Објаснимо најпре на који начин нам је допуштено коришћење лењира и шестара. Помоћу лењира можемо конструисати праву која пролази кроз две задате тачке тј. може се повући довољно дугачак део праве која пролази кроз две тачке. Шестаром описујемо круг тако што поставимо врх једног крака шестара у прву задату тачку (тачку која треба бити центар круга) и врх другог крака шестара у другу задату или произвољну тачку. Иако из описа коришћења шестара не следи да је могуће описати нови круг истим отвором, у геометријским конструкцијама се подразумева да је могуће описати више кругова истог полупречника са различитим центрима (особина преношења дужи). С тим у вези, довољно је доказати да се може конструисати други круг чији је центар различит од центра првог круга, а полупречник једнак полупречнику првог круга помоћу шестара који није сачувао отвор дужине полупречника првог круга[1]. Такође, коришћење шестара као преносиоца дужи не даје различит скуп решивих конструкција у односу на скуп решивих конструкција до кога се долази без коришћења те особине.

Свака конструкција лењиром и шестаром се састоји од коначно много изведених *елементарних конструкција или операција*:

I Избор произвољне тачке унутар датог дела равни.

II Конструкција праве која пролази кроз две већ изабране тачке или конструисане тачке.

III Конструкција круга коме је изабран или конструисан центар и тачка на периферији.

IV Одређивање тачке пресека две већ конструисане праве или конструисане праве са конструисаним кругом или два конструисана круга.

За даље разумевање текста потребно је да читалац буде упознат са конструкцијама које се истичу по својој једноставности и назваћемо их *основним конструкцијама*.

[1] Конструкцију круга са новим центром можете пронаћи у књизи Правилни полигони др Ђуре Паунића на страни 13.

Оне се у настави уводе поступно, још од градива шестог разреда основне школе. Јасно је да се *сложенија конструкција,* користећи више геометријских чињеница у процесу анализе, разлаже на низ основних конструкција које се лако изводе. Подела на основне и сложене конструкције није прецизно одређена, али постоје ипак неке основне конструкције које се не могу заобићи и морају се поменути, као што су: *пренос дужи и пренос углова, конструкција симетрале и средишта дужи, конструкција симетрале угла и средишта лука, конструкција праве која пролази кроз дату тачку и која је паралелна са датом правом, конструкција нормале из дате тачке на дату праву, дељење дате дужи на једнаке делове и у датој размери, основне конструкције троугла и др.*

1.1. Геометријске конструкције са ограничењима

Није ретко да су математичари покушавали да сведу коришћење лењира и шестара на коришћење само шестара или само лењира. Примећено је да је шестар савршенији инструмент од лењира што значи да неке конструкције могу бити изведене само шестаром као нпр. поделити круг на шест једнаких делова, конструисати тачку симетричну датој тачки у односу на дату праву итд. Правилан шестоугао се може конструисати коришћењем само шестара, док нам лењир служи само како бисмо спојили темена тј. нацртали странице на крају. Поставило се питање: Да ли је могуће конструисати сваки правилан полигон само шестаром, или, пак само лењиром? Уопштено говорећи, под којим условима се геометријска конструкција која је изводљива шестаром и лењиром, може извести само шестаром или само лењиром? Математичари који су дали највећи допринос развоју геометријских конструкција са ограничним средствима јесу Георг Мор, Лоренцо Маскерони и Јаков Штајнер. Још 1672. године дански математичар Георг Мор (*Gorg Mohr,* 1640-1697) у својој књизи „Дански Еуклид“ је доказао да свака конструкција која може да се изведе лењиром и шестаром, може да се изведе само шестаром. У то време тај доказ није био примећен, а поред тога и књига се загубила, те је тек пронађена 1927. у једној антикварници у Копенхагену. Тек 1797. године у Италији математичар Лоренцо Маскерони (Lorenzo Mascheroni, 1750-1800) је поново показао исто што је овај пут било запажено. Такође, следећи сугестије француског математичара Понслеа (*Jean Victor Poncelet,* 1788-1867), Штајнер (*Jakob Steiner*, 1796-1863) је доказао 1833. године да било која конструкција изведена лењиром и шестаром може бити изведена самим лењиром, ако су дати један круг и његов центар. Јасно је да се непрекидна права не може конструисати само шестаром, па се у геометрији шестара сматра да је права конструисана ако су конструисане било које њене две тачке. С друге стране, у конструкцијама само лењиром сматрамо да је тражени круг конструисан ако је одређен центар и полупречник.

1.2. Етапе у решавању конструктивних задатака

Приликом израде конструктивног задатка јавља се низ питања на која треба одговорити како би задатак био решен у потпуности и коректно. Да ли смо нашли сва решења? Како избор датих елемената утиче на могућност решења или број решења? Како спровести конструкцију на најједноставнији начин?

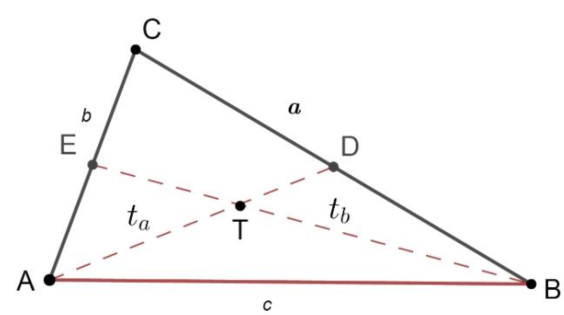
Имајући све то на уму, још за времена класичне Грчке, настала је шема која се састоји од четири узастопна корака:

1. анализа
2. конструкција
3. доказ
4. дискусија.

1. Анализа претходи самом извођењу конструкције те у овом кораку треба разложити задатак на низ елементарних конструкција или већ познатих задатака. Анализирамо тако што претпоставимо да је задатак већ решен и уочавамо зависности између датих и тражених објеката које би омогућиле решавање проблема. Од велике помоћи јесте и да се нацрта скица или цртеж датог и траженог, који се, уколико је потребно, допуни помоћним линијама, који нам служи као пројекат саме конструкције.
2. Конструкција се састоји у томе да се на основу анализе одреди извођење коначног броја елементарних конструкција и речима опише састављање тражене фигуре од датих елемената. Редослед одређивања појединих елемената произилази из низа зависности између њих, утврђених претходно анализом. За израду цртежа користе се искључиво лењир и шестар, осим ако није другачије договорено. Конструкцију можемо тумачити и као алгоритам у коме су улаз дати елементи задатка, а излаз решење задатка.
3. Доказ је корак у коме треба доказати да свака, конструкцијом добијена фигура, одговара свим условима задатка. За доказ је често потребно користити ставове обрнуте ставовима примењеним при вршењу анализе.
4. Дискусија утврђује услове егзистенције решења као и број решења. Обично се у конструкцији ограничава на конструкцију једног решења, при чему претпостављамо да су кораци конструкције сви могући. Међутим, да би се потпуно решио конструкивни задатак мора да се одговори на још нека питања:
а) За које величине и какав међусобни положај датих објеката је могуће конструисати тражену фигуру?
б) Колики је број решења у зависности од података?
При томе се подударна решења не сматрају за различита и кажемо да задатак има једно решење (до на подударност).
Јасно је да је могуће неке конструктивне задатке решавати и са нешто измењеном шемом. Дакле, није нужно да сваки конструктивни задатак садржи истакнуте кораке јер у једноставнијим конструкцијама неки од ових корака су тривијални и непосредно следе један из другог. У наставку текста дајемо пример решеног задатка.

<u>Пример 1.2.1.</u> Конструиши троугао ABC ако су задате страница AB, тежишне дужи t_a и t_b из темена A односно темена B троугла ABC.

Анализа. Замислимо да је задатак решен (сл. 1). Тежиште T је пресек задатих тежишних дужи t_a и t_b. На основу теореме:
Теорема 1.2.2. Тежишне дужи троугла се секу у тачки која дели сваку тежишну дуж у односу $1:2$.

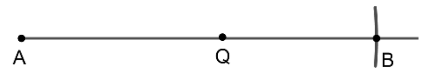


Сл. 1.

Можемо уочити троугао ABT чије су странице дуж AB (задата), $BT = \frac{2}{3}BE$ (дуж $BE = t_b$ је задата) и $AT = \frac{2}{3}AD$ (дуж $AD = t_a$ је задата). Одатле лако добијамо тачке E и D. Даље, продужавањем дужи AE и BD преко тачака E и D добијамо тачку C као тачку пресека продужетака.

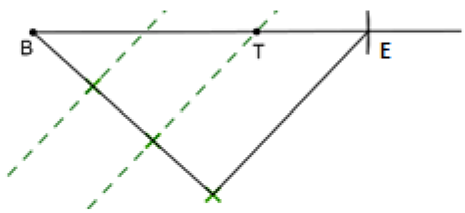
Конструкција.

1. Конструишемо дуж AB према датој величини (сл. 2), коришћењем основне конструкције *преношење дужи*: конструишемо тачку A, полуправу AQ, тачку $B = k(A, c) \cap AQ$.

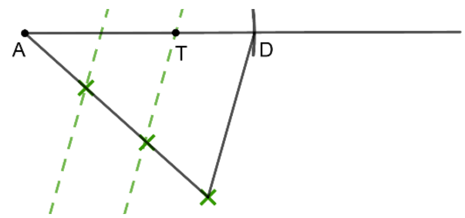


Сл. 2.

2. Конструишемо дуж BT дужине $BT = \frac{2}{3}BE$ (сл. 3).
3. Конструишемо дуж AT дужине $AT = \frac{2}{3}AD$ (сл. 4).

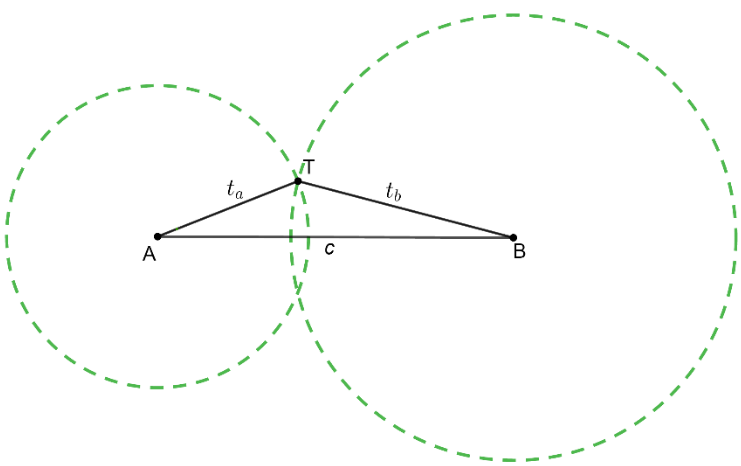


Сл. 3.



Сл. 4.

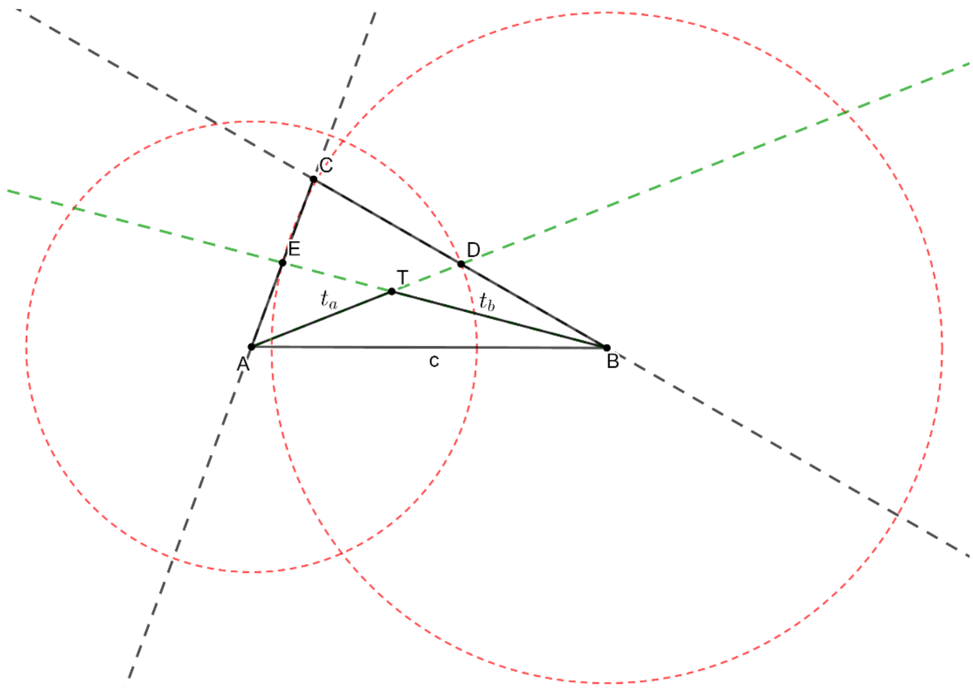
4. Конструишемо троугао ABT са страницама AB, BT и AT (сл. 5).



Сл. 5.

5. Страницу AT продужимо преко темена T и од A нанесемо задату дуж AD (сл. 6).
6. Страницу BT продужимо преко темена T и од B нанесемо задату дуж BE (сл. 6).

7. Конструишемо пресек права $p(A, E)$ и $p(B, D)$ и означимо га тачком C, што је теме траженог троугла ABC (сл. 6).



Сл. 6.

Доказ. Како је $TD : TA = -\frac{1}{2}$, а исто тако и $TE : TB = -\frac{1}{2}$ то су троуглови ABT и DET хомотетични са коефицијентом хомотетије $-\frac{1}{2}$. То даље значи да је $ED : AB = \frac{1}{2}$, па ED сече странице AC и BC у њиховим средиштима. То, даље, директно значи да су AD и BE тежишне дужи троугла ABC.

Дискусија. Сви су кораци у конструкцији увек изводљиви осим, можда, корака 4. Наиме, конструкција троугла је изводљива ако за те три странице важи неједнакост троугла која гласи:
Теорема 1.2.3. Свака страница троугла је мања од збира и већа од разлике друге две.

Стога, треба да важи

$$\frac{2}{3}(BE - AD) < AB < \frac{2}{3}(BE + AD),$$

односно

$$\frac{2}{3}(t_b - t_a) < AB < \frac{2}{3}(t_b + t_a).$$

Дакле, задатак има једно решење уз горњи услов, у противном нема решење.

II КОНСТРУКТИВНЕ МЕТОДЕ

2.1. О методама

Најистакнутије геометријске методе решавања конструктивних задатака јесу: *метода пресека (геометријских места тачака), метода помоћних фигура*, *методе геометријских трансформација (метода осне симетрије, метода ротације, метода централне симетрије, метода транслације, метода хомотетије, метода сличности)*. Ове методе се у настави могу непосредно примењивати јер за њих ученици уче теоријску основу. Примећујемо да су то већином методе геометријских трансформација. У геометрији кругова веома се често употребљава *метода инверзије* за коју је потребна посебна теоријска основа. У нацртној геометрији важну улогу имају *метода афиности* и *метода колинеације*.

Често се, из саме формулације задатка наслућује, која геометријска метода је најефикаснија, нпр:
- конструкција круга са задатим полупречником који додирује дату праву и дати круг (метода геометријских места тачака);

- конструкција петоугла коме су задата средишта страница (метода централне симетрије);

- конструкција квадрата коме су задати средиште и по једна тачка на суседним страницама (метода ротације);

- конструкција круга који додирује три задата круга (метода инверзије);

- конструкција круга који садржи дату тачку P и додирује две дате праве које нису паралелне (метода хомотетије).

Многи конструктивни задаци се могу решити на више начина, тј. користећи различите методе. Наравно, често се комбинују две или више метода при решавању једног задатка. Међутим, понекад се догоди да, ма колико се трудили и покушавали, не успевамо да решимо тражену конструкцију. У таквим случајевима уме да буде од помоћи тзв. *алгебарска метода*. О њој ће бити речи касније.

Кроз овај рад ћемо се боље упознати са горе наведеним метода и за сваку од њих илустроваћемо по један конструктивни задатак.

Основне елементе троугла ABC, ако није посебно назначено, обележаваћемо на доле написан начин. Исписане су само ознаке које одговарају темену A. За темена B и C ознаке су аналогне.

a – страница BC;
α – угао $\angle BAC$;
h_a – висина из темена A;
t_a– тежишна дуж из темена A;

2.2. Метода пресека (метода геометријских места тачака)

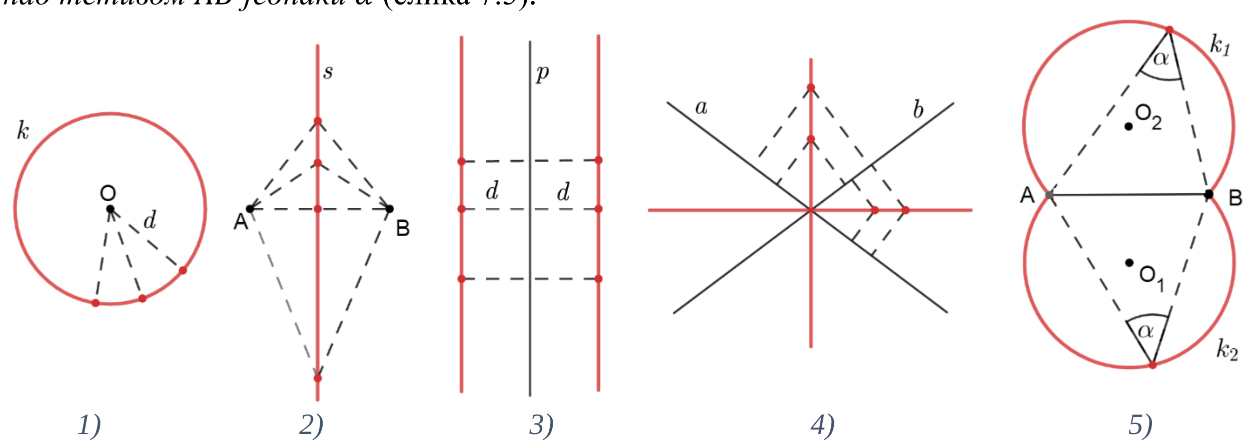
Већина геометријских конструкција које се изводе у основним и средњим школама се решавају помоћу методе пресека скупова тачака или, другачије речено, методе геометријских места тачака.

Дефиниција 2.2.1. ГМТ(α) - Геометријско место тачака равни је скуп свих тачака које задовољавају одређени услов α.

Ако је S наведено геометријско место тачака ГМТ(α), тада S задовољава следећа два услова:
1. Свака тачка у равни која задовољава услов α припада скупу S.
2. Свака тачка скупа S има особину α.
Основна идеја примене методе ГМТ је следећа. Ради се о конструкцији кључне тачке X која истовремено има особине α и β. Због тога X лежи у пресеку фигура $\Phi_1 =$ ГМТ(α) и $\Phi_2 =$ ГМТ(β).

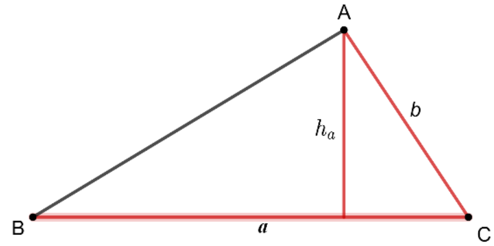
За коришћење ове методе неопходно је познавање основних геометријских места тачака, оних којих се најчешће срећу. То су:

I Геометријско место тачака чија су растојања од дате тачке O подударна датој дужи d је *круг са центром у тачки* O *полупречника* d (слика 7.1).
II Геометријско место тачака чија су растојања од датих тачака A и B подударна јесте *симетрала дужи* AB (слика 7.2).
III Геометријско место тачака чија су растојања од дате праве p подударна датој дужи d је *скуп од две праве паралелне са* p *на растојању* d *од ње* (слика 7.3).
IV Геометријско место тачака чија су растојања од две дате праве a и b подударна, при чему праве a и b нису паралелне, је *скуп од две узајамно нормалне праве одређене симетралама углова које образују праве* a *и* b (слика 7.4).
V Геометријско место тачака из којих се дата дуж AB види по датим углом α је *унија два кружна лука* $\widehat{AB}$ *осносиметрична у односу на праву* AB *такви да су периферијски углови над тетивом* AB *једнаки* α (слика 7.5).



Сл. 7.

Следи пример задатка у коме ћемо користити методу ГМТ:



Сл. 8.

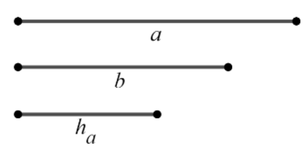
<u>Пример 2.2.2.</u> Конструиши троугао ABC коме су задате странице a и b висина h_a.

Анализа. Нека је ABC тражени троугао. Означимо дате елементе и испитајмо односе међу њима (сл. 8). Будући да је дата страница a, темена B и C можемо конструисати директно. Треће теме A мора задовољавати следећа два услова:

1. Због датог h_a, тачка A мора бити удаљена од праве BC за дужину h_a. Према томе, A припада ГМТ III, тј. скупу тачака чија су растојања од праве BC једнака h_a. То су две праве паралелне са BC свака на растојању h_a од BC.

2. Због датог b, тачка A мора бити удаљена од тачке C за дужину b. Следи да A припада ГМТ I, тј. кругу са центром C и полупречником b.

Дакле, теме A је у пресеку та два геометријска места тачака.



Конструкција.

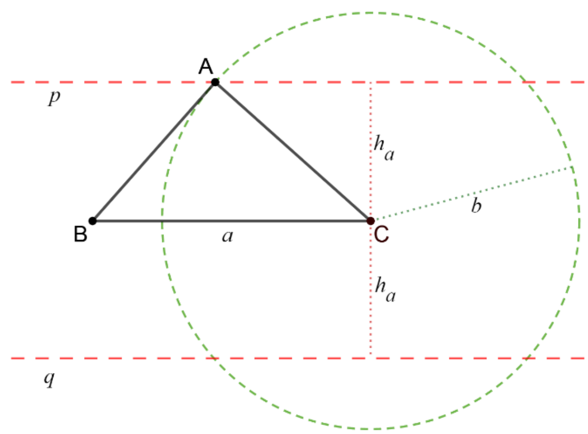
1. Конструишимо дуж BC подударној датој дужи a.

2. Конструишемо паралелне праве p и q као ГМТ чија су растојања од праве BC једнака h_a.

3. Конструишемо круг са центром у тачки C и полупречником b.

4. Означимо са A пресек правих p и q са кругом $k(C, b)$.

5. Троугао ABC је тражени (сл. 9).



Сл. 9

Доказ. Доказ следи из анализе и конструкције.

Дискусија. Очигледно, задатак има онолико решења колико има тачака A, а то је једнако броју тачака пресека правих p и q и круга $k(C, b)$. Случајеви су следећи:

(а) $h_a >$ b. Нема решења.

(б) $h_a =$ b. Две тачке пресека. Како су добијени троуглови подударни (осносиметрични), једно решење.

(в) $h_a <$ b. Четири тачке пресека и два решења.

2.3. Метода допунских фигура

Као што нам је већ познато, у анализи претпоставимо да је задатак решен, скицирамо тражену фигуру и обележимо познате елементе. Уколико је, на основу добијеног цртежа, тешко извести конструкцију, често је могуће скицу тражене фигуре допунити новим линијама (деловима правих и кругова). Тако се добија тзв. *допунска фигура*. Након конструкције допунске фигуре конструкција тражене фигуре може бити знатно поједностављена.

<u>Пример 2.3.1.</u> Конструисати правоугли троугао ABC ако су дати оштар угао α код темена A и збир катета a и b.

Анализа. Нека је ΔABC тражени троугао (сл. 10). Будући да збир катета $a+b$, идеја је да се добије фигура који садржи баш тај елеменат $a+b$. Продужићемо катету AC преко C за дуж $CD=a$. Сада добијамо ΔABD у коме је познато: страница $AD=a+b$, угао α код темена A и угао код темена D, $\angle D=45°$, јер је ΔCDB једнакокрако-правоугли. У овом задатку је коришћена допунска фигура ΔABD.

Конструкција.

1. Конструишимо дуж $AD=a+b$ (сл. 11).

2. Преносимо угао α на теме A, тј. $\angle DAL=\alpha$ (основна конструкција *преношење угла*).

3. Конструишемо угао од $\angle ADM=45°$.

4. Нека је $B=DM\cap AL$.

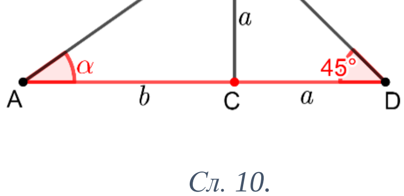
5. Конструишемо нормалу n из тачке B на праву AQ.

6. Нека је $C=AQ\cap n$.

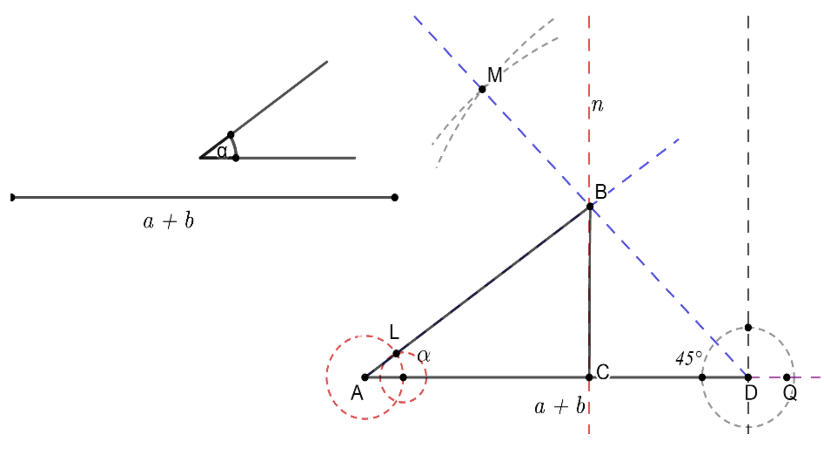
7. ΔABC (сл. 11).

Доказ: Доказ следи из анализе и конструкције

Дискусија: Задатак има увек јединствено решење.



Сл. 10.



Сл. 11.

2.4. Коришћење геометријских трансформација

Претпоставимо да је у конструктивном задатку кључна конструкција тачака A и B које су повезане неком геометријском трансформацијом f, тј. $B = f(A)$. Притом тачка A припада датој фигури F_1, а тачка B датој фигури F_2. Тада тачку B добијамо у пресеку фигура $f(F_1)$ и F_2.
Има више погодности ове методе. Рецимо, у доказу конструкције могу згодно користити особине трансформације f. Осим тога, најчешће је број решења једнак броју заједничких тачака фигура $f(F_1)$ и F_2.

2.4.1. Метода осне симетрије

За пар тачака A и A' кажемо да су *симетричне* у односу на осу s, ако је дуж AA' окомита на праву s и ако права s садржи средиште дужи AA'.

Дефиниција 2.4.1.1. Трансформацију у равни која пресликава сваку тачку равни A на њој симетричну тачку A' у односу на неку праву s, зовемо *осном симетријом* у односу на ту осу s.[2]

Следи решење задатка у којем илуструјемо примену методе осне симетрије.

Пример 2.4.1.2. Дати су кругови k_1 и k_2 и права s. Конструисати једнакостраничан троугао ABC тако да теме A припада кругу k_1, теме B кругу k_2, док висина из темена C припада правој s.

Анализа. Нека је ΔABC тражени троугао (сл. 12). Будући да је троугао ABC једнакостраничан, симетричан је у односу на праву s. Тачка A припада кругу k_1, па слика тачке A (тачка B) у датој осној рефлексији припада слици круга k_1 (кругу k_1'). Дакле, тачка B је пресечна тачка кругова k_2 и k_1'. Тачка C је пресечна тачка праве s и круга са центром у тачки B, полупречника AB.

Конструкција.

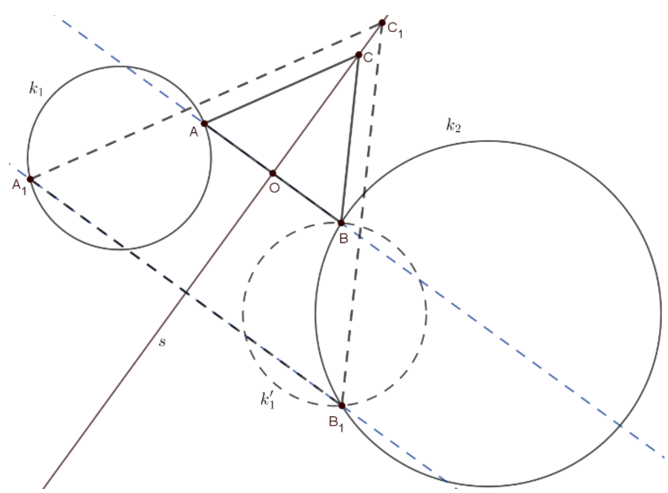
1. Конструишимо и означимо са k_1' круг симетричан кругу k_1 у односу на праву s.

2. Нека је B једна од пресечних тачака кругова k_2 и k_1'.

3. Са A означимо симетричну тачку тачки B у односу на праву s.

4. Нека је $C = k(B, AB) \cap s$.

5. ΔABC (сл. 12).



Сл. 12.

[2] Д. Палман, *Геометријске конструкције*, стр. 36.

Доказ. На основу конструкције и анализе тачка B припада кругу k_2, тачка A кругу k_1 и тачка C правој s. Тачка O припада правој s и представља средиште дужи AB. Дуж CO је тражена висина троугла ABC из темена C и припада правој s. Важи $BO = AO$ и $BA \perp s$, па су ΔAOC и ΔBOC правоугли и међусобно подударни, одакле следи $BC = AC$. Како је $AB = BC$, ΔABC је једнакостраничан.

Дискусија. Број решења зависи од броја заједничких тачака кругова k_2 и $k_1{}'$. Случајеви су следећи:

(а) Кругови k_2 и $k_1{}'$ се секу. За сваку пресечну тачку ових кругова тачка C може да се изабере на по два (симетрична) начина. Како су добијени троуглови подударни, два решења.

(б) Кругови k_2 и $k_1{}'$ се додирују. Задатак има једно решење

(в) Кругови k_2 и $k_1{}'$ су идентични. Задатак има бесконачно решења.

(г) Иначе нема решења.

2.4.2. Метода ротације и централне симетрије

Још једна геометријска транформација у равни која се може лепо употребити при решавању конструктивних задатака јесте метода ротације.

Дефиниција 2.4.2.1. Нека је дата тачка S и оријентисани угао α. Некој тачки равни A придружимо тачку A' тако да је $SA = SA'$ и $\angle ASA' = \alpha$. Такву бијективну трансформацију равни зовемо *ротацијом* равни око центра S за оријентисани угао α.[3]

Централна симетрија је врста ротације, тачније ротација за 180°. Зато је није потребно посебно описивати. Можемо је такође приказати и као комбинацију две узастопне осне симетрије којима су осе две међусобно окомите праве. Централна симетрија се издваја под посебним називом због својих својстава и једноставне и лако уочљиве примене.

Илуструјмо и разјаснимо примену ротације у следећем примеру.

Пример 2.4.2.2. Дате су праве b, c и тачка A. Конструисати једнакостранични троугао ABC тако да му је теме B на прави b, а теме C на прави c.

Анализа. Нека је ΔABC тражени троугао (сл. 13). С обзиром да је троугао једнакостраничан, угао код темена A износи 60°. Ротирањем праве b око тачке A за 60° добијамо слику праве b коју ћемо обележити са b'. Тачка C је пресек праве c и праве b'. Ротацијом тачке C у супротном смеру око тачке A добијамо тачку B која припада правој b.

Конструкција.

1. Конструишимо кроз тачку A праву нормалну на праву b и означимо је са са n.

2. Нека је $M = n \cap b$.

[3] Д. Палман, *Геометријске конструкције*, стр. 51.

3. Нека је M' тачка добијена ротацијом тачке M око тачке A за $60°$.

4. Конструишимо кроз тачку M' праву нормалну на крак AM' означимо је са b'.

5. Нека је $C = c \cap b'$.

6. Нека је B тачка добијена ротирањем тачке C око тачке A за $60°$, у супротном смеру.

7. Троугао ABC је тражени (сл. 13).

Доказ. На основу конструкције тачка C припада правој c, а тачка B правој b. Уочимо да се ротацијом око тачке A за угао од $60°$ тачка B пресликава у тачку C, док се ротацијом у супротном смјеру тачка C пресликава у тачку B. Важи $AB = AC$ и $\angle BAC = 60°$, одакле следи да је троугао ABC једнакокраки и да су углови на основици од $60°$. Дакле, троугао ABC је једнакостраничан.

Дискусија. Број решења зависи од положаја тачке A према правама b и c као и од величине угла који те две праве образују.

(а) $\{A\} = b \cap c$ и $\angle(b, c) \neq 60°$.

Задатак нема решења.

(б) $\{A\} \neq b \cap c$ и $\angle(b, c) = 60°$.

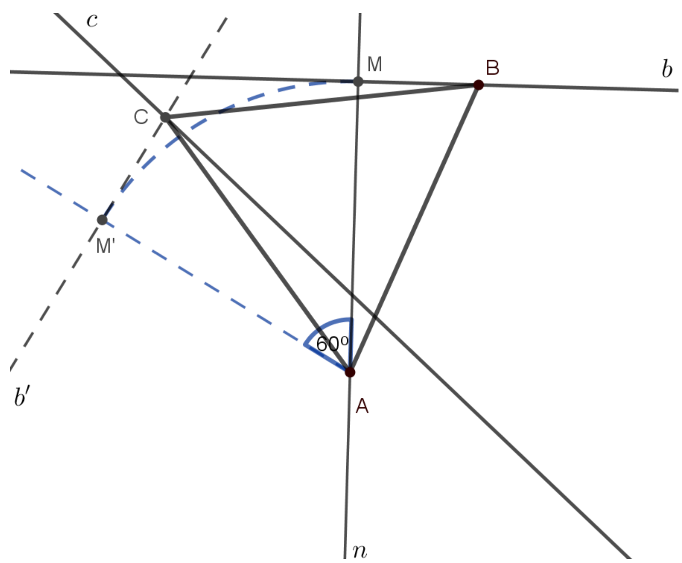
Задатак има једно решење

(в) $\{A\} \neq b \cap c$ и $\angle(b, c) \neq 60°$.

Задатак има два решења јер ротацију можемо изводити у два смера.

(г) $\{A\} = b \cap c$ и $\angle(b, c) = 60°$.

Задатак има бесконачно много решења.



Сл. 13.

2.4.3. Метода транслације

Дефиниција 2.4.3.1. Нека је у равни задата једна оријентисана дуж $\overrightarrow{AA'}$. Свакој тачки равни X придружимо тачку X' такву да дуж $\overrightarrow{XX'}$ има исту дужину као и дуж $\overrightarrow{AA'}$, те исти смер и оријентацију. Такву транформацију зовемо *транслацијом*.[4]

<u>Пример 2.4.3.2.</u> Дати су кругови k_1 и k_2 и права p. Конструисати праву паралелну са p која сече k_1 у тачкама A_1 и B_1, а k_2 у тачкама A_2 и B_2, тако да је збир дужи A_1B_1 и A_2B_2 подударан датој дужи d.

[4] Д. Палман, *Геометријске конструкције*, стр. 42.

Анализа. Нека је l тражена права (сл. 14). Обележимо са C_1 и C_2 подножја нормала из тачака O_1 и O_2 на праву l. Такође, C_1 и C_2 су средишта тетива A_1B_1 и A_2B_2, редом. Такође, праве O_1C_1 и O_2C_2 су нормалне p. Нека је круг $k_2{}'$ добијен транслацијом круга k_2 дуж праве l тако да се тачке A_2 и B_1 поклапају. Вектор транслације је $\overrightarrow{O_2O_2{}'}$ је дужине $O_2S - \frac{1}{2}d$ (S је подножје нормале из тачке O_2 на праву O_1C_1).

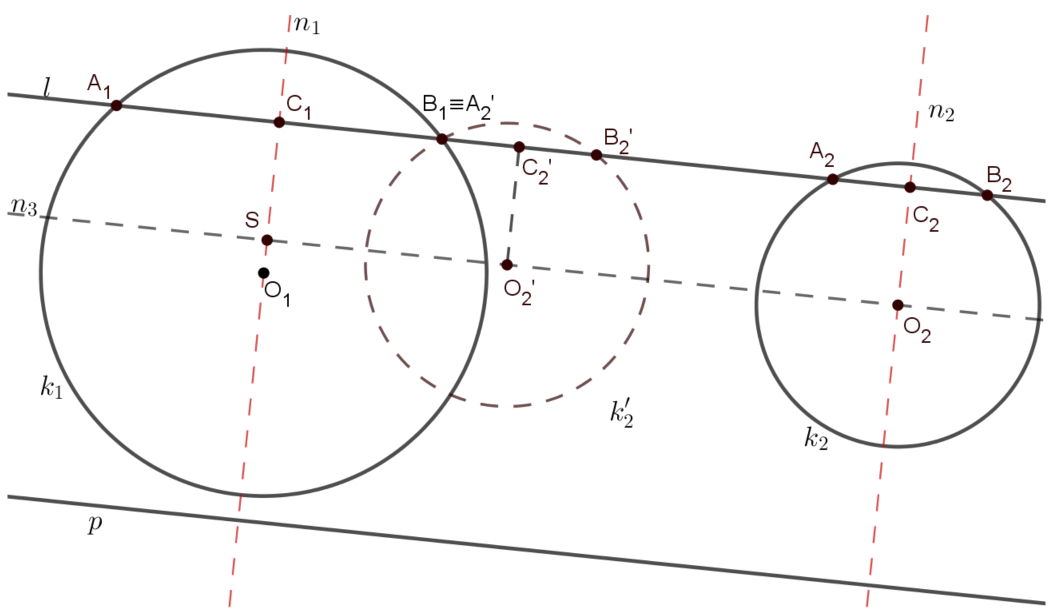
Конструкција.

1. Нека су n_1 и n_2 праве које су нормалне на праву p и пролазе кроз O_1 и O_2, редом.
2. Нека је n_3 права нормална на праву n_1 пролази кроз O_2.
3. Нека је $S = n_1 \cap n_3$.
4. Транслирајмо k_2 за вектор дужине $O_2S - \frac{1}{2}d$ у правцу p и добијени круг означимо са $k_2{}'$.
5. Нека је $B_1 = k_1 \cap k_2{}'$.
6. Означимо са l праву паралелну са p која пролази кроз B_1.

Доказ. Вектор $\overrightarrow{O_2O_2{}'}$ се може наћи јер је

$$O_2O_2' = O_2S - SO_2' = O_2S - \frac{1}{2}(A_1B_1 + A_2B_2) = O_2S - \frac{1}{2}d.$$

Дискусија. Постоји два, једно или ниједно решење у зависности од тога секу ли се кругови k_2 и $k_1{}'$ у две, једној или ниједној тачки.



Сл. 14.

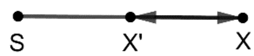
2.4.4. Метода сличности (метода хомотетије)

Дефиниција 2.4.4.1. Нека је S фиксна тачка равни. Било којој тачки X у равни (различитој од S) придружимо тачку X' која је колинеарна са X и са S и за коју вреди

$$\frac{\overrightarrow{SX'}}{\overrightarrow{SX}} = k \text{ (или } \overrightarrow{SX'} = \overrightarrow{SX} \cdot k \text{),}$$

где су $\overrightarrow{SX}$ и $\overrightarrow{SX'}$ оријентисане дужи, а k било који реалан број различит од 0. Такву трансформацију зовемо *хомотетијом*, тачку S зовемо *центром хомотетије*, а број k *коефицијентом хомотетије* (сл. 15, 16. и 17).[5]

Сл. 15. Хомотетија равни са центром у тачки S и коефицијентом $k = 3$.



Сл. 16. Хомотетија равни са центром у тачки S и коефицијентом $k = \frac{1}{2}$.

Сл. 17. Хомотетија равни са центром у тачки S и коефицијентом $k = -2$.

Сличност је таква трансформација тачака код које су свака два придружена сегмента у размери. Хомотетија је сличност за коју мора бити испуњено да су сваке две придружене тачке колинеарне са центром хомотетије.
Следи решење задатка добијено применом методе сличности.

<u>Пример 2.4.4.2.</u> Конструисати квадрат $ABCD$ ако дата дужина p, представља дужину удаљености средишта P странице CD квадрата $ABCD$ од темена A.

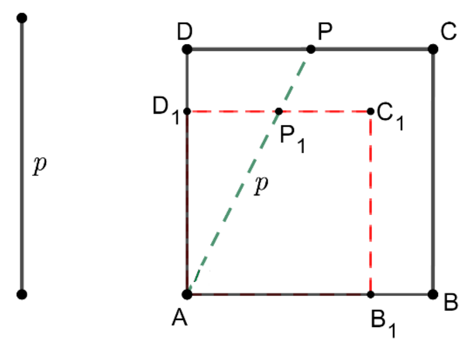
Анализа. Свака два квадрата су слична. Најпре се конструише било који квадрат, уочи удаљеност једног његовог темена од средишта једне наспрамне странице, а затим конструише квадрат коме је таква удаљеност тачно p.

Конструкција.

1. Конструишимо квадрат $AB_1C_1D_1$ произвољно.
2. Нека је P_1 средиште његове странице C_1D_1.
2. Конструишимо дуж AP на правој AP_1 дужине p.
3. Конструишимо квадрат $ABCD$ тако да је P средиште његове странице CD (сл. 18).

Доказ. Доказ је на основу анализе очигледан.

Дискусија. Задатак има увек јединствено решење.



Сл. 18.

[5] Д. Палман, *Геометријске конструкције*, стр. 63.

2.5. Алгебарска метода

Понекад се догоди да ниједном од наведених метода геометријског конструисања не можемо решити конструктиван задатак без обзира колико покушавали. У том случају покушаћемо применити *алгебарску методу решавања конструктивних задатака*.

Нека су у конструктивном задатку дате дужи дужине $a, b, c, \ldots, k$ и нека је за решење задатка потребно конструисати непознату дуж дужине x. Дужину x изразимо неким алгебарским изразом односно формулом помоћу датих величина

$$x = f(a, b, c, \ldots, k).$$

Како су дужине увек позитивне вредности, горњи израз f има смисла само ако поприма позитивне вредности.

Посматрајмо најпре неке једноставније конструкције алгебарских израза које ћемо назвати *основним изразима*. Ако је израз сложенијег облика (*сложени алгебарски израз*), потребно је трансформисати га у основне изразе.

2.8.1. Основни алгебарски изрази

1. $x = a + b$ (сабирање дужи дужина a и b).

Дуж дужине x добијамо ако на исту праву нанесемо дужину a и затим на њу надовежемо дужину b, тако да те две дужине имају само једну заједничку тачку (сл. 19).

2. $x = a - b, a > b$ (одузимање дужи дужина a и b).

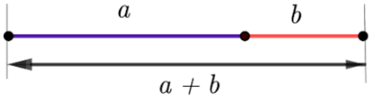
Дуж дужине x добијамо ако на исту праву нанесемо дужину a, затим и дужину b, али тако да им се једна крајња тачка поклапа и да постоје заједничке тачке датих дужина (сл. 20).

3. $x = n \cdot a, n \in \mathbb{N}$ (множење дужи дужине a природним бројем n)

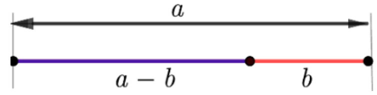
На основу сабирања дужи следи да дуж дужине x добијамо када n пута саберемо дуж дужине a (сл. 21).

4. $x = \frac{a}{n}, n \in \mathbb{N}$ (дељење дужи дужине a природним бројем n)

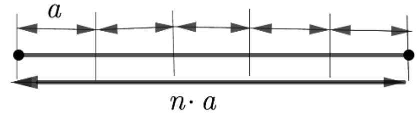
Нека је дата дуж OA дужине a. Конструишимо произвољно крак из O različит од OA и на њему нанесимо произвољну дужину b, n пута. Важи $OB = n \cdot b$. Кроз крајњу тачку B_1 конструишимо праву паралелну са AB која сече OA у тачки A_1. Важи $OA_1 = \frac{OA}{n}$ (сл. 22).



Сл. 19.



Сл. 20.



Сл. 21.

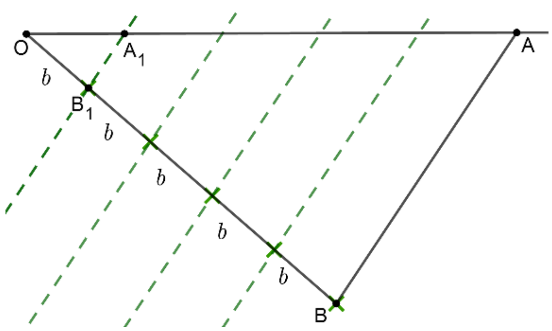
5. $\boldsymbol{x = \frac{n}{m} \cdot a,\quad n, m \in \mathbb{N}}$

Ова конструкција се изводи применом конструкције **4.** где поделимо a на m једнаких делова, а затим применом конструкције **3.** где се m-ти део повећа n пута.

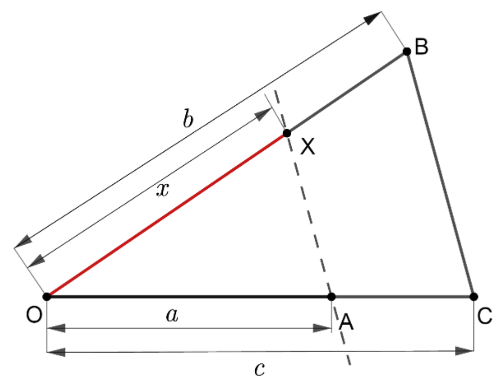
6. $\boldsymbol{x = \frac{ab}{c}}$ **,** $\boldsymbol{a, b, c \in \mathbb{N}}$ **(конструкција четврте пропорционале)**

На исту полуправу нанесемо дуж $OA = a$ и дуж $OC = c$. Конструишимо произвољно крак из O различит од OC и на њему нанесимо дуж $OB = b$. Конструишимо праву паралелну са BC која пролази кроз тачку A. Нека је X тачка пресека те праве и OB. OX је тражена дуж.

Доказ. Како је $\angle OCB = \angle OAX$ и $\angle OBC = \angle OXA$, следи да су троуглови OCB и OAX слични. Због сличности је $OX : OB = OA : OC$, односно $x : b = a : c$. Добијамо $x = \frac{ab}{c}$ (сл. 23).



Сл. 22.



Сл. 23.

7. $\boldsymbol{x = \sqrt{ab}}$ **,** $\boldsymbol{a, b \in \mathbb{N}}$ **(геометријска средина дужи дужина** $\boldsymbol{a}$ **и** $\boldsymbol{b}$**)**

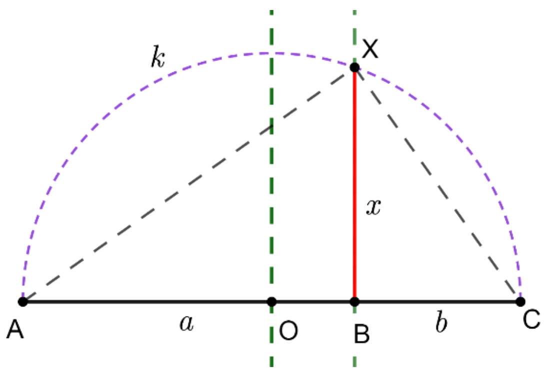
По конструкцији **1.** конструишимо дуж AC као збир дужи $AB = a$ и дуж $BC = b$. Нека је O средиште дужи AC. Конструишимо круг са центром у тачки O полупречника $OC = \frac{a+b}{2}$. Нека је тачка X пресек круга k и праве нормалне на AC која пролази кроз тачку B. Дуж BX је тражена дуж дужине x.

Доказ. Према теореми о односу централног и периферијског угла над истим кружним луком[6] следи да је $\angle AXC$ прав угао. Троуглови ABX и ACX су слични јер су им углови једнаки. Такође, троуглови CXB и ACX су слични. Применом транзитивности релације „бити сличан“, следи да је троугао ABX сличан троуглу CXB. Одатле произилази да су одговарајуће странице пропорционалне, па је $AB : BX = BX : BC$, тј. $a : x = x : b$. Важи $x = \sqrt{ab}$ (сл. 24).

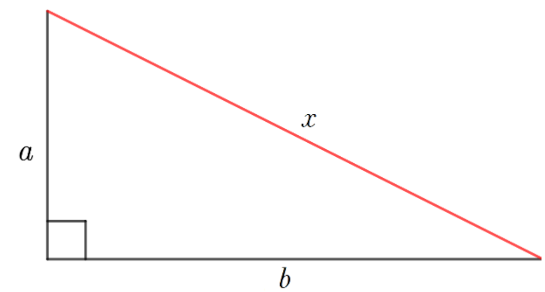
8. $\boldsymbol{x = \sqrt{a^2 + b^2},\ (x = \sqrt{a^2 - b^2}),\ a, b \in \mathbb{N}}$

[6] Централни угао је два пута већи од периферијског угла над истим кружним луком.

Према Питагориној теореми, очито је да је x дужина хипотенузе правоуглог троугла чије су катете дужине a и b, (x је дужина једне катете правоуглог троугла чија је дужина хипотенузе a, а дужина друге катете је b) (сл. 25).



Сл. 24 .



Сл. 25 .

Намаће се питање, да ли се сваки алгебарски израз може конструисати? Мада прерано (а даље у раду и оправдано) ћемо изнети следећу теорему:
Теорема 2.8.1.1. Сваки онај израз који добијамо из датих дужи коначним бројем рационалних операција и налажењем квадратног корена може се конструисати.

2.8.2. Сложени алгебарски изрази

Сада кад знамо да конструишемо једноставније изразе, можемо конструисати и много сложеније изразе тако што их раставимо у низ једноставнијих конструкција које смо управо описали. У вези с тим, урадићемо следећи пример.

<u>Пример 2.8.2.1</u>. Конструисати дужину дужи x ако вреди $x = a \cdot \sqrt{n}$, $n \in \mathbb{N}$.

Конструкцију ћемо решити на три начина.

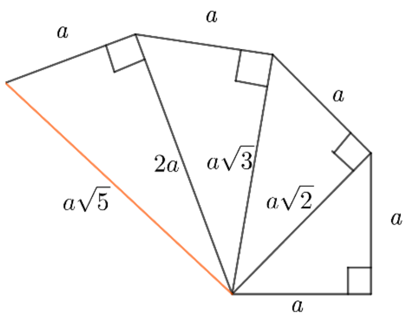
1. Дати израз можемо записати као $x = \sqrt{n \cdot a^2}$. Применом $n-1$ конструкција **8.** на изразе

$$x_1 = \sqrt{a^2 + a^2},\ x_2 = \sqrt{{x_1}^2 + a^2}, \dots, x_{n-1} = \sqrt{{x_{n-2}}^2 + a^2},$$

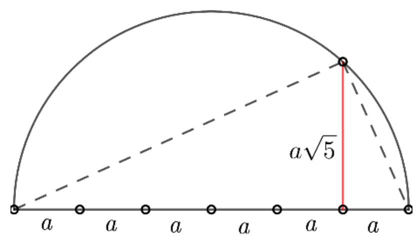
добијамо тражену конструкцију (сл. 26. за $n = 5$).

2. Ако је $n = p \cdot q$, где су p и q природни бројеви, онда дати израз можемо написати у облику $x = \sqrt{(pa) \cdot (qa)}$. Сада изразе $x_1 = pa$ и $x_2 = qa$ конструишемо конструкцијом **3.** Дати израз можемо записати помоћу $x = \sqrt{x_1 \cdot x_2}$ и конструисати га применом конструкције геометријске средине бројева x_1 и x_2 (сл. 27. за $n = 5$).

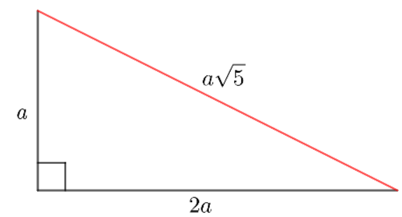
3. Ако је $n = p^2 + q^2$, где су p и q природни бројеви, дати израз можемо записати у облику $x = \sqrt{(pa)^2 + (qa)^2}$, што се своди на конструкције **3**. и **8**. (сл. 28. за $n = 5$).



Сл. 26.



Сл. 27.



Сл. 28.

2.8.3. Примена алгебарске методе у конструктивном задатку

<u>Пример 2.8.3.1.</u> Дат је троугао ABC. Конструисати кругове тако да се свака два додирују и да су центри кругова темена датог троугла.

Анализа. Претпоставимо да је задатак решен (сл. 29). Са a, b и c обележимо дужине страница троугла, а са x, y и z полупречнике тражених кругова. Са слике се одмах види да вреди $x + y = c$, $y + z = a$ и $z + x = b$. Решавањем овог система од три линеарне једначине са три непознате добијамо

$$x = \frac{c+b-a}{2}, \ y = \frac{a+c-b}{2} \ \text{и} \ z = \frac{b+a-c}{2}.$$

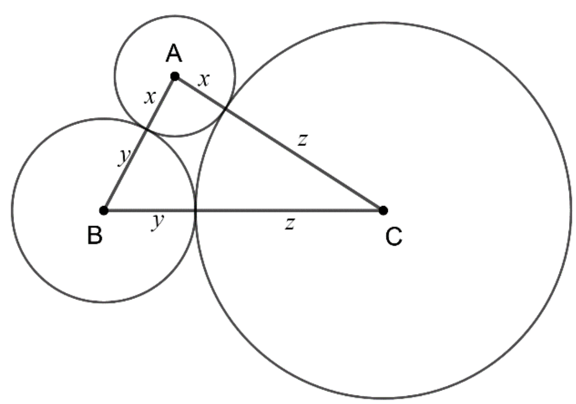
Конструкција. Применом конструкција **1**, **2** и **4.** најпре конструишемо једну од датих величина, рецимо x, и то $x_1 = b + c, x_2 = x_1 - a, x_3 = x = \frac{x_2}{2}$. Сада се око тачака A, B и C опишу кругови полупречника x, $c - x$ и $b - x$.

Доказ. Следи из анализе.

Дискусија. Конструкција је јединствена. За троугао ABC, из неједнакости троугла, вреди да је $c + b > a$, па тиме x се може конструисати. Осим тога је

$$c - x = c - \frac{c+b-a}{2} = \frac{a+c-b}{2} > 0.$$

Па је $c > x$. Слично добијамо и $b > x$.



Сл. 29.

III КОНСТРУКЦИЈА ПРАВИЛНИХ ПОЛИГОНА

3.1. Појам правилног полигона

Полигон је врло чест појам у математици, да чак су и основци врло брзо упознати са дефиницијама и особинама које они задовољавају. Правилан полигон је полигон чије су странице међусобно једнаке, углови међусобно подударни и само две суседне странице имају теме полигона као заједничку тачку.[7] Угао правилног многоугла са n темена се рачуна тако што се збир свих углова подели бројем углова (темена), тј. бројем n. Ако са α_n обележимо угао правилног n-тоугла, тада је

$$\alpha_n = \frac{(n-2)\cdot 180°}{n}.$$

Сваки правилан многоугао има описани и уписани круг. Центри тих кругова се поклапају и та тачка представља центар правилног многоугла. Једнакокраки троугао чија је основица страница правилног n-тоугла, а врх центар тог n-тоугла јесте карактеристични троугао правилног n-тоугла. Угао при врху карактеристичног троугла је $\varphi = \frac{360°}{n}$. Као што је већ речено, темена правилног полигона се налазе на кругу и узастопна темена деле круг на n једнаких лукова. Овај проблем се назива циклотомија. Циклотомија у буквалном преводу значи „резање круга“ и била је енигма коју су још пре 2000 година покушавали решити грчки математичари и филозофи. О циклотомији ће бити још речи касније.

3.2. Конструкција правилних полигона кроз историју

3.2.1. Антика

Кроз историју људске цивилизације правилни полигони су се показали као веома занимљиви геометријски објекти. Најстарија цивилизација у којој се математика изучава апстрактно, а геометрија развија као наука је старогрчка цивилизација. У старом Египту и Месопотамији геометрија се изучавала тек до познавања неких класичних поступака примењујући их у пракси и занату. Отуда и разлог што је конструкција, нарочито правилних полигона прво изучавана у Антици. Најчувеније и најутицајније дело из геометрије су „Елементи“ које је саставио александријски математичар **Еуклид,** у којој се налазе основе

[7] Ђ. Пауниħ, *Правилни полигони*, Предговор

конструкције. Оскудни су подаци који су дошли до нас из античке старине о Еуклидовом животу, његовој личности и времену у ком је живео. Зна се да је млађи од Платонових ученика, а старији од Ератостена и Архимеда, да је највише стварао отприлике 300. године пре нове ере. Елементи су састављени од тринаеаст књига од којих се првих шест односи на геометрију равни – планиметрију, следеће четири књиге нису геометријског карактера и баве се проблемима теорије бројева, а последње три се односе на геометрију простора – стереометрију. Четврта књига посвећена је полигонима чија темена припадају кругу или ивице додирују неки круг. Сви ставови у овој књизи конструктивног су карактера. У ставовима IV.2 – IV.5. конструише се троугао са задатим угловима (сличан датом троуглу) уписан у задати круг или описан око њега, и круг уписан или описан око задатог троугла. Ставови IV.6 – IV.9. су аналогни претходним ставовима, уз замену троугла за квадрат, тј. конструкција квадрата уписаног у неки круг или описаног око њега, и круг описан или уписан у квадрат. У ставу IV.10. Еуклид конструише једнакокраки троугао у коме су углови на основици два пута већи од угла при врху. У ставовима IV.11 – IV.14. конструише се правилан петоугао уписан или описан око задатог круга, и круг уписан или описан око датог петоугла. Еуклид четврту књигу завршава ставовима IV.15. и IV.16. у којима конструише правилни шестоугао и правилни петнаестоугао. Такође, у Антици су спознали да је за дати полигон могуће конструисати полигон са двоструким бројем страница, и још, да је могуће конструисати полигон са mn бројем страница, где су m и n узајамно прости бројеви, ако је позната конструкција полигона са m, односно са n страница. Конструкцију правилног седмоугла је првенствено проучавао **Архимед** и његови записи су делимично сачувани у арапском преводу.

3.2.2. Арапски математичари

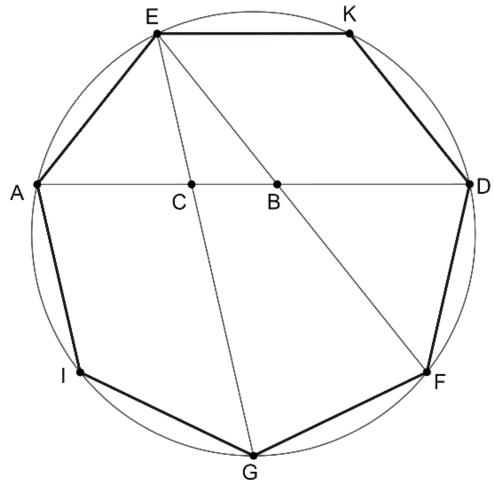
Анализа конструкције правилног седмоугла започета је још у Антици. Архимедови списи о конструкцији правилног седмоугла су сачувани на арапском језику, те су многи средњевековни арапски математичари (из 10. и 13. века) настављали и усавршавали Архимедов рад. Арапске конструкције су обелодањене 1984. године, захваљујући Јану Хохендејку, холандском историчару математике. За конструкцију правилног седмоугла, поред лењира и шестара, морају се користити конусни пресеци (хипербола, парабола) или уметање[8]. Архимед доказује да се може конструисати правилан седмоугао ако се на некој најдужој дијагонали знају тачке пресека са две друге најдуже дијагонале. Тачније, ако се знају две пропорције које задовољавају дужи на најдужој дијагонали добијене пресецима са друге две најдуже дијагонале, при чему те друге две дијагонале полазе из једног истог темена оне странице правилног седмоугла која је паралелна дијагонали која се пресеца, тј.

$$AB \cdot AC = BD^2 \text{ и } CD \cdot CB = AC^2,$$

што ћемо назвати *Архимедови услови* (сл. 30). Након доказивања утврђено је да се може конструисати правилан седмоугао ако је могуће на дужи AD одредити тачке B и C тако да важе Архимедови услови.

[8] Најчешће постављање праве да пролази кроз задату тачку, а да две дате линије (праве или криве) на њој одсецају дуж задате дужине. Овај поступак се практично изводи тако што се на ивици лењира означе крајеви дате дужи па се лењир обрће око задате тачке тако да једна означена тачка клизи по једној од задатих кривих док се друга означена тачка не нађе на другој задатој кривој.

Геометријски приказ ових услова извео је сам Архимед, а за конструкцију тачака A, B, C и D се користи уметање. Наиме Архимед полази од квадрата где кроз једно теме треба конструисати праву тако да је површина троуглова који одсеца од дијагоналног троугла у квадрату једнака површини троугла који одсеца на једној несуседној страници и продужетку друге.[9] Морамо напоменути да није јасно како се практично изводи поменуто уметање, јер га нема у Архимедовим списима, а нажалост, нека Архимедова дела су изгубљена. У општем случају уметање се не може извести лењиром и шестаром, због тога су арапски математичари сматрали уметање недопустивом операцијом па су покушавали да га замене „фиксном“ геометријом, најчешће, поред правих и кругова, користећи конусне пресеке као помоћна средства. Математичари који су конструисали Архимедову праву користећи хиперболе и параболе, јесу абу’л Џуд, ал-Сагани и ибн Јунис. Ибн-ал-Хајтам и ал-Кухи су конструисали Архимедове услове директно, такође користећи параболе и хиперболе, док је Абу’л Џуд конструисао правилан седмоугао користивши сопствену анализу уместо Архимедове.



Сл. 30.

За конструкцију правилног деветоугла потребно је познавати конструкцију трисекције угла[10] од $120°$, јер су унутрашњи углови деветоугла $40°$. Иако су старогрчки математичари, Архимед и Папос, знали извршити трисекцију угла уметањем, није познато да су се занимали конструкцијом деветоугла. Позната имена која се помињу у вези са конструкцијом деветоугла су синови Мусе ин Шакира (Мухамед, Ахмед и ал-Хасан), Абу’л Џуд и персијски математичар ал-Бурини.

3.2.3. Гаусов учинак и његово значење

Немачки математичар Карл Фридрих Гаус (*Carl Friedrich Gauss*, 1777-1855) је доказао да се правилан седамнаестоугао може конструисати помоћу лењира и шестара. Са својих непуних 19 година Гаус је докучио до јасног доказа о могућности конструкције правилних n-тоуглова лењиром и шестаром, а то је објавио у Аритметичким расправама 1801. године. Због овог фасцинантног окрића Гаус је одлучио да ће се бавити математиком пре свега, иако је био врстан у многим пољима. Познат је као „принц математике“ и сматра се једним о најутицајних математичара у историји.

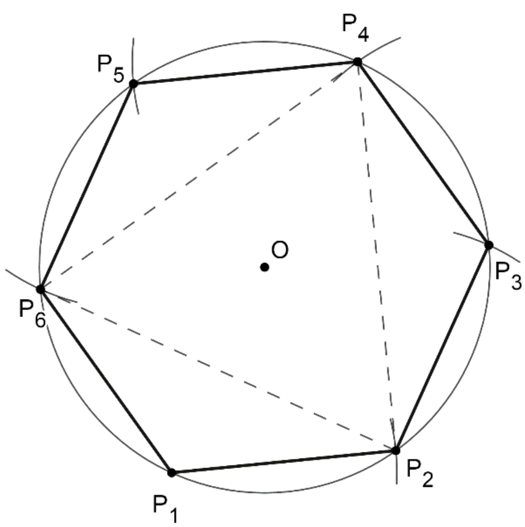

Сл. 31. Карл Фридрих Гаус

[9] Доказ да ово уметање даје потребну поделу дијагонале за конструкцију правилног седмоугла је детаљно образложено на странама 81. и 82. *Правилних полигона* др. Ђуре Паунића.
[10] Архимедова конструкцију за трисекцију угла уметањем, *Правилни полигони*, стр. 83.

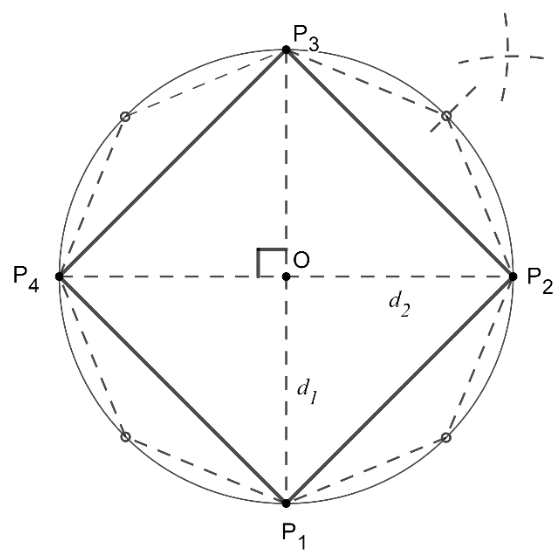
3.3. Конструкција правилног шестоугла и правилног троугла

Конструсати правилан шестоугао је лако јер је страница правилног шестоугла уписаног у круг, полупречник тог круга. Правилан троугао (једнкостраничан троугао) се добија када се споји свако друго теме правилног шестоугла. Ако је задат круг k полупречника r конструкција правилног шестоугла уписаног у k се изводи на следећи начин.

Одаберимо тачку P_1 на датом кругу k као једно теме траженог шестоугла (сл. 32). Теме P_2 је пресек круга k и круга са центром у тачки P_1 полупречника r. Понављањем тог поступка из тачке P_2 добијамо тачку P_3 итд. Поступак се завршава када добијемо тачку P_6. Неким другим одабиром тачке P_1 на k добили бисмо неки други шестоугао уписан у круг k. Но, како је већ речено, сви тако добијени шестоуглови међусобно су подударни и представљају једно решење.
Ако је дат конструисан правилни шестоугао у датом кругу, онда можемо једноставно конструисати и правилан дванаестоугао, тако што ћемо конструисати средишта лукова између два суседна темена шестоугла. Таквим поступком половљења лукова, можемо од конструисаног једнакостраничног троугла односно правилног шестоугла уписаног у дати круг, конструисати $(2^{\nu} \cdot 3)$ -тоугао, где је $\nu = 0, 1, 2, 3, \ldots$ Јасно, за $\nu = 0$ у питању је једнакостраничан троугао, за $\nu = 1$ шестоугао итд.



Сл. 32.



Сл. 33.

3.4. Конструкција правилног четвороугла

Конструкција правилног четвороугла уписаног у задати круг k полупречника r се изводи на следећи начин.

Одаберимо тачку P_1 на k као једно теме траженог четвороугла (сл. 33). Пречник d_1 круга k

који пролази кроз тачку P_1 сече k у P_3. Тачке P_2 и P_4 добијају се у пресеку круга k и пречника d_2 који је окомит на d_1. На тај начин добили смо сва четири темена траженог четвороугла.

Половљењем кружних лукова између два суседна темена, можемо конструисати (2^{ν})-тоугао, где је $\nu = 2,3,...$ За $\nu = 2$ у питању је квадрат, за $\nu = 3$ осмоугао итд.

3.5. Конструкција правилног петоугла и правилног десетоугла

3.5.1. Конструкција златног пресека

Конструкција правилног петоугла и правилног десетоугла захтева познавање дефиниције и конструкције *златног пресека.*

Дефиниција 3.5.1.1. Нека тачка C дели дуж AB тако да вреди $AB : AC = AC : BC$. Дуж AC зовемо златним пресеком (sectio aurea) дужи AB.

Ако са a, x и $a - x$ означимо AB, AC и BC редом, добијамо $a : x = x : (a - x)$. Решавањем квадратне једначине

$$x^2 + ax - a^2 = 0,$$

следи

$$x = \frac{a}{2}\left(\sqrt{5} - 1\right),$$

што представља дужину златног пресека дужи $AB = a$.[11]

Конструкција златног пресека. Над дужи AB као катетом конструишемо правоугли троугао ABO, тако да је друга катета $BO = \frac{1}{2}AB$ (сл. 34). На основу Питагорине теореме добијамо

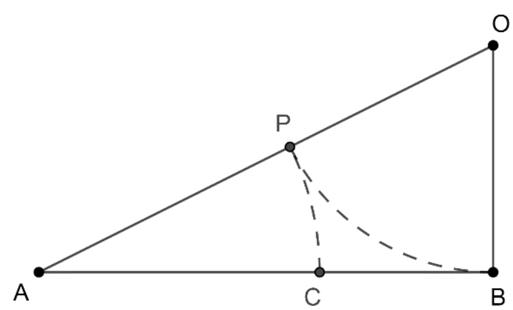
$$OA^2 = AB^2 + \frac{1}{4}AB^2 = a^2 + \frac{1}{4}a^2 = \frac{5}{4}a^2.$$

Одатле је $OA = \frac{a}{2}\sqrt{5}$.

На дуж OA нанесемо дуж $OP = OB$. Из $AC = AP$, следи

$$AC = OA - OP = \frac{a}{2}\left(\sqrt{5} - 1\right).$$

Теорема 3.5.1.2. У правоуглом троуглу у коме је дужина једне катете једнака половини дужине друге катете, златни пресек веће катете једнак је разлици хипотенузе и мање катете. [12]



Сл. 34.

[11] Д. Палман, *Геометријске конструкције*, стр. 103.
[12] Д. Палман, *Геометријске конструкције*, стр. 104.

3.5.2. Конструкција десетоугла ако је познат полупречник описаног круга

Нека је AB страница правилног десетоугла који је уписан у круг са центром O полупречника r (сл. 35). Централни угао α тетиве AB је тада

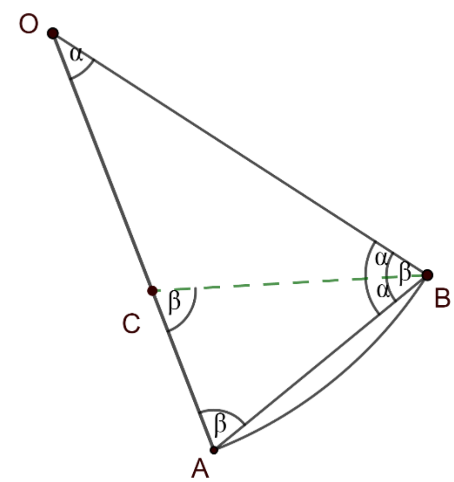
$$\alpha = \angle AOB = \frac{360°}{10} = 36°.$$

Троугао OAB је једнакокраки. Како је $2\beta + \alpha = 180°,\ \beta = 72°$. Симетрала угла у темену B троугла AOB сече страницу OA у тачки C. Како важи $\angle ABC = \frac{1}{2}\beta = \alpha$ и $\angle ACB = \beta$ добијамо $AB = BC = OC$. Троуглови OAB и BAC су слични па вреди $OA : AB = AB : AC$. Из $AB = OC$, добијамо да је OC златни пресек дужи $OA = r$.

Теорема 3.5.2.1. Страница правилног десетоугла уписаног у круг једнака је златном пресеку полупречника тог круга.[13]

Помоћу наведене теореме добијамо да је лако конструисати правилан десетоугао у полазни круг ако је познат полупречник круга.

Према теореми 3.5.1.2. и слици 34. конструишемо златни пресек OC дужи $OA = r$. Како дужина дужи OC представља дужину странице десетоугла, добијамо теме B као пресек кружног лука са центром у C полупречника OC и кружног лука са центром у A полупречника OC. Даље није тешко довршити конструкцију.



Сл. 35.

3.5.3. Страница и дијагонала правилног петоугла

Да бисмо одредили странице правилног петоугла ако му је задат полупречник описаног круга r, можемо користити познату Птоломејеву теорему (Claudius Ptolemaeus, Алксандрија, око 100. – око 178) коју нећемо доказивати.

Теорема 3.5.3.1. Нека је у круг уписан четвороугао $ABCD$, и нека су AC и BD његове дијагонале, тада важи

$$AC \cdot BD = AB \cdot CD + AD \cdot BC$$

тј. производ дијагонала тетивног четвороугла једнак је збиру производа парова супротних страница (важи и обрнуто)[14].

[13] Д. Палман, *Геометријске конструкције*, стр. 105.
[14] Д. Палман, *Геометријске конструкције*, стр. 105.

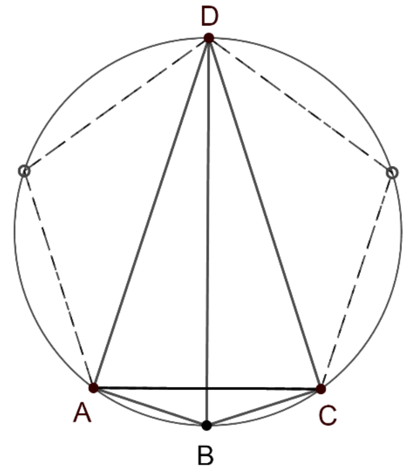
Уочимо три темена A, B, C правилног десетоугла уписаног у круг полупречника r и још четврто теме D које је дијаметрално супротно темену B (сл. 36). Према томе је

$$AB = BC = s_{10} = \frac{r}{2}\left(\sqrt{5} - 1\right).$$

Важи још и

$$BD = 2r.$$

Дијагонала правилног петоугла је дуж која спаја два темена петоугла која не леже на истој страници. Све дијагонале правилног петоугла су једнаке. Према слици 36. следи



Сл. 36.

$$AD = DC = \sqrt{BD^2 - AB^2} = \frac{r}{2}\sqrt{10 + 2\sqrt{5}} \qquad (3.1)$$

што представља дужину дијагонале правилног петоугла изражену помоћу полупречника описаног круга. Примењујући Птоломејеву теорему и једнакости $AB = BC$ и $AD = DC$ добијамо

$$AC = 2 \cdot \frac{BC \cdot AD}{BD}\text{, па је коначно } AC = s_5 = \frac{r}{2}\sqrt{10 - 2\sqrt{5}}. \qquad (3.2)$$

Дакле, изразили смо страницу правилног петоугла помоћу полупречника описаног круга тог петоула.

3.5.4. Конструкција правилног петоугла помоћу полупречника описаног круга

У датом кругу k са центром у O полупречника r повуче се пречник AB и нормално на њега полупречник OP_1 (сл. 37). Нека је N средиште полупречика OA. Са центром у тачки N повучемо кружни лук кроз P_1. Тај лук сече пречник AB у тачки Q. Уочимо правоугли троугао NOP_1. Имамо

$$NQ = NP_1 = \sqrt{NO^2 + {OP_1}^2} = \sqrt{\left(\frac{r}{2}\right)^2 + r^2} = \frac{r}{2}\sqrt{5}.$$

Даље је

$$OQ = NQ - NO = \frac{r}{2}\sqrt{5} - \frac{r}{2} = \frac{r}{2}\left(\sqrt{5} - 1\right) = s_{10}$$

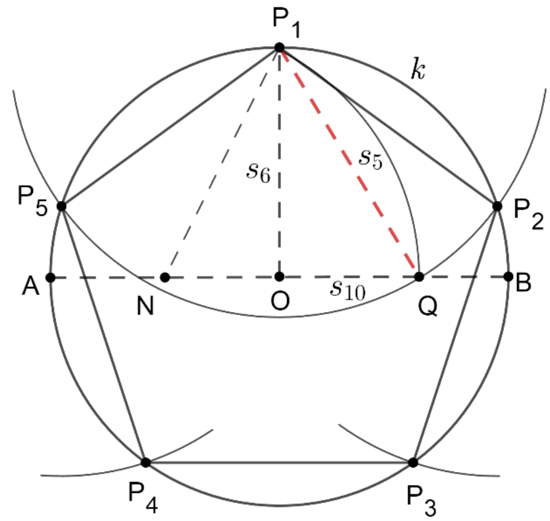
$$P_1Q = \sqrt{P_1O^2 + OQ^2} = \sqrt{r^2 + \left(\frac{r}{2}\left(\sqrt{5} - 1\right)\right)^2} = \frac{r}{2}\sqrt{10 - 2\sqrt{5}} = s_5.$$

На основу добијеног и према слици 37. добијамо

$$s_5{}^2 = s_{10}{}^2 + r^2\text{, односно } s_5{}^2 = s_{10}{}^2 + s_6{}^2. \qquad (3.3)$$

Тиме смо добили и доказ Еуклидове теореме XIII.10, да је страница правилног петоугла хипотенуза правоуглог троугла у коме је једна катета полупречник описаног круга, а друга већи део при подели полупречника описаног круга по златном пресеку[15].

Нека је конструисана страница петоугла на начин који је приказ на слици 37. Даље извођење конструкције петоугла је лако. Опише се кружни лук са центром у P_1 полупречника P_1Q да се у пресеку са кругом k добију тачке P_2 и P_5 које представљају два темена петоугла. Преостала два темена P_3 и P_4 добијамо као пресеке кружних лукова са центрима у P_2 и P_5 полупречника P_1Q са полазним кругом k.



Сл. 37.

3.5.5. Конструкција правилног петоугла ако је задата страница

Нека је на слици 38. дуж P_1P_2 ($P_1P_2 = a$) страница правилног петоугла. Конструишимо средиште дате странице и обележимо га са N. Затим у тачки P_2 подигнемо нормалу P_2M на P_1P_2 тако да је $P_2M = P_1P_2$. Даље, тачку пресека кружног лука са центром у N полупречника NM и продужетка странице P_1P_2 обележимо са Q. Сада теме P_3 траженог петоугла добијамо као пресек кружног лука са центром у P_1 који пролази кроз Q и кружног лука са центром у P_2 који пролази кроз P_1.

На основу слике 38. добијамо

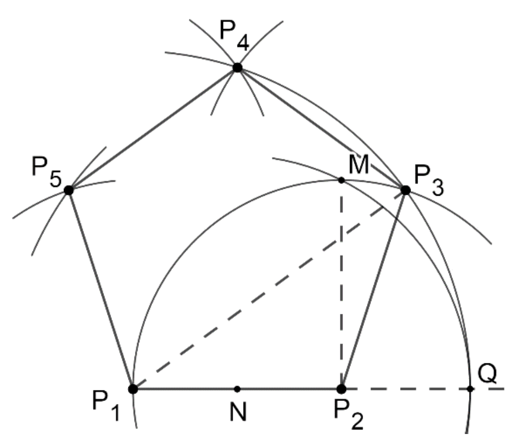
$NP_2 = \frac{a}{2}$,

$NM = \sqrt{NP_2^{\,2} + MP_2^{\,2}} = \sqrt{\left(\frac{a}{2}\right)^2 + a^2} = \frac{a}{2}\sqrt{5}$,

како је $NM = NQ$ имамо

$P_1P_3 = P_1Q = P_1N + NQ = \frac{a}{2} + \frac{a}{2}\sqrt{5} = \frac{a}{2}\left(\sqrt{5}+1\right)$.

Овим смо добили дужину дијагонале P_1P_3 помоћу странице a.



Сл. 38.

[15] Ђ. Паунић, *Правилни полигони*, стр. 26.

Из (3.1) и (3.2) следи

$$\frac{d}{a} = \frac{\frac{r}{2}\sqrt{10+2\sqrt{5}}}{\frac{r}{2}\sqrt{10-2\sqrt{5}}} = \frac{\sqrt{5}+1}{2},$$

одакле добијамо

$$d = \frac{a\left(\sqrt{5}+1\right)}{2},$$

тј. да је P_1P_3 заиста дијагона траженог петоугла. Чиме је ова конструкција доказана. Сада није тешко добити остала темена петоугла.

3.6. Конструкција правилног седмоугла и правилног деветоугла уз помоћна средства

3.6.1. Конструкција правилног седмоугла уз помоћна средства

Изведимо и докажимо сад конструкцију правилног седмоугла користећи особину да је могуће на дужи AD одредити тачке B и C тако да важе Архимедови услови $AB \cdot AC = BD^2$ и $CD \cdot CB = AC^2$.

Нека су A, B, C и D тачке на правој са наведеном особином (сл. 39). Конструишемо тачку E тако да је $CE = CA$ и $BE = BD$ и опишемо круг око троугла AED. Доказаћемо да је страница правилног седмоугла AE.

Троуглови ACE и DBE су једнакокраки. Једнаке углове у ΔACE означимо са β, а у ΔDBE са α. Продужимо дуж EB преко B до пресека са кругом и ту тачку означимо са F. Продужимо дуж EC преко C до пресека са кругом и ту тачку означимо са G. Дуж AF ће сећи EG у H.

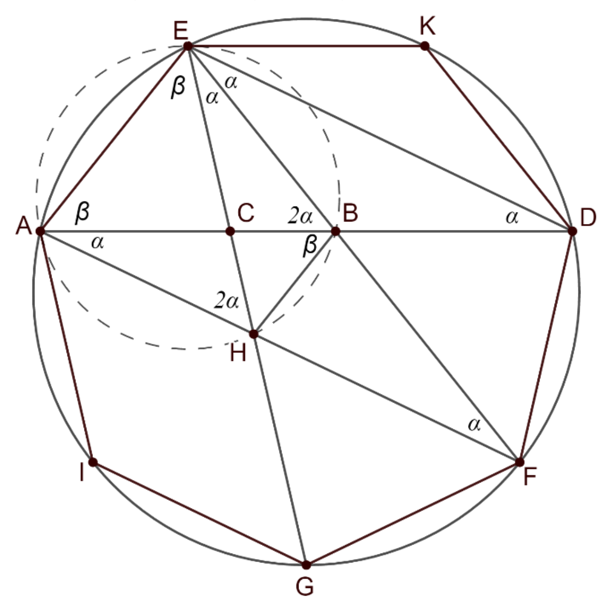
Из $CD \cdot CB = AC^2$ и $AC = EC$ добијамо $CB : CE = CE : CD$, тј. ΔBCE и ΔECD су слични јер имају заједнички угао код C, а налегле странице на тај угао су пропорционалне. Даље следи да је

$$\angle CBE = \angle CED = 2\alpha$$

јер је $\angle CBE$ спољашњи угао за ΔEDB. Тада је $\angle CEB = \alpha$.

Посматрајмо сада ΔEHF. Имамо

$$\angle HEF = \angle CEB = \alpha$$
$$\angle HFE = \angle AFE = \angle ADE = \alpha$$



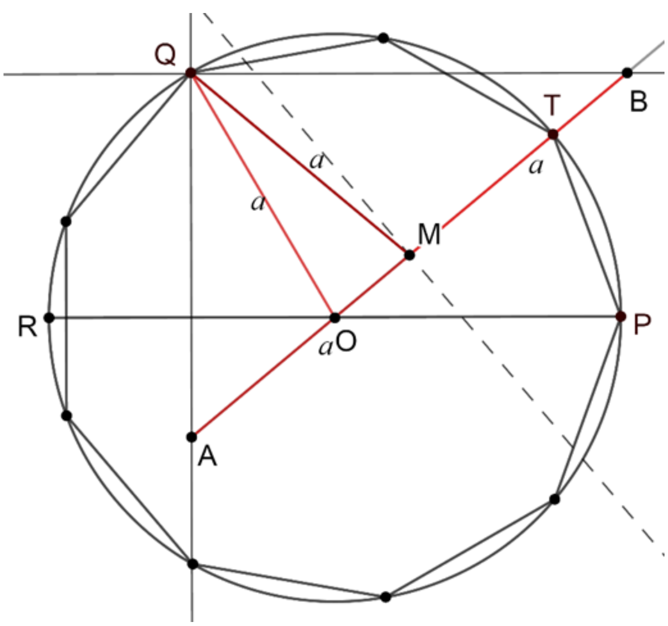
Сл. 39.

(као периферијски углови над једнаким луковима). Добијамо $\angle AHE = 2\alpha$ и $\angle ABE = 2\alpha$, те је четвороугао $AHBE$ тетивни. Углови $\angle HAB$ и $\angle HEB$ су периферни над истим кружним луком и једнаки су α. Троуглови ΔACH и ΔECB су подударни јер су углови код A и E једнаки α, $AC = EC$ по конструкцији углови код C су унакрсни, па следи $AH = EB$. Из тетивног четвороугла $AHBE$ добијамо $\angle ABH$ који је једнак углу $\angle AEH$ и који једнак β. Из особине тачака A, B, C и D, $AB \cdot AC = BD^2$, $EB = BD$ и $EB = AH$ добијамо $AB : AH = EB : EC$ тј. да су труглови ΔBAH и ΔBEC слични. Један угао им је једнак, $\angle BAH = \angle BEC = \alpha$, а налегле странице на тај угао су пропорционалне. Из ове сличности добијамо да је $\beta = 2\alpha$. Овим је доказ завршен јер је показано да луковима ED и AG одговарају периферијски углови 2α, чиме добијамо поделу круга на седам једнаких лукова (јер сваком од тих лукова одговара исти периферијски угао α).

3.6.2. Конструкција правилног деветоугла уз помоћна средства

Нека је дат круг k са центром у O полупречника a (сл. 40). Конструишимо угао $\angle POQ = 120°$ који ћемо да поделимо на три дела (унутрашњи углови деветоугла су по $40°$) према Архимедовој конструкцији за трисекцију угла уметањем помоћу круга. Кроз тачку Q конструисаћемо паралелу пречнику PR и из Q ћемо спустити нормалу n на пречник PR. Сада следи уметање, тј. кроз тачку O повући ћемо праву тако да одсечак AB буде једнак $2a$ и да QB буде веће од QA, где је A пресечна тачка праве кроз O и нормале n, а B је пресечна тачка праве и паралеле.

Нека је M средиште дужи AB, тада су ΔMQO и ΔMQB једнакокраки. Углови $\angle POB$ и $\angle OBQ$ су једнаки (углови са паралелним крацима).



Сл. 40.

Троугао ΔMQB је једнакокраки па је спољашњи угао

$$\angle QMO = 2\angle MBQ = 2\angle BOP.$$

Будући да је ΔMQO једнакокраки важи $\angle QMO = \angle MOQ$ и добија се да је

$$\angle POB = \frac{1}{3}\angle POQ = 40°.$$

Даље није тешко довршити конструкцију деветоугла.

3.7. Приближна конструкција правилног седмоугла и правилног деветоугла

Може се догодити из практичних разлога да треба нацртати правилан седмоугао или правилан деветоугао. У ту сврху, будући да није могуће конструисати правилан седмоугао и правилан деветоугао, прибегнемо некој приближној конструкцији таквих n-тоуглова. Постоји низ таквих конструкција којима добијамо седмоуглове и деветоуглове с неком мањом или већом грешком. Обично су те грешке далеко мање од грешака које чинимо слободним цртањем, зато су такве приближне конструкције сасвим задовољавајуће за праксу.

3.7.1. Приближна конструкција правилног седмоугла

Нека је дат круг k са полупречником r и нека треба конструисати правилни седмоугао уписан у тај круг. Одаберимо један полупречник OM (сл. 41) и конструишимо симетралу тог полуречника. Једну пресечну тачку те симетрале и круга k означићемо са K, а средиште дужи OM са L. Дуж KL има дужину приближно једнаку дужину странице правилног седмоугла уписаног у дати круг. На слици видимо да важи следеће

$$KL = \frac{r}{2} \cdot \sqrt{3} = r \cdot 0{,}8660 \ldots \tag{3.4}$$

Нека да је дат јединични круг k, и нека је у њему уписан правилан полигон. Такав n-тоугао можемо поделити на n једнакокраких троуглова (карактеристичних троуглова) којима је дужина кракова 1, с теменом у центру круга и са основицом која је и страница посматраног полигона. Дужина странице s_n правилног n-тоугла уписаног у јединични круг је

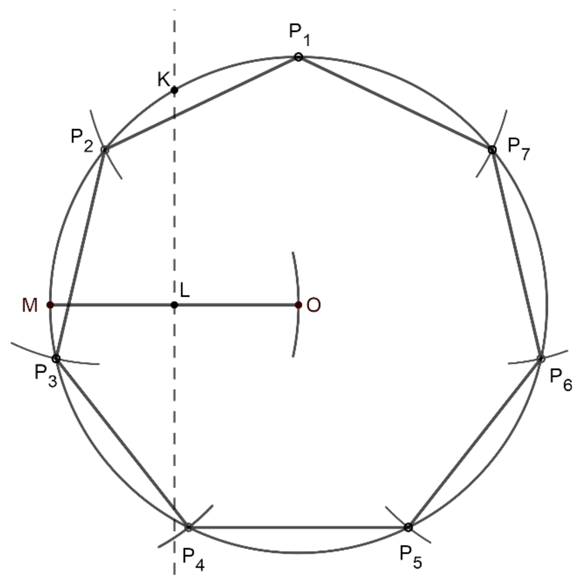
$$s_n = 2 \cdot \ sin\frac{\pi}{n}. \tag{3.5}$$

За страницу правилног седмоугла уписаног у јединични круг важи

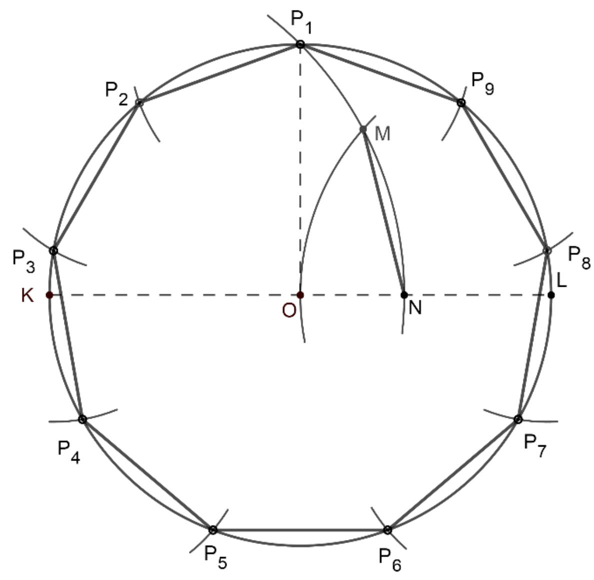
$$s_7 = 2 \cdot \ sin\frac{\pi}{7} = 2 \cdot \ sin\, 25{,}7143 = 0{,}867767 \approx 0{,}868$$

Приметимо, за полупречник од $10cm$, из (3.4) добијамо да страница приближно конструисаног седмоугла износи $8{,}66$, док тачно конструисаног седмоугла (када би таква конструкција била могућа, што није случај) би износила $8{,}68$. Добијамо да грешка износи мање од два десета дела милиметра, што је практички занемарљиво.

Такође, угао при врху карактеристичног троугла приближно, односно тачно конструисаног седмоугла износи $51{,}317812°$, односно $\frac{360°}{7} = 51{,}428571°$, што даје процентуалну грешку од $0{,}216\%$.



Сл. 41.



Сл. 42.

3.7.2. Приближна конструкција правилног деветоугла

Нека је дат круг k са полупречником r у који треба конструисати правилни деветоугао. Одредимо произвољно неки пречник и означимо га са KL. Конструишимо полупречник OP_1 који је окомит на KL (сл. 42). Са центром у тачки K опишимо кружни лук кроз тачку P_1, а са центром у тачки L опишимо кружни лук кроз тачку O. Нека кружни лук кроз P_1 сече пречник KL у тачки N, а нека се оба ова кружна лука секу у тачки M. Дуж MN нам је тада приближно једнака страници правилног деветоугла уписаног у круг k.

Аналогно, користећи формулу (3.5) добијамо да је дужина странице правилног деветоугла уписаног у јединични круг 0,68404, док је дужина странице приближног конструисаног деветоугла 0,68493. Такође, упоређујући углове при врху карактеристичног троугла у деветоуглу и карактеристичног троугла у деветоуглу добијеног приближном конструкцијом, добијамо вредности $\frac{360°}{90} = 40°$ и 39,91° што даје процентуалну грешку од 0,226%.[16]

Постоји још неколико приближних конструкција правилног седмоугла и правилног деветоугла, али горе описане се издвајају по једноставности и најмањим начињеним грешкама.

[16] Подаци добијени преко програма *Geogebra*, приликом конструкције са слике 42.

IV ОСВРТ НА АЛГЕБРУ

Да бисмо се бавили озбиљним конструкцијама лењиром и шестаром потребно је знање и вештина владања моћним алгебарским оружјем (алгебарским структурама, полиномима, решавањем једначина, проширењем поља, теоријом група, теоријом Галоа....). Навешћемо најосновније из наведених области у циљу даљег разумевања решивости конструкција лењиром и шестаром.

4.1. Решавање једначина

4.1.1. Квадратна једначина

Решавање једначина је био један од најзначајних проблема старих математичара, а морамо признати и проблем свих који би хтели да се математичарима назову. Бар са једначинама другог степена није тешко и то сваки средњошколац зна, решења једначине

$$ax^2+bx+c=0 \tag{4.1}$$

јесу

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

До ових решења долазимо тако што формулу (4.1) трансформишемо у

$$a\left[x^2+2\frac{b}{2a}x+\left(\frac{b}{2a}\right)^2\right]-a\left(\frac{b}{2a}\right)^2+c=0,$$

тј.

$$a\left(x+\frac{b}{2a}\right)^2-\frac{b^2-4ac}{2a}=0,$$

одакле изразимо x.

4.1.2. Кубна једначина

За време ренесансе, 1539. године, алгебарско решење кубне једначине је открио Никола Тартаља (Niccolo Tartaglia, oko 1500-1557), учествујући у тада често организованим математичким такмичењима узмеђу градова република.

Међутим, Ђироламо Кардано (Girolamo Cardano, 1501-1576) успева убедити Тартаљу да му открије своју тајну формулу, и он је коначно објављује у књизи „Велика вештина“, додавши још и геометријске доказе за решења. Због тога се обрасци за алгебарско решење кубних једначина називају *Карданови обрасци.*

Сл. 43. Никола Тартаља

Сваку кубну једначину

$$ax^3+bx^2+cx+d=0$$

поделивши са a и увођењем смене $x \to x-\dfrac{b}{3}$

сводимо на облик

$$x^3+px+q=0, \qquad (4.2)$$

где су p и q изражене преко коефицијената полазне једначине. Увођењем смене $x=u+v$ у (4, 2) добијамо

$$\left(u^3+v^3\right)+(u+v)(3uv+p)+q=0.$$

Претпоставимо да је $u^3+v^3=-q$, тада добијамо да је $u^3v^3=-\dfrac{p^3}{27}$. Користећи Вијетове обрасце[17] долазимо до квадратне једначине,

$$z^2+qz-\frac{p^3}{27}=0$$

која се назива *квадратна резолвента* кубне једначине и чија су решења u^3 и v^3. А њени корени су

$$z_{1,2}=-\frac{q}{2}\pm\sqrt{\left(\frac{q}{2}\right)^2+\left(\frac{p}{3}\right)^3}.$$

Враћајући се на u, односно v, морамо имати у виду да кубни корен из z_1, односно из z_2 има три вредности у пољу комплексних бројева. Означимо главно решење са u, односно v, остале две вредности су ξu и $\xi^2 u$, односно $\xi^2 v$ и ξv, где су $\xi=-\frac{1}{2}+\frac{\sqrt{3}}{2}i$ и $\xi^2=-\frac{1}{2}-\frac{\sqrt{3}}{2}i$ комплексни кубни корени из јединице.

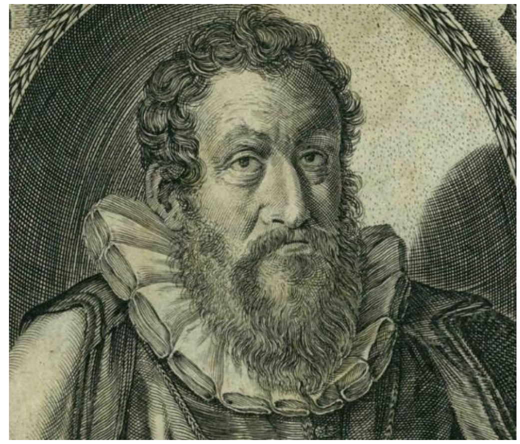
[17] Бројеви x_1 и x_2 су решења квадратне једначине $ax^2+bx+c=0, a,b,c\in\mathbb{R}, a\neq 0$, ако и само ако важи $x_1+x_2=-\frac{b}{a}$ и $x_1 x_2=-\frac{c}{a}$.

Коначно добијамо обрасце за три решења почетне кубне једначине тзв. Карданове обрасце (а сетимо се да су p и q изражени преко коефицијената полазне једначине):

$$x_1 = \sqrt[3]{-\frac{q}{2}+\sqrt{\left(\frac{q}{2}\right)^2+\left(\frac{p}{3}\right)^3}} + \sqrt[3]{-\frac{q}{2}-\sqrt{\left(\frac{q}{2}\right)^2+\left(\frac{p}{3}\right)^3}}$$

$$x_2 = \xi\sqrt[3]{-\frac{q}{2}+\sqrt{\left(\frac{q}{2}\right)^2+\left(\frac{p}{3}\right)^3}} + \xi^2\sqrt[3]{-\frac{q}{2}-\sqrt{\left(\frac{q}{2}\right)^2+\left(\frac{p}{3}\right)^3}}$$

$$x_3 = \xi^2\sqrt[3]{-\frac{q}{2}+\sqrt{\left(\frac{q}{2}\right)^2+\left(\frac{p}{3}\right)^3}} + \xi\sqrt[3]{-\frac{q}{2}-\sqrt{\left(\frac{q}{2}\right)^2+\left(\frac{p}{3}\right)^3}}.$$



Сл. 44. Ђироламо Кардано

4.1.3. Једначина четвртог степена

Карданов ученик, Лодовико Ферари (Lodovico de Ferrari, 1522-1565), је успео доћи до опште формуле за решења једначине четвртог степена изражених преко њених коефицијената. Слично као једначине другог и трећег степена, једначину чевртог степен можемо свести на облик

$$x^4 + px^2 + qx + r = 0. \tag{4.3}$$

Трансформацијама и увођењем α горња једначина постаје

$$\left(x^2+\frac{p}{2}+\alpha\right)^2 - 2\alpha x^2 + qx + \left(r-\frac{p^2}{4}-p\alpha-\alpha^2\right) = 0.$$

Да би важило

$$2\alpha x^2 - qx - \left(r-\frac{p^2}{4}-p\alpha-\alpha^2\right) = 2\alpha\left(x-\frac{q^2}{4\alpha}\right)^2$$

дискриминанта мора бити једнака нули, тј.

$$q^2 + 8\alpha\left(r-\frac{p^2}{4}-p\alpha-\alpha^2\right) = 0,$$

што представља кубну једначину по α. Познавајући Карданове формуле, α можемо изразити преко коефицијената p, q и r преко четири рационалне операције и операције кореновања. Дакле, из

$$\left(x^2+\frac{p}{2}+\alpha\right)^2 - 2\alpha\left(x-\frac{q^2}{4\alpha}\right)^2 = 0$$

Сл. 45. Лодовико Ферари

добијамо

$$\left[\left(x^2+\frac{p}{2}+\alpha\right)-\sqrt{2\alpha}\left(x-\frac{q^2}{4\alpha}\right)\right]\left[\left(x^2+\frac{p}{2}+\alpha\right)-\sqrt{2\alpha}\left(x-\frac{q^2}{4\alpha}\right)\right]=0. \qquad (4.4)$$

Једначину (4.4) решавамо једноставно решавајући две квадратне једначине од који се састоји, а њена решења представљају решења једначине (4.3) четвртог степена.

Дакле, решења једначина другог, трећег и четвртог степена могу да се изразе формулама у којима се налазе операције сабирања, одузимања, множења, дељења или кореновања коефицијената полазне једначине, и такве изразе називамо *радикалима*.

За једначине вишег степена од четвртог не постоје опште формуле решења у радикалима, и Галоа (Évariste Galois, 1811-1832) је у својој теорији разјаснио по којим условима једначина било ког степена има решење изражено у радикалима.

4.2. Радикални изрази. Конструктибилни бројеви

У српском језику значење придева „радикалан" јесте суштински, коренски. У математици у изразу $\sqrt{x}$ знак корена „$\sqrt{\ }$" називамо радикални знак, а x називамо радиканд. Сваки израз који садржи радикал назива се радикалним изразом. Квадратни радикални израз или *квадратна ирационалност* јесу радикални изрази у којима се појављују квадратни корени. Прецизније, то су изрази састављени од коначно много рационалних операција и коначно много налажења квадратних корена на природне бројеве. На основу алгебарске методе добијамо да је број записан у облику квадратне ирационалности **конструктибилан број**. Пример радикала је

$$\alpha=\frac{\sqrt{a+\sqrt{b}}+\sqrt{c}}{\sqrt{d+\sqrt{e+\sqrt{f}}}}.$$ [18]

Висином n квадратне ирационалности подразумеваћемо највећи број појављивања квадратног корена по дубини унутар радикала. У горњем примеру висина је 3 (радикал у имениоцу). Радикале у којима се та висина реализује називамо максималним радикалима. Број максималних радикала називамо ширином m квадратне ирационалности. У горњем примеру ширина је 1. Ширина m броји само оне максималне радикале који се не могу да изразити рачунским операцијама преко осталих радикала исте висине или мање. Дакле, свакој квадратној ирационалности можемо доделити пар (n, m) који се зове *тип радикала*. Радикални израз α је рационални број ако и само ако је типа $(0,0)$.

[18] F. Klein, *Elementary Mathematics from an advanced standpoint of Arithmetic, Algebra and Analysis,* стр. 53.

Ако два квадратна радикална израза имају различите висине n и n', нижи тип ће имати онај радикални израз чија је висина мања; ако два квадратна радикална израза имају исте висине нижи тип ће имати онај радикални израз чија је ширина мања.

Тврђење 4.2.1. Сваки радикални израз x типа (n, m) можемо записати у облику $x = P + Q\sqrt{R}$, где су P, Q и R радикални израз нижег типа.
Доказ. Нека је $\sqrt{R}$ један од максималних радикала висине n посматраног радикала x. Запишимо x у облику

$$x = \frac{\alpha + \beta\sqrt{R}}{\gamma + \delta\sqrt{R}}, \qquad \gamma + \delta\sqrt{R} \neq 0$$

где $\alpha, \beta, \gamma, \delta$ садрже највише $m - 1$ понављања висине n, а R је висине $n - 1$.

Овде је $\gamma - \delta\sqrt{R} \neq 0$, јер није могуће $\gamma = \delta = 0$, нити $\sqrt{R} = \frac{\gamma}{\delta}$, пошто би тада важило да се максимални радикал може представити рачунским операцијама преко осталих радикала исте или мање висине. Проширивањем x са $\gamma - \delta\sqrt{R}$, добијамо

$$x = \frac{\alpha + \beta\sqrt{R}}{\gamma + \delta\sqrt{R}} \cdot \frac{\gamma - \delta\sqrt{R}}{\gamma - \delta\sqrt{R}} = P + Q\sqrt{R},$$

где су P и Q рационалне функције од $\alpha, \beta, \gamma, \delta$ које су највишег типа $(n, m - 1)$.

4.3. Алгебарске структуре

Како овај рад не би премашио опсег једног мастер рада и не би много скренуо с теме, ево кратког приручника о основним дефиницијама и теоремама алгебре, углавном без доказа истих.

Дефиниција 4.3.1. **Групоид** је уређени пар $(G,*)$, где је G непразан скуп, а $*$ бинарна операција на G.

Дефиниција 4.3.2. **Полугрупа** је асоцијативни групоид.

Дефиниција 4.3.3. **Група** је најзначајнија алгебарска структура. Групоид $(G,\cdot)$ је група ако у G постоји елеменат e, тако да важи:
(1) За свако $x, y, z \in G$ важи $x \cdot (y \cdot z) = (x \cdot y)$.
(2) За свако $x \in G$ важи $x \cdot e = e \cdot x = x$, (e је неутрални елемент операције $\cdot$).
(3) За свако $x \in G$ постоји $x^{-1} \in G$, тако да је $x \cdot x^{-1} = x^{-1} \cdot x = e$, ($x^{-1}$ је инверзни елемент за x операције $\cdot$)
Ако је операција у групи комутативна, тј. ако за све $x, y \in G$ важи $x \cdot y = y \cdot x$, онда је група *комутативна* или *Абелова.*

Дефиниција 4.3.4. **Ред групе** $(G,\cdot)$ је кардиналност $|G|$. Ред елемента x групе $(G,\cdot)$ је најмањи позитиван број n за који важи $x^n = e$.

Дефиниција 4.3.4. **Прстен** је алгебарска структура $(R, +, \cdot)$, са две бинарне операције, за које важи:

(1) $(R, +)$ је Абелова група;

(2) $(R, \cdot)$ је полугрупа;

(3) испуњени су следећи дистрибутивни закони: за свако $x, y, z \in R$ важи

$x \cdot (y + z) = x \cdot y + x \cdot z$ и $(x + y) \cdot z = x \cdot z + y \cdot z$.

Дефиниција 4.3.5. **Поље** је прстен $(P, +, \cdot)$ у коме је $(P \setminus \{0\}, \cdot)$ Абелова група. [19]

Дефиниција 4.3.6. Нека је $(P, +, \cdot)$ поље и e је неутрални елемент за операцију $\cdot$. Нека је за $n \in \mathbb{N}$ дефинисано $na = \underbrace{a + a + \cdots + a}_{n}$. Нека је $S = \{n \mid ne = 0\}$. Ако је $S \neq \emptyset$ тада је $p = min\, S$ **карактеристика поља** $(P, +, \cdot)$. Ако је $S = \emptyset$, тада је $p = 0$ (или бесконачно).

Другачије речено, карактеристика поља је ред неутралног елемента операције $\cdot$ у групи $(P, +)$.

Ако је поље коначне карактеристике, $p \neq 0$, онда је p прост број.

Дефиниција 4.3.7. Нека је $(G, \cdot)$ група, а A подскуп скупа G. Подгрупа генерисана скупом A, у ознаци $\langle A \rangle$, је најмања подгрупа групе $(G, \cdot)$ чији домен садржи скуп A. Група G је **циклична** ако и само ако је генерисана неким једноелементним скупом.

Дефиниција 4.3.8. Нека су $G = (G, \cdot)$ и $H = (H, *)$ две групе. Пресликавање $G \to H$ је **хомоморфизам** групе G у групу H ако и само ако важи: $\forall a, b \in G\ f(a \cdot b) = f(a) * f(b)$ (сажето се формулише са: слика производа једнака је производу слика). Инјективни, односно сирјективни, односно бијективни хомоморфизам зове се **мономорфизам** (утапање), односно **епиморфизам**, односно **изоморфизам**. Ако је H баш G онда говоримо о **ендоморфизму**, тј **аутоморфизму** (бијективном ендоморфизму).

Дефиниција 4.3.9. Нека је H погрупа групе G и нека $a \in G$. Дефинишимо $aH \stackrel{\text{def}}{=} \{ah \mid h \in H\}$. H је **нормална подгрупа** групе G, у ознаци $H \triangleleft G$, ако и само ако важи, $g \in G\ gH = Hg$.

Тврђење 4.3.10. Нека је H нормална подгрупа групе G. Тада је $G/H = \langle \{aH \mid a \in G\}, \cdot \rangle$, где је $aH \cdot bH \stackrel{\text{def}}{=} abH$, тзв **фактор група** групе G по групи H.

Тврђење 4.3.11. За коначне групе важи:

а) Ако је ред групе прост број, група је циклична.

б) Група чији је ред степен простог броја p је је p-група.

[19] Дефиниција 4.3.1 –Дефиниција 4.3.5. узете из Б. Шешеља, А. Тепавчевић, *Алгебра 1*

Дефиниција 4.3.12. **Нормални низ групе** G је коначан низ подгрупа групе G, $G = G_0 \supset G_1 \supset \cdots \supset G_{k-1} \supset G_k = E$, где је за свако i, $1 \leq i \leq k$, G_i нормална погрупа групе G_{i-1}.

Дефиниција 4.3.13. Нормални низ је решив ако и само ако су сви његови фактори Абелове групе, тј G_{k-1}/E.

Теорема 4.3.14. Група је **решива** ако и само ако има решиви нормални низ чији су фактори цикличне групе простог реда. Коначне p-групе су решиве.

Теорема 4.3.15. Коначне p-групе су решиве.[20]

4.4. Прстен полинома

Дефиниција 4.4.1. Нека је R комутативан прстен, а x промењљива. Израз

$$p_0 + p_1 x + p_2 x^2 + \cdots + p_n x^n, \quad p_i \in R, i = 0,1, \dots, n, \quad p_n \neq 0,$$

јесте **полином** са коефицијентима из R степена n и означавамо са $p(x)$. Нормализован полином је онај за који важи $p_n = 1$.

Скуп полинома са коефицијентима из комутативног прстена R је такође прстен и означавамо га са $R[x]$.

Дефиниција 4.4.2. **Корен полинома** α је број за који важи $p(\alpha) = 0$.

Теорема 4.4.3. (**Безуова теорема**). α је корен полинома f ако и само ако полином $x - \alpha$ дели полином f тј. важи $f(x) = (x - \alpha)g(x) + r(x)$, при чему је $r(x) \equiv 0$ или је степен $r(x)$ мањи од степена $g(x)$.

Скуп полинома са коефицијентима из комутативног прстена R је такође прстен и означавамо га са $R[x]$.

Дефиниција 4.4.4. Полином са коефицијентима из комутативног прстена јесте **сводљив** ако може да се представи као производ два полинома мањег степена, а **несводљив** ако то не важи.

Нпр. $x^2 - 2 = (x + \sqrt{2})(x + \sqrt{2})$ је сводљив над пољем реалним бројева, а несводљив над пољем рационалних.

Теорема 4.4.5.(**Ајзенштајнов критеријум**) Нека је дат полином са целим коефицијентима

$$f = a_0 + a_1 x + \cdots + a_n x^n .$$

[20] Дефиниција 4.3.6 –Дефиниција 4.3.13, Тврђење 4.3.10. Тврђење 4.3.11, Теорема 4.3.14. узете из М. З. Груловић, *Основи теорије група*

Ако постоји прости број p такав да:

(1) p не дели најстарији коефицијент a_n,

(2) p дели све остале коефицијенте $a_{n-1}, \ldots, a_1, a_0$

(3) p^2 не дели слободни члан a_0,

тада је полином f несводљив у $\mathbb{Q}[x]$.[21]

Теорема 4.4.6. Сваки комплексни полином са комплексним коефицијентима има комплексни корен.

Као последицу ове теореме добијамо да се сваки комплексни полином може записати у облику $f = a_n(x - x_1) \cdot \ldots \cdot (x - x_n)$. У пољу комплексних бројева сваки полином степена n има тачно n корена који не морају бити међусобно различити и то тврђење се назива *основни став алгебре.*

Теорема 4.4.7. **(Рационални корени целобројних полинома)**. Нека је

$$f = a_0 + a_1x + \cdots + a_nx^n$$

полином са целобројним коефицијентима. Ако је нескративи разломак $\alpha = \frac{p}{q}$ корен полинома f, тада важи да је p делилац коефицијента a_0, а q делилац коефицијента a_n.

Доказ. Како је α корен полинома f важи

$$a_0 + a_1\frac{p}{q} + \cdots + a_n\left(\frac{p}{q}\right)^n = 0.$$

Множењем са q^{n-1} добијамо

$$a_0q^{n-1} + a_1q^{n-2}p + \cdots + \frac{a_np^n}{q} = 0. \tag{4.5}$$

Из (4.5) добијамо да важи $q \mid a_np^n$ (јер су остали сабирци цели бројеви).

Множењем (4.5) са q добијамо $a_0q^n + a_1q^{n-1}p + \cdots + a_np^n = 0$, односно

$$a_0q^n = -p(a_1q^{n-1} + \cdots + a_np^{n-1})$$

одакле добијамо $p \mid a_0q^n$.

Пошто је разломак $\frac{p}{q}$ нескратив, из $q \mid a_np^n$, односно $p \mid a_0q^n$, остаје да важи $q \mid a_n$, односно $p \mid a_0$, чиме је теорема доказана.

Тврђење 4.4.8. Ако кубна једначина $x^3 + ax^2 + bx + c = 0$ има конструктибилни корен, она има и рационални корен.

[21] Дефиниција 4.4.1, Дефиниција 4.4.2, Дефиниција 4.4.4, Теорема 4.4.3, Теорема 4.4.5 преузете из Ђ. Пауновић, *Правилни полигони*

Доказ. Нека је α корен дате кубне једначине, који је радикални израз типа (n, m). Показаћемо да ће и радикални израз нижег типа бити корен кубне једначине.

Искористићемо тврђење која каже да сваки радикални израз типа (n, m) можемо записати у облику $\alpha = P + Q\sqrt{R}$, где су P, Q и R радикални израз нижег типа, те добијамо

$$\left(P + Q\sqrt{R}\right)^3 + a\left(P + Q\sqrt{R}\right)^2 + b\left(P + Q\sqrt{R}\right) + c = A + B\sqrt{R} = 0$$

за
$$A = P^3 + 3PQ^2 + aP^2 + aQ^2R + bP + c$$
$$B = Q^3R + 3QP^2 + 2aPQ + bQ.$$

Важи $B = A = 0$, јер ако је $B \neq 0$, добијамо $\sqrt{R} = -\frac{A}{B}$, што значи да се максимални радикал $\sqrt{R}$ изража рационално преко радикалних израза P и Q, што није могуће, јер ширина броји само оне максималне радикале који не могу да се изразе, рачунским операцијама, преко осталих радикала исте висине или мање.

Лако се види да је и $\beta = P - Q\sqrt{R}$, такође корен наше једначине. Према Вијетовим обрасцима добијамо

$$\alpha + \beta + \gamma = -a, \text{ тј. } 2P + \gamma = -a$$

одакле је $\gamma = -a - 2P$, што је радикални израз нижег типа од типа израза α и β. Добијамо да γ може једино бити типа $(0,0)$, односно рационалан број, јер би у супротном добили да постоји корен нижег типа од типа γ, а тим и од типа α и β, што би било немогуће јер су једини корени α, β и γ.[22]

Ако овај доказ изанализирамо користећи се алатима из области „проширивање поља“ (о чему говоримо у наредном поглављу), те добијамо следећа запажања. Ако са K_0 означимо поље рационалних бројева, онда би решења α и β посматране кубне једначине припадала неком адјункцијом проширеном пољу K_n $(n \geq 1)$ поља K_0, од n квадратних корена. За $\alpha = P + Q\sqrt{R}$ би важило P, Q, $R \in K_{n-1}$ и $\sqrt{R} \notin K_{n-1}$. Уврстивши $P + Q\sqrt{R}$ у кубну једначину, као њен корен, добијамо $A, B \in K_{n-1}$. Решења α и β била би различита, супротно, из $\alpha - \beta = 2Q\sqrt{R} = 0$ добијамо да је $Q = 0$ што би значило $\alpha = \beta = P \in K_{n-1}$ што није могуће према својствима K_n. Даље, долазећи до трећег корена $\gamma = -a - 2P \in K_{n-1}$, добијамо да је γ рационалан број, јер у супротном, понављајући поступак за γ, добили бисмо да $\alpha \in K_{n-2}$, што је немогуће.

4.5. Проширење поља

Поље L је **проширење поља** K ако је поље K потпоље поља L. Свако проширење ћемо посматрати као векторски простор над пољем K, при чему је сабирање у пољу L сабирање

[22] Теорема 4.4.6, Теорема 4.4.7, Тврђење 4.4.8. узети из А. Липковски, *Елементарна алгебра I део*

вектора, а множење елемента из L елементом из K је множење вектора скаларом. Присетимо се да је база векторског простора скуп вектора који је генеришу и који су линеарно независни, те да све базе имају исти број елемената који представља димензију тог векторског простора. Стога, димензија поља L посматраног као векторски простор над пољем K назива се степен екстензије и означава са $[L : K]$. Ако је степен екстензије природан број, онда је проширење **коначно проширење**, у супротном је бесконачно.

Пример 4.5.1. Степен екстензије поља комплексних бројева над пољем реалних бројева је 2, јер је једна база $\{1, i\}$.

Свако коначно проширење је алгебарско проширење. Наиме, ако је проширење коначно онда је $[L : K] = n$, где је n коначан број. Посматрајући било који елемент α поља L, који је вектор, и $n + 1$ вектора $\alpha^0 = e, \alpha^1, \alpha^2, \dots, \alpha^n$, који морају бити линеарно зависни (јер ако су линеано независни, били би база, а свака база има исти број елемената), односно, постоје скалари $a_i, 0 \leq i \leq n$ из K, од којих бар један мора бити различит од нуле, такви да важи

$$\sum_{i=0}^{n} a_i \alpha^i = 0.$$

Овим закључујемо да је наш посматрани елемент α уствари корен ненула полинома $f(x) = \sum_{i=0}^{n} a_i x^i$, односно полинома чији су коефицијенти елементи поља K, стога га називамо *алгебарским елементом над* K. А проширење је *алгебарско* ако су сви његови елементи алгебарски над K. Треба имати на уму да полином $f(x)$ није једини полином који припада прстену $K[x]$ и који се поништава у тачки α, јер такав је и сваки полином $f(x)g(x)$, за било који полином $g(x) \in K[x]$. Међу свим оваквим полиномима постоји онај најмањег степена, који нормиран, назива се *минималним полиномом,* у ознаци $f_\alpha(x)$, а његов степен назива се степен елемента α на пољем K.

Тврђење 4.5.2. (**О минималном полиному**). Нека $f(x) \in K[x]$ и нека је $f(\alpha) = 0$, за $\alpha \in L$, где је L проширење поља К. Тада је $f(x)$ минимални полином за α ако и само ако је $f(x)$ несводљив у $K[x]$, у ознаци $f_\alpha(x) \in K[x]$.

Проширења настала адјункцијом

Нека је L проширење поља К и $\alpha \in L$. Релацијом $f(x) \to f(\alpha)$ вршимо пресликавање прстена $K[x]$ у поље L. Најмањи потпрстен поља L који садржи K и α је

$$K[\alpha] = \{f(\alpha) \mid f(x) \in K[x]\}.$$

У случају да је α алгебарски број, комутативни прстен са јединичним елементом без делитеља нуле, $K[\alpha]$, увек има и инверзни елемент сваког ненултог елемента, па је поље, и пишемо $K[\alpha] = K(\alpha)$. Прецизније, $K(\alpha)$ је најмање потпоље поља L који садржи K и α, и кажемо да настаје **адјункцијом** елемента α пољу K. Уместо само једног елемента $\alpha \in L$, може се адјунговати цели подскуп A поља L, у ознаци $K[A]$. Ако се A састоји само од алгебарских елемената онда је $K[A] = K(A)$ алгебарско проширење поља K, а ако је скуп A још и коначан, онда је $K(A)$ коначно алгебарско проширење.

Тврђење 4.5.3. (**О степену екстензије**). Нека је L проширење поља К и нека је $\alpha \in L$ алгебарски елемент над K степена n. Тада је минимални потпрстен $K(\alpha)$ поља L који садржи K и α, коначно проширење поља K екстензије $[K(\alpha)\ : K] = n$.

Пример. Нека је $K = \mathbb{Q}$ и $L = \mathbb{C}$.

a) Посматрајмо полином $f(x) = x^2 - 2 \in K[x]$. Полином $f(x)$ је ненулти, нормиран и несводљив над K, на основу Ајзенштајновог критеријума за $p = 2$, његов корен је $\alpha = \sqrt{2}$. Зато је $f(x)$ минимални полином елемента α над K, чији је степен 2. База векторског простора $K(\sqrt{2})$ над K је $\{1, \sqrt{2}\}$. Односно $K(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in K\}$.

b) Посматрајмо полином $f(x) = x^2 + 1 \in K[x]$. Полином $f(x)$ је ненулти, нормиран и несводљив над K, његов корен је $\alpha = i$. Зато је $f(x)$ минимални полином елемента α над K, чији је степен 2. База векторског простора $K(i)$ над K је $\{1, i\}$. Односно $K(i) = \{a + bi \mid a, b \in K\}$.

c) За полином $f(x) = x^3 - 2x + 6 \in K[x]$. Полином $f(x)$ је ненулти, нормиран и несводљив над K, на основу Ајзенштајновог критеријума за $p = 2$, и према основном ставу алгебре он мора имати бар један корен α у L Зато је $f(x)$ минимални полином елемента α над K, чији је степен 3. База векторског простора $K(\alpha)$ над K је $\{1, \alpha, \alpha^2\}$. Односно $K(\alpha) = \{a + b\,\alpha + c\,\alpha^2 \mid a, b, c \in K\}$.

Поље разлагања

Како смо већ рекли, ако је L проширење поља К и $\alpha \in L$ алгебарски елемент, онда постоји нормирани несводљиви полином из $K[x]$ чија је једна нула α. Међутим, да ли за сваки нормирани несводљиви полином из $K[x]$ постоји проширење L поља К који садржи бар једну нулу тог полинома? На основу **Кронекерове теореме** долазимо до закључка да постоји такво проширење L. Односно, ако једна од нула $\alpha' \in L'$, онда постоји изоморфизам поља $\varphi: K[\alpha] \to K[\alpha']$, тако да $\varphi(\alpha) = \alpha', \varphi(a) = a, a \in K$. Долазимо до закључка да постоји проширење L поља K које садржи све нуле несводљивог полинома степена n из $K[x]$, односно вреди $f(x) = a_0 \prod_{i=0}^{n}(x - \alpha_i) \in L[x]$ и такво L се назива **поље разлагања** полинома $f(x)$ у односу на K.

Нормално проширење

Теорема 4.5.4. Коначно проширење L поља K је **нормално проширење** поља K, ако и само ако је L поље разлагања неког полинома $f(x) \in K[x]$ у односу на K.

Пример 4.5.5. Нека је $K = Q$ поље рационалних бројева, а $f(x) = x^4 - 2 \in K[x]$. Примећујемо да је $f(x)$ несводљив (на основу Ајзенштајновог критеријума за $p = 2$).

Коначно проширење L поља K јесте $L = K[\sqrt{2}]$, $f(x) = (x^2 - \sqrt{2})(x^2 + \sqrt{2})$, и то је поље разлагања полинома $g(x) = x^2 - 2 \in K[x]$, јер поред нуле $\sqrt{2}$ садржи и $-\sqrt{2}$. Зато је L коначно и нормално проширење поља K.

Посматрајмо полином $h(x) = (x^2 - \sqrt{2}) = (x - \sqrt[4]{2})(x + \sqrt[4]{2}) \in L[x]$. Коначно проширење M поља L јесте $M = L[\sqrt[4]{2}] = K[\sqrt[4]{2}]$ и то је поље разлагања полинома $h(x)$ у односу на L. Зато је M коначно и нормално проширење поља L.

Поље M садржи корене $\pm\sqrt[4]{2}$ полинома $f(x) = x^4 - 2 \in K[x]$, али не садржи $\pm\sqrt[4]{2}i$, па због тога није нормално проширење поља K.

Закључак: Нормално проширење нормалног проширења не мора бити нормално проширење полазног поља.

Релативни мономорфизам

Дефиниција 4.5.6. (**Релативни мономорфизам**). Нека су L и M два проширења поља K. Изоморфизам $\varphi: L \to M$ зове се *релативни мономорфизам* у односу на К, ако вреди $\varphi: a \to a,\ a \in K$. Ако постоји релативни мономорфизам $\varphi: L \to M$ у односу на К, онда су L и M еквивалентна проширења.

Лема 4.5.7. Нека је L алгебарско проширење поља K, а M алгебарски затворено поље.Тада се сваки мономорфизам $\varphi_0: K \to M$ може продужити до мономорфизма $\varphi: L \to M$. Ако је $L = K[\alpha]$ једноставно алгебарско проширење поља K, тада тих проширења има управо онолико колико минимални полином $f(x) \in K[x]$ елемента α у односу на K има различитих нула (у неком свом пољу разлагања).[23]

Сепарабилно проширење

Дефиниција 4.5.8. (**Сепарабилно проширење**). Нека је L проширење поља K. За елемент $\alpha \in L$ кажемо да је сепарабилан над K ако је α алгебарски елемент над K, а осим тога минимални полином $f_\alpha(x) \in K[x]$ елемента α у односу на K има само једноструке нуле. L је *сепарабилно проширење* поља K ако је сваки елемент $\alpha \in L$ сепарабилан над K.

Теорема 4.5.9. Коначно проширење L поља K је сепарабилно ако и само ако постоји управо $[L : K]$ релативних мономорфизама $\varphi: L \to \overline{L}$.[24]

[23] Дефиниција 4.5.8. и Лема 4.5.9. узете из В. Перић, *Алгебра II*

[24] Дефиниција 4.5.10. и Теорема 4.5.11. узето из .В. Перић, *Алгебра II*

Галоаова теорија

Ако је поље L проширење поља K, онда се подгрупа групе $Aut(K)$ са доменом $\{\sigma \in Aut(K) \mid \sigma|_K = i_K\}$ зове група Галоа и означава са $Gal(L/K)$. Другим речима, то је група свих релативних аутоморфизама поља L у односу на поље K. Нека је G подгрупа групе $Gal(L/K)$ поље инваријаната је $L_G = \{\alpha \in L \mid \sigma(\alpha) = \alpha, \forall\sigma \in G\}$ и то је домен међупоља $K \subset L_G \subset L$. Ако је L проширење коначно, нормално и сепарабилно проширење поља K тада је $G = Gal(L/K)$ коначна и вреди $|Gal(L/K)| = [L : K]$ и $K = L_G$.

Напомена. Ниједан од услова нормалности и сепарабилности не сме бити изостављен. На пример, $\left[\mathbb{Q}\left(\sqrt[3]{2}\right) : \mathbb{Q}\right] = 3$, али $\left|Gal\left(\mathbb{Q}\left(\sqrt[3]{2}\right)/\mathbb{Q}\right)\right| = 1$.Ово проширење поља $\mathbb{Q}$ није нормално проширење јер садржи само једну нулу несводљивог полинома $x^3 - 2 \in \mathbb{Q}[x]$. Полином $x^3 - 2$ је сепарабилан.

Лема 4.5.10. Нека је K поље карактеристике p, а n природан број, такав да $p \nmid n$ (p може бити нула). Ако је L поље разлагања полинома $x^n - 1$ над K тј. поље деобе круга на n једнаких делова, тада је група $Gal(L/K)$ изоморфна подгрупи групе $(\{l \mid 1 \leq l < n, (k,n) = 1\}, \cdot_n)$.

Доказ. Полином $x^n - 1$ је сепарабилан (његов извод је nx^{n-1}, с обзиром да важи $p \nmid n$, па је $(x^n - 1, nx^{n-1}) \sim 1$), а скуп свих његових нула је домен подгрупе мултипликативне групе поља L. Та подгрупа је циклична и реда n. Примењујући знање о цикличним групама добијамо да, ако је ξ један генераторни елемент те групе (значи $L = K[\xi]$), онда су елементи групе $Gal(L/K)$ одређени сликом елемента ξ, а то опет мора бити генераторни елемент дате цикличне групе (ако $\sigma \in Gal(L/K)$ и $\sigma(\xi) = \xi^i$, тада и ξ и ξ^i имају исти мултипликативни ред). Према томе, елементи групе $Gal(L/K)$ су облика σ_l, где је $1 \leq l < n, (k,n) = 1$ и $\sigma_l(\xi) = \xi^l$. Коресподенција $\sigma_l \to l$ је инјективно пресликавање (утапање) групе $Gal(L/K)$ у групу $(\{l \mid 1 \leq l < n, (k,n) = 1\}, \cdot_n)$.

Група $Gal(L/K)$ је Абелова јер је група $(\{l \mid 1 \leq l < n, (k,n) = 1\}, \cdot_n)$ Абелова, па је таква и њена подгрупа која је изоморфна са $Gal(L/K)$. Група $(\{l \mid 1 \leq l < n, (k,n) = 1\}, \cdot_n)$ је циклична ако је n прост број, па је циклична и свака њена подгрупа, па и група $Gal(L/K)$.

4.6. Примитивни n-ти корени из јединице

Једначина $x^n - 1 = 0$ дели јединични круг на nједнаких делова и има n решења изражених тригонометријским функцијама. У наставку ћемо се бавити алгебарским решењима ове једначине. Као што је већ речено поред броја 1, остала решења једначине $x^n - 1 = 0$ су n-ти корени из јединице

$$\xi_k = cos\frac{2k\pi}{n} + isin\frac{2k\pi}{n}, k = 1, 2, \dots, n-1.$$

Нека је ξ n-ти корени из јединице, тада је ред броја ξ, у ознаци $ord(\xi)$, најмањи број $k \in \mathbb{N}$ такав да важи $\xi^k = 1$, док за сваки $m \in \mathbb{Z}$ важи $\xi^m = 1$ ако и само ако $k \mid m$ (одакле добијамо да $k \mid n$). Посматрано ξ је примитиван n-ти корени из јединице ако је $k = n$ и тада је скуп $\{\xi^0, \xi^1, \dots, \xi^{n-1}\}$ скуп n-тих корена из јединице. На тај начин су n-ти корени из јединице генерисани, познавањем једног примитивног корена. Коначно долазимо до веома битног закључка који ће нам служити у каснијим доказима.

Лема 4.6.1. Нека је ξ примитивни n-ти корени из јединице. Тада је и ξ^a примитивни n-ти корени из јединице ако и само ако је $(n, a) = 1$.

Доказ. Нека је $ord(\xi^a) = d$. Тада је $\xi^{ad} = 1$ ако и само ако $n \mid ad$. Нека важи $(n, a) = 1$, тада добијамо да $n \mid d$. одакле следи да је $d = 0$ или $d \geq n$. То значи да је ред елемента ξ^a једнак n, па је ξ^a примитиван корен.
С друге стране, ако је $(n, a) = l$, $l > 1$, и нека је $n = l \cdot n_1$ и $a = l \cdot a_1$ тако да је $(n_1, a_1) = 1$. Тада имамо $(\xi^a)^{n_1} = (\xi^{la_1})^{n_1} = (\xi^{ln_1})^{a_1} = (\xi^n)^{a_1} = 1^{a_1} = 1$, те добијамо да је ред елемента ξ^a највише реда $n_1 < n$, па није примитивни корен, где долазимо до контрадикције и да важи $(n, a) = 1$.

Дакле, примитивних n-тих корена из јединице има управо онолико колико у низу 1, 2, 3, ..., n природних бројева који нису већи од n има оних који су релативно прости са n. Овим закључујемо да управо, добро позната, Ојлерова функција, $\varphi(n)$, броји примитивне n-те корене. Присетимо се, $\varphi(n) \stackrel{\text{def}}{=} |\{a \mid 1 \leq a < n, (a, n) = 1\}|$. За канонски облик броја $n = {p_1}^{\alpha_1} \cdot \dots \cdot {p_k}^{\alpha_k}$, Ојлерова функција гласи $\varphi(n) = n \cdot \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right)$.

Дефиниција 4.6.2. Нека је n произвољан природан број. Тада n-тим циклотомичним полиномом називамо моничан полином чији су корени примитивни n-ти корени из јединице (и притом нема двоструких нула)

$$\Phi_n(x) = \prod_{\substack{1 \leq i < n \\ (i,n)=1}} \left(x - \xi^i\right)$$

Одавде следи да је $x^n - 1 = \prod_{d|n} \Phi_d(x)$.

Из

$$\Phi_1(x) = x - 1 \text{ и } x^2 - 1 = \Phi_1(x)\Phi_2(x) = (x-1)\Phi_2(x)$$

добијамо да је $\Phi_2(x) = x + 1$.

Поступак је аналоган за израчунавање $\Phi_n(x)$ за $n > 2$.

V АЛГЕБАРСКА АНАЛИЗА КОНСТРУКЦИЈА ПРАВИЛНИХ ПОЛИГОНА

5.1. Циклотомијска једначина

Проблем конструкције правилног полигона са n-страна своди се на решавање једначине поделе круга $x^n - 1 = 0$, која је у XVII веку названа циклотомијском једначином.

Теорема 5.1.1. Правилан n-тоугао се може конструисати лењиром и шестаром ако и само ако се једначина $x^n - 1 = 0$ може решити низом линеарних и квадратних једначина.

Гаус је први одредио за које n је могуће решити циклотомијску једначину помоћу низа квадратних једначина и то је објавио 1801. године у седмом делу својих „Аритметичких расправа". Тиме је геометријски проблем сведе на алгебарско решење (решење у форми радикала).

Много је једноставније наћи комплексна решења циклотомијске једначине, тачније факторисати је над комплексним бројевима. У том случају бавимо се конструкцијама правилних полигона уписаних у јединични круг, чија темена представљају комплексна решења једначине $z^n - 1 = 0$, изражена тригонометријским обликом и притом је једно теме у тачки $(1,0)$. Поред броја 1, остала решења једначине $z^n - 1 = 0$ су n-ти корени из јединице (сл. 46)

$$\xi_k = cos\frac{2k\pi}{n} + isin\frac{2k\pi}{n}, k = 1, 2, \dots, n-1. \qquad (5.1)$$

Када је k узајамно просто са n добија се примитиван n-ти корен из јединице, најчешће се користи за $k = 1$.

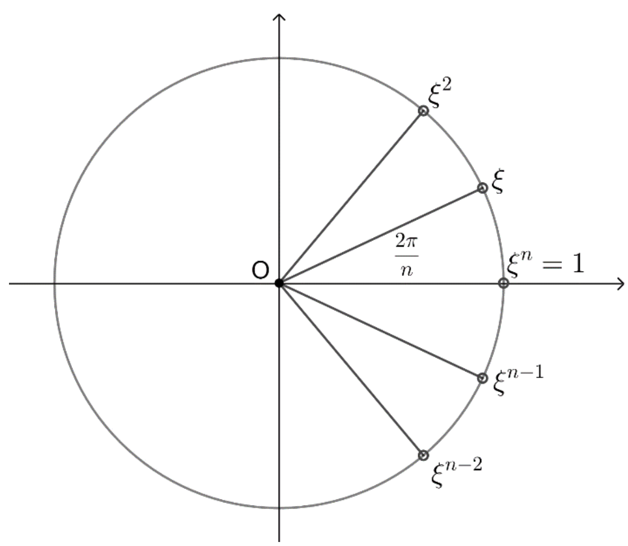
Да бисмо боље разумели (5.1) присетимо се степеновања тригонометријског облика комплексног броја $z = r(cos\varphi + isin\varphi)$, тј. чувене Моаврове формуле

$$z^n = r^n(cos\, n\varphi + i\, sin\, n\varphi). \qquad (5.2)$$

Будући да посматрамо комплексне бројеве на јединичном кругу, тј. чија је апсолутна вредност $|z| = r = 1$, из (5.2) следи да је $z^n = cos\, n\varphi + i\, sin\, n\varphi$, што са $z^n = 1$, даје $cos\, n\varphi + i\, sin\, n\varphi = 1$. Из $cos\, n\varphi = 1$ следи да је

$$n\varphi = 0, 2\pi, 4\pi, \dots,$$

а одавде да је $\varphi = 0, \frac{2\pi}{n}, \frac{4\pi}{n}, \dots$



Сл. 46. Примитивни n-ти корен из јединице

Дакле, сваки корен цикличне једначине је облика (5.1).

Приметимо, n-те корене из јединице можемо приказати и као степене $\xi^0, \xi^1, \dots, \xi^{n-1}$ примитивног корена $\xi = cos\frac{2\pi}{n} + isin\frac{2\pi}{n}$ за $k = 1$. Важно је истаћи још да је

$$\xi^{n-k} = \xi^{-k} = cos\frac{2k\pi}{n} - isin\frac{2k\pi}{n}, \text{ дакле } \xi_{n-k} = \overline{\xi_k} \text{ за } k = 0,1,2,\dots,n-1. \qquad (5.3)$$

Како је

$$x^n - 1 = (x-1)(x^{n-1} + x^{n-2} + \cdots + x + 1)$$

проблем конструкције правилних полигона се своди на решавање једначине

$$x^{n-1} + x^{n-2} + \cdots + x = -1.$$

5.2. Алгебарска анализа конструкције правилног троугла и правилног четвороугла

Пре него што почнемо анализирати циклотомијску једначину за одређени полигон, присетимо се да је дужина странице s_n правилног n-тоугла уписаног у јединични круг

$$s_n = 2 \cdot sin\frac{\pi}{n}.$$

За $n = 3$, правилни полигон је једнакостранични троугао и вреди $s_3 = 2 \cdot sin60°$, односно $s_3 = \sqrt{3}$. За $n = 4$, правилни полигон је квадрат и вреди $s_4 = 2 \cdot sin45°$, односно $s_4 = \sqrt{2}$. На овај начин видимо решивост конструкција правилног троугла и четвороугла лењиром и шестаром ($\sqrt{3}$ и $\sqrt{2}$ су конструктибилни бројеви).

Користећи познату формулу $1 - cos\,\alpha = 2 \cdot sin^2\frac{\alpha}{2}$, долазимо до дужина страница $2n$-тоугла уписаног у јединични круг. Из

$$1 - \sqrt{1 - sin^2\frac{\pi}{2}} = 2 \cdot sin^2\frac{\pi}{2n},$$

добијамо

$$2 - \sqrt{4 - {s_n}^2} = {s_{2n}}^2$$

те следи

$$s_{2n} = \sqrt{2 - \sqrt{4 - {s_n}^2}}. \qquad (5.4)$$

5.3. Алгебарска анализа конструкције правилног петоугла

Темена правилног петоугла добијају се као решења циклотомијске једначине $z^5 - 1 = 0$. Према досадашњем излагању пети корени јединице морају задовољавати

$$z^4 + z^3 + z^2 + z = -1.$$

Из (5.3) добијамо да је $\xi^4 = \xi^{-1}, \xi^3 = \xi^{-2}$, па горњу једначину можемо записати у облику

$$\xi + \xi^{-1} + \xi^2 + \xi^{-2} + 1 = 0.$$

Уврстимо ли смену $\xi + \xi^{-1} = y$, одакле је и $\xi^2 + \xi^{-2} = y^2 - 2$, па добијамо једначину

$$y^2 + y - 1 = 0. \tag{5.5}$$

Корени једначине (5.5) су $y_{1,2} = \frac{-1\pm\sqrt{5}}{2}$. Када уврстимо y_1 у $\xi + \xi^{-1} = y$ добијамо да је

$$\xi = \frac{1}{4}(\sqrt{5} - 1 + i\sqrt{10 + 2\sqrt{5}}) \tag{5.6}$$

Како је већ установљено, вреди

$$\xi = cos\frac{2\pi}{5} + isin\frac{2\pi}{5}. \tag{5.7}$$

Из (5.6) и (5.7) добијамо да је

$$cos\frac{2\pi}{5} = \frac{\sqrt{5} - 1}{4} \tag{5.8}$$

што представља координату подножја нормале ξ на x -осу, чиме је решен проблем конструкције правилног петоугла.

Приметимо још,

$$y = \xi + \xi^{-1} = 2cos\frac{2\pi}{5} = 2\sin\left(\frac{\pi}{2} - \frac{2\pi}{5}\right) = 2sin\frac{\pi}{10} = s_{10}.$$

Једначина (5.5) има два корена, позитиван и негативан. Позитиван корен нам даје дужину странице правилног десетоугла, одакле се лако добија дужина странице правилног петоугла користећи (5.4)

$${s_5}^2 = \frac{1}{4}\left(10 - 2\sqrt{5}\right) = 1 + {s_{10}}^2.$$

Према томе, вреди (3.3), тј. да је страница правилног петоугла хипотенуза правоугла троугла чија је једна катета страница правилног десетоугла, а друга катета је јединична дуж (погледати конструкцију правилног петоугла на слици 37ч).

5.4. Алгебарска анализа конструкције правилног седмоугла

Решивост конструкције правилног седмоугла своди се на решивост једначине

$$z^6 + z^5 + z^4 + z^3 + z^2 + z = -1.$$

Примењујући (5.3) добијамо да је $\xi^6 = \xi^{-1}, \xi^5 = \xi^{-2}, \xi^4 = \xi^{-3}$, горња једначина постаје

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

Уводимо смену $\xi + \xi^{-1} = y$, одакле је $\xi^2 + \xi^{-2} = y^2 - 2$ и $\xi^3 + \xi^{-3} = y^3 - 3y$ па добијамо једначину

$$y^3 + y^2 + 2y - 1 = 0. \tag{5.9}$$

На основу теореме 4.4.7. добијамо да ако кубна једначина (5.9) има рационални корен $\alpha = \frac{p}{q}$, онда мора важити да и p и q деле број 1, одакле добијамо да је $\alpha = \pm 1$. Будући да ни 1 ни -1 нису корени једначине (5.9) закључујемо да она нема рационалних решења. Најзад, према тврђењу 4.4.8, ова једначина нема ни конструктибилне корене. То значи да се број $cos\frac{2\pi}{7}$ не може изразити квадратним радикалним изразом.

5.5. Алгебарска анализа конструкције правилног деветоугла

Решење проблема конструкције правилног деветоугла шестаром и лењиром је аналогно решењу конструкције правилног седмоугла.

Ако је ξ девети корен јединице, онда је ξ^3 трећи корен јединице. Дакле вреди

$$(\xi^3)^2 + \xi^3 + 1 = 0, \text{ тј. } \xi^6 + \xi^3 + 1 = 0.$$

Из (5.3) добијамо да је $\xi^6 = \xi^{-3}$, горња једначина постаје

$$\xi^3 + \xi^{-3} + 1 = 0.$$

Уводимо смену $\xi + \xi^{-1} = y$, добијамо да је $\xi^3 + \xi^{-3} = y^3 - 3y$ одакле добијамо

$$y^3 - 3y + 1 = 0. \tag{5.10}$$

Аналогно као у случају правилног седмоугла, примењујући теорему 4.4.7. и тврђење 4.4.8. на (5.10) долазимо до закључка да конструкција правилног деветоугла лењиром и шестаром није могућа.

VI РЕШИВОСТ КОНСТРУКЦИЈА ЛЕЊИРОМ И ШЕСТАРОМ

6.1. Уводни део

При решавању конструктивних задатака користимо се разним методама геометријског конструисања. Једно од основних питања јесте: Које се конструкције могу решити помоћу лењира и шестара? У елементарној геометрији не постоји алгоритам којим би се, у општем случају, могло одредити који се конструктивни задатак може решити помоћу лењира и шестара, а који не. Одговор на ово питање добија се применом аналитичке геометрије, уз теорију алгебарских једначина. Коришћењем теорије алгебарских једначина утврђено је да се шестаром и лењиром могу извести само оне конструкције које се своде на алгебарске једначине чија се решења добијају вршењем рационалних операција и извлачењем квадратног корена коначан број пута. Вратимо се на аглебарску методу конструкције и страну 18. где смо представили конструкцију дужи x ако су задате дужи a и b тако да је $x = a - b$, $x = a - b$, $x = \frac{a}{b}$, $x = \sqrt{ab}$, користили смо рационалне операције и кореновање. Дакле, дуж дужине x се може конструисати ако је x конструктибилан број. Дуж је одређена двема крајњим тачкама, односно координатама тих тачака. Узимајући да је у равни дат Декартов правоугли координатни систем и тачка $E(1,0)$, где дуж OE представља јединичну дуж. Лако је увидети да се сваки конструктивни проблем може свести на одређивање тражених тачака, полазећи од коначног скупа тачака у равни. Јасно, ако је задата нека тачка $A(a, b)$ онда можемо конструисати сваку тачку чије координате леже у пољу $\mathbb{Q}(a, b)$.

Анализирајући елементарне конструкције (са стране 3):
I Избор произвољне тачке унутар датог дела равни.
II Конструкција праве која пролази кроз две већ изабране тачке или конструисане тачке.
III Конструкција круга коме је изабран или конструисан центар и тачка на периферији.
IV Одређивање тачке пресека две већ конструисане праве или конструисане праве са конструисаним кругом или два конструисана круга.

Имајући у виду да се праве у равни представљају једначинама првог степена са две променљиве

$$Ax + By + C = 0,$$

а круг квадратном једначином са две непознате

$$Ax^2 + Bxy + Ay^2 + Cy + D = 0,\ A \neq 0,\ B^2 + C^2 - 4AD > 0$$

долазимо до закључка да се свака конструкција лењиром и шестаром, тј. помоћу правих и кругова, може свести на решавање низа линеарних и квадратних једначина.

Детаљније, ако се у равни уведе координатни систем, тада свакој линији одговара једна једначина са две непознате, а пресеку двеју линија одговара решење система од две једначине којима су представљене те линије и обрнуто, сваком систему од две једначине са две непознате одговара пар линија које ће се сећи или не, већ према томе да ли тај систем има или нема решење.

Лема 6.1.1. Ако је $P(\alpha, \beta)$ конструктибилна тачка, онда је $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}] = 2^k$, за $k \geq 0$ (k је ненегативан цели број).

Доказ. Због једноставнијег записа убудуће ћемо писати $\mathbb{Q}(P)$.

Нека су се у процесу добијања тачке P јављале елементарном конструкцијом IV редом тачке P_1,..., $P_n = P$, где је $P_i = (\alpha_i, \beta_i)$. Индукцијом по n ћемо показаћети да је степен екстензије $[\mathbb{Q}(P_1, \ldots, P_n) : \mathbb{Q}]$ степен броја два.

Случај $n = 1$ је обрађен у прелазу из k у $k + 1$. Претпоставимо да је $[\mathbb{Q}(P_1, \ldots, P_{k-1}) : \mathbb{Q}]$ степен броја 2. Тачка P_k је добијена пресеком или две праве, или праве и круга или два круга. Праве су одређене тачкама са координатама из $\mathbb{Q}(P_1, \ldots, P_{k-1})$, кругови су одређени центром чије су координате из $\mathbb{Q}(P_1, \ldots, P_{k-1})$и полупречником једнаким растојању двеју тачака са координатама из $\mathbb{Q}(P_1, \ldots, P_{k-1})$.

Ако су дате две тачке $A(\gamma_i, \delta_i)$ и $B(\gamma_j, \delta_j)$, једначина праве кроз њих је

$$y - \delta_i = \frac{\delta_j - \delta_i}{\gamma_j - \gamma_i}(x - \gamma_i). \tag{6.1}$$

Ако је круг са центром у тачки (γ_s, δ_s) и полупречником једнаким растојању тачака (γ_r, δ_r) и (γ_t, δ_t), његова једначина је

$$(x - \gamma_s)^2 + (y - \delta_s)^2 = (\gamma_r - \gamma_t)^2 + (\delta_r - \delta_t)^2. \tag{6.2}$$

Ако је тачка P_k пресек две праве типа (6.1), тј. пресек две праве у чијим једначинама су коефицијенти из $\mathbb{Q}(P_1, \ldots, P_{k-1})$, онда су њене координате такође у пољу $\mathbb{Q}(P_1, \ldots, P_{k-1})$, односно $\mathbb{Q}(P_1, \ldots, P_{k-1}) = \mathbb{Q}(P_1, \ldots, P_{k-1}, P_k)$. У том случају се решава систем од две линеарне једначине које су одређене тим правама. Ако систем има једно решење праве се секу, ако има бесконачно много решења праве се поклапају, а ако нема решења праве су паралелне. За решавање овог система користе се сабирање, одузимање, множење и дељење.

Ако је тачка P_k пресек праве типа (6.1) и круга типа (6.2) тј. пресек линија у чијим једначинама су коефицијенти из $\mathbb{Q}(P_1, \ldots, P_{k-1})$, онда су њене координате или у пољу $\mathbb{Q}(P_1, \ldots, P_{k-1})$ или неком проширењу тог поља степена екстензије 2. У том случају се после елиминације једне променљиве решавање своди на решавање једне квадратне једначине са једном непознатом (ту квадратну једначину ћемо означити са (*) ради, на даље, лакшег праћења текста). Решавање квадратне једначине (*) поред рационалних операција, у случају када дискриминанта није потпун квадрат, захтева и извлачење квадратног корена.

Ако је дискриминанта негативна тада се праве и круг не секу. Јасно, када је дискриминанта потпун квадрат, решење се налази у пољу коефицијената и добија се, као и у претходном случају, да важи $\mathbb{Q}(P_1, \dots, P_{k-1}) = \mathbb{Q}(P_1, \dots, P_{k-1}, P_k)$. Ако дискриминанта није потпун квадрат, тада је

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

где су a, b, c коефицијенти квадратне једначине (*) добијени примењивањем рационалних операција на коефицијенте једначина посматране праве и круга (коришћена су латинична слова a, b, c уместо слова алфабета због једноставније нотације). Дакле, пољу коефицијената $\mathbb{Q}(P_1, \dots, P_{k-1})$ се адјунгује број $\sqrt{D}$, степен екстензије

$$[\mathbb{Q}(P_1, \dots, P_{k-1}) : \mathbb{Q}(P_1, \dots, P_{k-1}, P_k)] = 2,$$

јер је полином $x^2 - D = 0$ минимални полином за $\sqrt{D}$, који је несводљив над $\mathbb{Q}(P_1, \dots, P_{k-1})$, јер ако би био сводљив тада би $\sqrt{D}$ припадао пољу $\mathbb{Q}(P_1, \dots, P_{k-1})$.

Коначно, ако је тачка P_k добијена пресеком два круга типа (6.2), одређивање решења система се своди на претходни случај. Поново ћемо, ради боље прегледности, уместо слова алфабета користити латинична слова. Нека је, дакле, тачка P_k, пресек кругова

$$k_1 \colon a_1(x^2 + y^2) + b_1 x + c_1 y + d_1 = 0$$
$$k_2 \colon a_2(x^2 + y^2) + b_2 x + c_2 y + d_2 = 0,$$

где је $a_1 a_2 \neq 0$. Ако се прва једначина помножи са a_2, друга a_1 и једначине се одузму тада је

$$(a_2 b_1 - a_1 b_2)x + (a_2 c_1 - a_1 c_2)y + a_2 d_1 - a_1 d_2 = 0,$$

па се решење своди на решавање ове линеарне једначине и једначине једног од два круга, тј. на претходни случај.

Пример 6.1.2. (**Проблем удвостручавања коцке**) Ако је дата коцка чије су странице дужине 1, да ли је конструктибилна тачка $(\alpha, 0)$ за коју важи $\alpha^3 = 2$ (коцка са страницама α која има дупло већу запремину од полазне)?

Доказ. Како је $\alpha = \sqrt[3]{2}$ и како је $\left[\mathbb{Q}\left(\sqrt[3]{2}\right) \colon \mathbb{Q}\right] = 3$ (јер је полином $x^3 - 2 \in Q[x]$ несводљив према Ајзенштајновом критеријуму), одговор је, према претходној леми, одричан, јер није степен двојке. Наравно, исто би било и да смо за дужину странице полазне коцке узели ма који други позитиван рационални број.

Пример 6.1.3. (**Квадратура круга**) Да ли је могуће конструисати квадрат чија је површина једнака површини круга полупречника 1?

Доказ. Ако за једно теме траженог квадрата узмемо координатни почетак, а за остале $(\alpha, 0)$, $(0, \alpha)$ и (α, α), видимо да је $\alpha = \sqrt{\pi}$. Како је π трансцедентан број, трансцедентан је и $\sqrt{\pi}$, дакле $[\mathbb{Q}(\sqrt{\pi}):\mathbb{Q}] = \infty$, што према претходној леми поново значи да је немогуће конструисати.

Сада се намеће питање: Да ли се овај проблем може посматрати из супторног смера?

Теорема 6.1.4. Нека је дата тачка $P(\alpha, \beta)$. Ако поље $\mathbb{Q}(\alpha, \beta)$ садржи низ потпоља

$$\mathbb{Q} = K_0 \subset K_1 \subset \cdots \subset K_{n-1} \subset K_n = \mathbb{Q}(\alpha, \beta)$$

где је $[K_{n-1} : K_n] = 2, i = 1, \dots, n$, онда је тачка $P(\alpha, \beta)$ конструктибилна.

Доказ. Доказаћемо индукцијом по n. Случај $n = 0$ је тривијалан, тада су координате тачке P рационални бројеви. Претпоставимо да су све тачке поља K_{i-1} конструктибилне. Како је $[K_i : K_{i-1}] = 2$, то је, за ма које $\gamma \in K_i \setminus K_{i-1}$, $K_i = K_{i-1}(\gamma)$. Нека је

$$p(x) = x^2 + ax + b = \left(x + \frac{1}{2}a\right)^2 + b - \frac{1}{4}a^2$$

минимални полином елемента γ над K_{i-1}.

Ако је $\delta = \gamma + \frac{1}{2}a$, тада је $\delta^2 = \gamma^2 + a\gamma + b + \frac{1}{4}a^2 - b = \frac{1}{4}a^2 - b$. Према томе δ^2 је ненегативан елемент поља K_{i-1}, а $K_i = K_{i-1}(\gamma) = K_{i-1}(\delta)$. С обзиром да је тачка $(\delta^2, 0)$ конструктибилна, консруктибилне су и тачке $(\pm\delta, 0)$, $(\pm\gamma, 0)$.

Тврђење 6.1.5. Нека је дата тачка $P(\alpha, \beta)$. Ако је поље $\mathbb{Q}(\alpha, \beta)$ нормално проширење поља $\mathbb{Q}$ такво да $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}] = 2^k$ (за неки ненегативан цели број k), онда је тачка P конструктибилна.

Доказ. Нека је $\mathbb{Q}(\alpha, \beta)$ нормално проширење поља $\mathbb{Q}$. Јасно, у питању је и сепарабилно проширење поља $\mathbb{Q}$, па је $|Gal(\mathbb{Q}(\alpha, \beta)/\mathbb{Q})| = [\mathbb{Q}(\alpha, \beta) : \mathbb{Q}] = 2^k, k \geq 0$. Претпоставимо да је k позитивно. Од раније знамо да је група $Gal(\mathbb{Q}(\alpha, \beta)/\mathbb{Q})$ решива. Нека је

$$Gal(\mathbb{Q}(\alpha, \beta)/\mathbb{Q}) = G_0 \supset G_1 \supset \cdots \supset G_{k-1} \supset G_k = E$$

њен решиви нормални низ; дакле, фактор групе G_{i-1}/G_i су цикличне групе реда 2. Придружимо том низу одговараући низ поља

$$\mathbb{Q} = K_0 \subset K_1 \subset \cdots \subset K_{n-1} \subset K_n = \mathbb{Q}(\alpha, \beta),$$

где је K_i поље инваријаната (под)групе G_i. Како је $G_i \triangleleft G_{i-1}$, то је поље K_i нормално над пољем K_{i-1} и $|Gal(K_i/K_{i-1})| = [K_i : K_{i-1}] = |G_{i-1}/G_i| = 2$.

Пример 6.1.6. (**Проблем трисекције угла**). Ако је дат угао α са једним краком на x-оси, да ли га је могуће конструктибилно поделити на три једнака?

Доказ. Јасно, довољно је само посматрати углове унутар првог квадранта. Нека је $0° < \alpha \leq 90°$. Нацртајмо круг са центром у координатном почетку, полупречника 1, и нека је P тачка пресека тог круга са другим краком. Тачка $R(cos\alpha, 0)$ је пројекција тачке P на x-осу; она нам је, дакле, дата, другим речима у полазном пољу се налазе тачке $O(0,0)$, $I(1,0)$ и $R(cos\alpha, 0)$. Проблем трисекције угла α је решив ако и само ако је тачка $\left(cos\frac{\alpha}{3}, 0\right)$ конструктибилна над полазним пољем. Из познате тригонометријске једнакости

$$cos\alpha = cos3 \cdot \frac{\alpha}{3} = 4cos^3\frac{\alpha}{3} - 3cos\frac{\alpha}{3}$$ [25]

следи да је $cos\frac{\alpha}{3}$ нула полинома $p(x) = 4x^3 - 3x - cos\alpha \in \mathbb{Q}(cos\alpha)[x]$.

Ако је полином $p(x)$ сводљив над пољем $\mathbb{Q}(cos\alpha)$, тада је $\left[\left(\mathbb{Q}(cos\alpha)\right)\left(cos\frac{\alpha}{3}\right) : \mathbb{Q}(cos\alpha)\right]$ или 1 или 2 и тачка $\left(cos\frac{\alpha}{3}, 0\right)$ је конструктибилна над полазним пољем.

У супротном је $\left[\left(\mathbb{Q}(cos\alpha)\right)\left(cos\frac{\alpha}{3}\right) : \mathbb{Q}(cos\alpha)\right] = 3$ и тачка $\left(cos\frac{\alpha}{3}, 0\right)$ није конструктибилна над полазним пољем.

Тривијалан пример угла за који имамо трисекцију је прав угао. Пример угла за који не постоји трисекција је 60°, јер $cos60° = \frac{1}{2} \in \mathbb{Q}$, а полином $4x^3 - 3x - \frac{1}{2}$ није сводљив над пољем $\mathbb{Q}$.

6.2. Конструктибилност правилних многоуглова

Посматрамо правилни n-тоугао уписан у круг са центром у координатном почетку и полупречника 1, чије је једно теме, A_0 на x-оси. Подразумевамо и да се остала темена $A_1, \dots, A_{n-1}$ ређају у смеру супротном кретању казаљке на сату. Такав n-тоугао је конструктибилан ако и само ако је конструктибилна тачка $A_1\left(cos\frac{2\pi}{n}, sin\frac{2\pi}{n}\right)$ ако и само ако је конструктибилна тачка $A'\left(cos\frac{2\pi}{n}, 0\right)$.

Лема 6.2.1. Нека је тачка $(cos\alpha, 0)$ конструктибилна. Тада су конструктибилне и тачке, $(cos\, k\alpha, 0)$, $(sin\, k\alpha, 0)$, где $k \in \mathbb{Z}$. Ако су тачке $(cos\alpha, 0)$ и $(cos\beta, 0)$ конструктибилне, конструктибилне су и тачке $(cos(k\alpha + m\beta), 0)$ и $(sin(k\alpha + m\beta), 0)$ где $k, m \in \mathbb{Z}$.

Доказ. У првом случају, за позитивно k користимо индукцију и тригонометријске трансформације

$$cos\big((k+1)\alpha\big) = cos\, k\alpha \cdot cos\, \alpha - sin\, k\alpha \cdot sin\, \alpha$$

$$sin\big((k+1)\alpha\big) = sin\, k\alpha \cdot cos\, \alpha + sin\, \alpha \cdot cos\, k\alpha.$$

Други део следи из првог и одговарајућих релација за косинусе и синусе збира углова. Користи се још $cos(-\gamma) = cos(\gamma)$ и $sin(-\gamma) = -sin(\gamma)$.

[25] Изведено из $\cos 3\alpha = cos^3\alpha - 3cos\, \alpha sin^2\alpha$.

У циљу поједностављења нотације обележићемо у наставку угао $\frac{2\pi}{n}$ са αn.

Тврђење 6.2.2. Нека су m и n позитивни цели бројеви. Ако је правилан mn- тоугао конструктибилан, конструктибилни су и правилан m- тоугао и правилан n- тоугао.

Доказ. Ако је тачка $(cos\ \alpha_{mn}, 0)$ конструктибилна, према претходној леми конструктибилне су и тачке $(cos\ (n \cdot \alpha_{mn}), 0)$ и $(cos\ (m \cdot \alpha_{mn}), 0)$, односно тачке $(cos\ \alpha_m, 0)$ и $(cos\ \alpha_n, 0)$.

Лема 6.2.3. Ако су правилни m-тоугао и правилни n-тоугао конструктибилни, и (m,n)=1, тада је конструктибилан и правилан mn-тоугао.

Доказ. Нека су испуњени услови леме и нека је за целе бројеве r, t и $rm + tn = 1$. Онда је $\alpha_{mn} = t\alpha_m + r\alpha_n$, а пошто су тачке $(cos\ \alpha_m, 0)$ и $(cos\ \alpha_n, 0)$ конструктибилне, конструктибилна је и тачка $(cos\ t\alpha_m + r\alpha_n, 0) = (cos\ \alpha_{mn}, 0)$.

Коначно долазимо до теореме која даје потпун одговор на питање конструктибилности правилних n-тоуглова. Пре тога, поновимо да су Фермаови прости бројеви прости бројеви облика $2^{2^m} + 1$; првих неколико су $3, 5, 17, 257, 65537, \ldots$

Теорема 6.2.4. Правилан n- тоугао је конструктибилан ако и само ако је

$$n = 2^k \cdot p_1 \cdot \ldots \cdot p_r,$$

где је $k, r \geq 0$ и где су за $r > 0$ $p_1, \ldots, p_r$ различити Фермаови прости бројеви.

Доказ.
$(\Rightarrow)$ Претпоставимо да је правилан n -тоугао конструктибилан и да важи $n = 2^k \cdot {p_1}^{k_1} \cdot \ldots \cdot {p_r}^{k_r}$. Према претходном тврђењу конструктибилан је и сваки правилан ${p_i}^{k_i}$- тоугао, за $1 \leq i \leq r$. Конструктибилне су, стога, тачке $\left(cos\ \alpha_{{p_i}^{k_i}}, 0\right)$, па је према леми 6.1.1. је $\left[\mathbb{Q}\left(cos\ \alpha_{{p_i}^{k_i}}\right) : \mathbb{Q}\right]$ степен броја 2. Нека је $\xi_{{p_i}^{k_i}} = cos\alpha_{{p_i}^{k_i}} + isin\alpha_{{p_i}^{k_i}}$. Јасно, $\xi_{{p_i}^{k_i}}$ је ${p_i}^{k_i}$-корен из јединице у пољу комплексних бројева. Из

$$\xi_{{p_i}^{k_i}} + \xi^{-1}{}_{{p_i}^{k_i}} = 2cos\alpha_{{p_i}^{k_i}}$$

следи

$$\xi^2{}_{{p_i}^{k_i}} - 2\xi_{{p_i}^{k_i}} \cdot \cos \alpha_{{p_i}^{k_i}} + 1 = 0,$$

те је $\left[\mathbb{Q}\left(\xi_{{p_i}^{k_i}}\right) : \mathbb{Q}\left(cos\ \alpha_{{p_i}^{k_i}}\right)\right]$ или 1 или 2. У сваком случају је $\left[\mathbb{Q}\left(\xi_{{p_i}^{k_i}}\right) : \mathbb{Q}\right]$ степен броја 2. С друге стране, је $\xi_{{p_i}^{k_i}}$ је нула несводљивог полинома

$$\Phi_{{p_i}^{k_i}}(x) = \prod_{\substack{1 \leq r < {p_i}^{k_i} \\ (r, p_i) = 1}} \left(x - \xi^r{}_{{p_i}^{k_i}}\right)$$

степена ${p_i}^{k_i} \cdot \left(1 - \frac{1}{p_i}\right) = {p_i}^{k_i - 1} \cdot (p_i - 1)$, према Ојлеровој функцији.

Како је ${p_i}^{k_i-1} \cdot (p_i - 1)$ степен броја 2, постоје само две могућности:
$p_i = 2$ и k_i је произвољно или $k_i = 1$ и $p_i - 1$ је степен броја 2, рецимо $p_i - 1 = 2^t$, тј. $p_i = 2^t + 1$ (што значи да сви непарни степени броја n се могу појављивати само на први степен, што и јесте тражено). Закључимо, коначно, да ако t није степен броја 2, онда $2^t + 1$ није прост број. Нека је $t = l \cdot m$, где је m непаран број (јер t није степен броја 2, па мора имати непаран фактор). Тада је $x^m + 1$ дељиво са $x + 1$, знамо да је

$$x^m + 1 = (x + 1) \cdot \left(x^{m-1} + \cdots + (-1)^{j+1} x^{m-j} + \cdots + 1\right)$$

а онда је и $x^t + 1 = (x^l)^m + 1$ дељиво са $x^l + 1$ (одакле добијамо да је и $x^t + 1$ сложен број). Према закону контрапозиције добијамо да ако је $x^t + 1$ прост број, онда је t степен броја 2, односно p_i је Фермаов прост број.

($\Leftarrow$) Нека је $n = 2^k \cdot p_1 \cdot \ldots \cdot p_r$, где је $k, r \geq 0$ и где су за $r > 0$ $p_1, \ldots, p_r$ различити Фермаови прости бројеви (ако их има). Ојлерова функција је за сваки од овако назначених фактора степен броја 2:

$\varphi(2^k) = 2^{k-1}(2 - 1) = 2^{k-1}$, а ако је $p_i = 2^{2^{m_i}} + 1$, тада је

$$\varphi\left(2^{2^{m_i}} + 1\right) = \left(2^{2^{m_i}} + 1\right) - 1 = 2^{2^{m_i}}.$$

Осврнимо се на Фермаове факторе. Опет, ако је ξ_{p_i} примитивни p_i-ти корен из јединице, видимо да је $\left[\mathbb{Q}\left(\xi_{p_i}\right) : \mathbb{Q}\right]$ степен броја 2. Јасно, $\mathbb{Q}\left(\xi_{p_i}\right)$ је сепарабилна и нормална екстензија поља $\mathbb{Q}$, а група $Gal\left(\mathbb{Q}\left(\xi_{p_i}\right) / \mathbb{Q}\right)$ је решива јер јој је ред степен броја 2. Шта више, та група је и Абелова, јер је према леми 4.5.12 изоморфна подгрупи групе $\left(\{l \mid 1 \leq l < p_i\}, \cdot_{p_i}\right)$. Како су све њене подгрупе (тривијално) нормалне, то су и сва међупоља (датих поља) нормална. Посебно, $\mathbb{Q}\left(cos\alpha_{p_i}\right)$ је нормална и сепарабилна екстензија поља $\mathbb{Q}$, чији је степен екстензије степен броја 2, што имплицира и да је тачка $\left(cos\alpha_{p_i}, 0\right)$ конструктибилна, према тврђењу 6.1.5. Лема 6.2.3 завршава доказ.

Литература

[1] З.Стојаковић, *Геометријске конструкције само шестаром*, Универзитет у Новом Саду, Завод за физику и математику, Нови Сад, 1966.

[2] Ђ. Паунић, *Правилни полигони*, Друштво математичара Србије, Београд 2006.

[3] З. Лучић, *Огледи из историје античке геометрије,* Службени гласник, Београд, 2008.

[4] Д. Палман, *Геометријске конструкције*, Елемент, Загреб, 1996.

[5] З. Курник, *Конструктивне методе*, МиШ (Математика и школа – часопис за наставу математике), 30/100, стр. 195 – 201, Елемент, Загреб, 2005.

[6] З. Курник, *Алгебарска метода рјешавања конструктивних задатака*, МиШ (Математика и школа – часопис за наставу математике), 42/100, стр. 51 – 56, Елемент, Загреб, 2007.

[7] Т. Малић, *Уџбеник математике за шести разред основне школе*, Нови Логос, Београд, 2019.

[8] А. Липковски, *Елементарна алгебра I део*, Математички факултет, Београд, 2000.

[9] Б. Шешеља, А. Тепавчевић, *Алгебра 1*, Природно-математички факултет, Департман за математику и информатику, Нови Сад, 2004.

[10] F. Klein, *Elementary Mathematics from an advanced standpoint of Arithmetic, Algebra and Analysis,* Dover Publication, New York, 1945.

[11] В. Перић, *Алгебра II,* Свјетлост, Сарајево, 1980.

[12] М. З. Груловић, *Предавања из Алгебре 4 (Теорија прстена и поља и Теорија Галоа)*, Природно-математички факултет, Департман за математику и информатику, Нови Сад, 2017.

[13] М. З. Груловић, *Основи теорије група*, Институт за математику у Новом Саду, Нови Сад, 1997.

[14] Г. Војводић, *Предавања из алгебре*, Универзитет у Новом Саду, Природно-математички факултет, Нови Сад, 2007.

[15] П. Јаничић, *Збирка задатака из геометрије*, Математички факултет, Београд, 2007.

[16] П. Миличић, В. Стојановић, З. Каделбург, Б. Боричић, *Математика за први разред средње школе*, Завод за уџбенике и наставна средства, Београд, 1993.

[17] Р. Тошић, В. Петровић, *Збирка задатака из основа геометрије*, Институт за математику у Новом Саду, Нови Сад, 1982.

[18] Д. Херцег, *Математичке формуле*, Змај, Нови Сад, 2002.