Construcţii geometrice

Paul A. Blaga

Cuprins

III Constructibilitate cu rigla şi compasul **5**

1 Fundamentele teoriei constructibilităţii **7**
1.1 Puncte constructibile şi numere constructibile . . . 7
1.2 Modalităţi elementare de construire a unor obiecte constructibile . . . 9
1.3 Corpul numerelor constructibile . . . 13
1.4 Caracterizarea numerelor constructibile . . . 15
1.4.1 Extinderi de corpuri . . . 15
1.5 Teorema (sau rezultatul) lui Wantzel . . . 17
1.6 Aplicaţii ale rezultatului lui Wantzel . . . 22
1.6.1 Cuadratura cercului . . . 22
1.6.2 Dublarea cubului . . . 23
1.6.3 Trisecţiunea unghiului . . . 23
1.7 Caracterizarea corpurilor $\mathcal{C}$ şi $\mathcal{C}(i)$ . . . 25
1.8 Reciproca rezultatului lui Wantzel . . . 26

2 Poligoane regulate **29**
2.1 Poligoane regulate constructibile . . . 29
2.2 Teorema lui Gauss . . . 30
2.3 Construcţii de poligoane regulate . . . 33
2.3.1 Triunghiul echilateral, pătratul, pentagonul regulat . . . 33
2.3.2 Poligonul cu 15 laturi . . . 36

A Transcendenţa numărului π **37**

Partea III

Constructibilitate cu rigla şi compasul

CAPITOLUL 1

Fundamentele teoriei constructibilităţii

1.1 Puncte constructibile şi numere constructibile

Am lămurit, sperăm, care este semnificaţia construcţiilor cu rigla şi compasul în planul euclidian. Abordarea de până acum, pur geometrică, nu ne permite, din păcate, să precizăm care figuri geometrice se pot construi folosind, în exclusivitate, aceste două instrumente clasice. Pentru a obţine răspunsul la această întrebare, trebuie să reformulăm o problemă de construcţii într-un alt limbaj. Cel mai potrivit s-a dovedit a fi cel algebric.

Vom începe, prin urmare, acest capitol tocmai cu formularea problemei de construcţii (mai precis, formularea noţiunii de *constructibilitate*) într-un limbaj algebric. Primul pas este să dăm o definiţie (deocamdată geometrică) riguroasă a noţiunii de *punct constructibil*.

Definiţia 1.1. Fie Π planul euclidian şi $\mathcal{B} \subset \Pi$ o submulţime finită a planului, care conţine cel puţin două elemente. Elementele lui $\mathcal{B}$ se numesc *puncte de bază*. Atunci:

(a) Un punct $M \in \Pi$ se numeşte *constructibil* cu rigla şi compasul dacă există un şir finit de muncte care se termină cu M: $M_1, M_2, \ldots, M_n = M$ astfel încât pentru fiecare i, $1 \leq i \leq n$ este un punct de intersecţie

- fie a două drepte,
- fie a unei drepte şi a unui cerc,
- fie a două cercuri,

aceste drepte şi cercuri obţinându-se, pentru fiecare i, cu ajutorul mulţimii $E_i = \mathcal{B} \cup \{M_1, \ldots, M_{i-1}\}$ în modul următor:

- orice dreaptă trece prin două puncte distincte din E_i,
- fiecare cerc are centrul într-un punct din E_i, iar raza sa este egală cu distanţa dintre două puncte din E_i.

(b) O dreaptă care trece prin două puncte constructibile se numeşte *constructibilă*.

(c) Un cerc ce are centrul într-un punct constructibil şi are raza egală cu distanţa dintre două puncte constructibile se numeşte *constructibil*.

Observaţia 1. Toate *punctele de bază* din $\mathcal{B}$ sunt constructibile cu rigla şi compasul. Fie, de exemplu, $P \in \mathcal{B}$ un punct de bază. Întrucât am admis că există cel puţin două puncte de bază, rezultă că există un punct $P' \in \mathcal{B}$, $P' \neq P$. Atunci P se poate obţine ca intersecţie a dreptei PP' cu cercul de centru P' şi de rază PP', ceea ce înseamnă că P este constructibil. Cum P este un punct de bază ales la întâmplare, rezultă că *orice* punct de bază este constructibil.

Observaţia 2. De acum încolo, dacă nu se menţionează explicit altfel, pentru noi *construcţie geometrică* va însemna *construcţie geometrică realizată cu rigla şi compasul* şi nu vom mai menţiona explicit instrumentele utilizate.

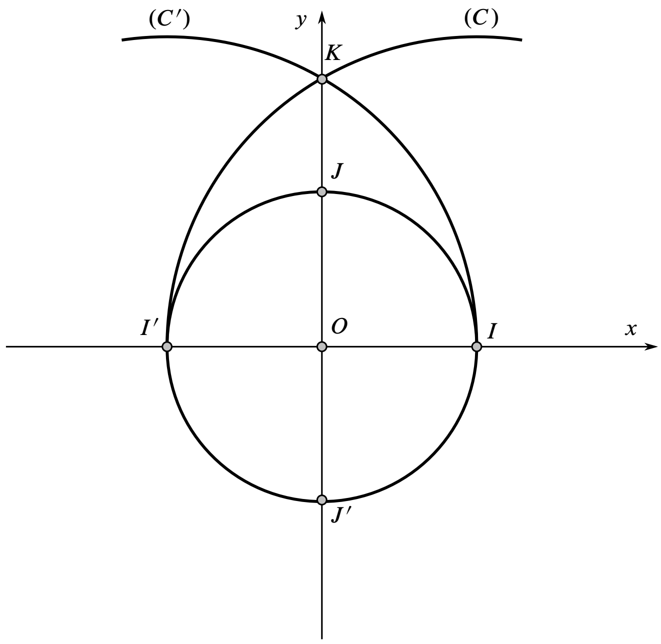

Figura 1.1

În cele ce urmează, scopul nostru este să introducem noţiunea de *număr constructibil*, alături de cea de *punct constructibil*. În acest scop, vom introduce un reper cartezian în plan, plecând de la două puncte de bază.

Mai precis, pe moment presupunem că există doar două puncte de bază, fie ele O şi I, adică $\mathcal{B} = \{O, I\}$. Vom evidenţia nişte puncte constructibile, plecând de la cele două puncte de bază.

Punctele O şi I determină dreapta OI (vezi figura 1.1). Considerăm cercul (constructibil) Γ, cu centrul în punctul O şi de rază OI. Cercul Γ intersectează dreapta OI în punctul I şi într-un al doilea punct, I', simetricul lui I faţă de punctul O. Prin urmare, punctul I' este constructibil. Vom construi acum mediatoarea segmentului II'. Pentru aceasta, considerăm, mai întâi, cercul C de centru I şi de rază II', precum şi cercul C', de centru I' şi de aceeaşi rază, II'. Notăm cu K unul dintre punctele de intersecţie dintre cele două cercuri. Evident, punctul K este constructibil, întrucât este intersecţia a două cercuri constructibile. Este uşor de demonstrat că dreapta OK este perpendiculară pe dreapta OI, deci ea este mediatoarea segmentului II'. Dreapta OK intersectează cercul Γ în două puncte, pe care le vom nota cu J şi J', ele fiind, de asemenea, constructibile.

Am pus, astfel, în evidenţă o serie de puncte constructibile: O, I, I', K, J, J'. Vom folosi unele dintre ele pentru a construi un reper ortonormat. Astfel, alegem ca unitate de lungime distanţa OI. Atunci, în mod evident, avem şi $OJ = 1$. Reperul nostru va fi $(O, \overrightarrow{OI}, \overrightarrow{OJ})$. Pentru a simplifica notaţiile, vom nota acest reper cu (O, I, J).

Avem acum tot ce ne trebuie pentru a da următoarea definiţie:

Definiţia 1.2. Un număr real se numeşte *constructibil* dacă el este una dintre coordonatele unui punct constructibil faţă de reperul ortonormat (O, I, J).

Observaţia 3. În mod normal, exprimarea corectă este că numărul real este *constructibil relativ la punctele de bază O şi I'*. Vom utiliza exprimarea prescurtată, de acum încolo.

Exemplul 1.1.1. Numerele reale $0, 1, -1$ sunt constructibile, deoarece ele sunt abscisele punctelor O, I, I'.

1.2 Modalităţi elementare de construire a unor obiecte constructibile

Propoziţia 1.1. *Dacă d este o dreaptă constructibilă, iar A este un punct constructibil, atunci perpendiculara pe d care trece prin A este, de asemenea, o dreaptă constructibilă.*

Demonstraţie. Din moment ce dreapta d este constructibilă, ea conţine cel puţin două puncte constructibile, fie ele B şi C. Considerăm cercul (evident constructibil) de centru A şi de rază AB. Acest cerc intersectează dreapta d în B şi într-un alt punct, fie el D. Construim acum două cercuri cu centrele în B şi D şi de rază BD. Aceste două cercuri se intersectează în două puncte, fie ele E şi F. Atunci dreapta AE este dreapta căutată. $\square$

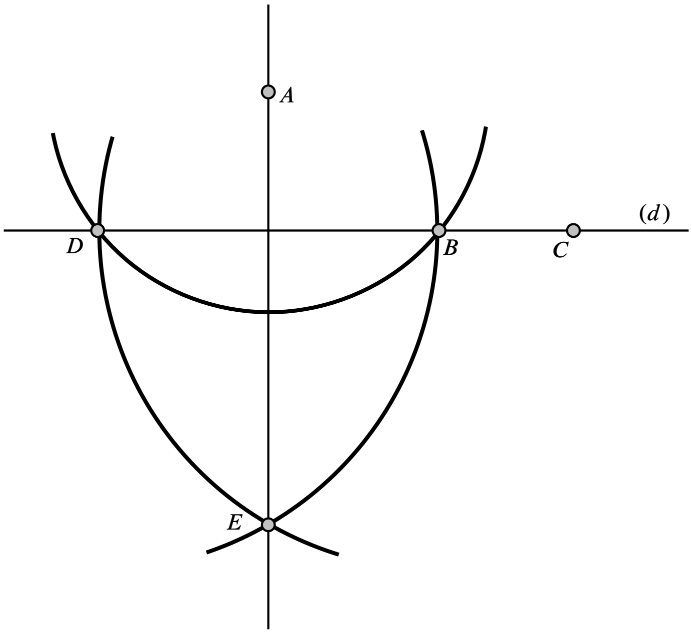

Figura 1.2

Observaţia 4. De remarcat că demonstraţia dată funcţionează doar dacă $A \neq B$. Dar dacă $A = B$, atunci, cu siguranţă, $A \neq C$, deci putem reface demonstraţia, folosind punctul C în locul punctului B.

Propoziţia 1.2. *Dacă d este o dreaptă constructibilă, iar A este un punct constructibil, care nu aparţine dreptei d, atunci paralela d' la d care trece prin A este, de asemenea, o dreaptă constructibilă.*

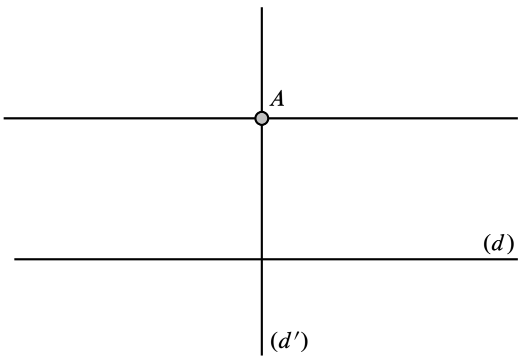

Figura 1.3

Demonstraţie. Conform propoziţiei 1.1, putem construi perpendiculara d'' care trece prin A. Atunci dreapta d' este perpendiculara care trece prin A pe dreapta d'', prin urmare, conform aceleiaşi propoziţii 1.1, este constructibilă (vezi figura 1.3). □

Propoziţia 1.3. *Dacă A şi B sunt două puncte constructibile, atunci mijlocul segmentului AB şi mediatoarea sa sunt, de asemenea, constructibile.*

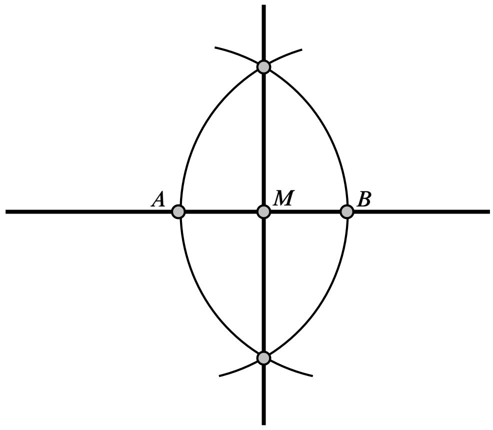

Figura 1.4

Demonstraţie. Cercurile de centre A şi B şi de raze egale cu AB sunt ambele constructibile. Cele două cercuri se intersectează în două puncte, care determină mediatoarea segmentului. Punctul de intersecţie dintre dreapta AB şi mediatoare determină mijlocul M segmentului, care este, prin urmare, constructibil (vezifigura 1.4). □

Propoziţia 1.4. *Dacă d şi d' sunt două drepte constructibile concurente, atunci bisectoarele unghiurilor formate de cele două drepte sunt, de asemenea, constructibile.*

Demonstraţie. Fie A punctul de intersecţie al dreptelor d şi d'. Considerăm cercul $(\mathcal{C})$ de centru A şi rază OI, care taie dreapta d în punctele B şi C şi dreapta d' în punctele B' şi C' (vezi figura 1.5). Considerăm, mai departe, cercurile: $(\mathcal{C}_1)$ de centru B, $(\mathcal{C}_2)$, de centru B', respectiv $(\mathcal{C}_3)$, de centru C, toate având raza OI. Cercurile $\mathcal{C}_1$ şi $\mathcal{C}_2$ se intersectează în D, iar cercurile $\mathcal{C}_2$ şi $\mathcal{C}_3$ se intersectează în E. E uşor de verificat că dreptele AD şi AE sunt bisectoarele unghiului, deci aceste bisectoare sunt constructibile. □

Propoziţia 1.5. *Un număr real t este constructibil dacă şi numai dacă punctul de pe axa Ox de abscisă t este constructibil. Analog, t este constructibil dacă şi numai dacă punctul de pe axa Oy de ordonată t este constructibil.*

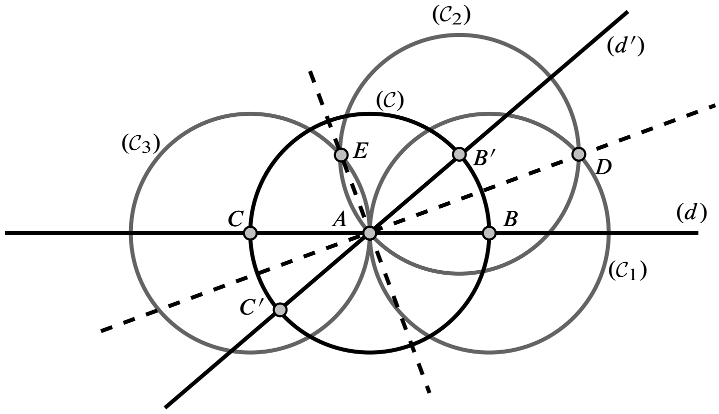

Figura 1.5

Demonstraţie. Vom face demonstraţia doar pentru afirmaţia referitoare la axa Ox, cealaltă se demonstrează în mod absolut analog (vezi figura 1.6).
($\Longrightarrow$) Dacă punctul de pe axa Ox de abscisă t este constructibil, atunci t este constructibil, din însăşi definiţia unui număr constructibil.

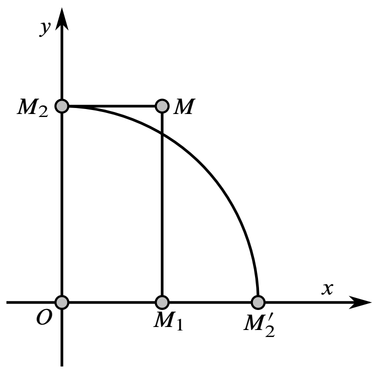

Figura 1.6

($\Longleftarrow$) Dacă t este un număr constructibil, atunci el este una dintre coordonatele unui punct constructibil M. Atunci proiecţiile M_1 şi M_2 ale lui M pe axa Ox, respectiv pe axa Oy, sunt constructibile, conform propoziţiei 1.1. Avem două cazuri:

- Dacă t este abscisa lui M, atunci el este şi abscisa lui M_1, iar rezultatul este stabilit.

- Dacă t este ordonata lui M, atunci el este şi ordonata lui M_2, prin urmare este şi abscisa punctului M_2', obţinut intersectând cercul (constructibil) de centru O şi rază OM_2 cu axa Ox.

□

Propoziţia 1.6. *Dacă A este un punct constructibil, iar t este un număr constructibil, atunci cercul de centru A şi de rază $|t|$ este constructibil.*

Demonstraţie. Punctul M de abscisă t de pe axa Ox este constructibil, conform propoziţiei 1.5. Cercul de centru A şi de rază $|t|$ este, atunci, cercul de centru A şi de rază OM, deci este constructibil. □

1.3 Corpul numerelor constructibile

Teorema 1.1. *Mulţimea $\mathcal{C}$ a numerelor reale constructibile este un subcorp al lui $\mathbb{R}$, stabil faţă de rădăcina pătrată*[1].

Demonstraţie. Ştim deja că numerele reale 0 şi 1 sunt constructibile, deoarece sunt abscisele punctelor de bază O şi I. Mai departe,

1) Dacă $u \in \mathcal{C}$, vom demonstra că şi $-u \in \mathcal{C}$. Într-adevăr, fie A punctul de pe axa Ox de abscisă u. Considerăm cercul cu centrul în O şi de rază $|u|$ (presupunem fireşte, că $u \neq 0$, altfel nu avem ce demonstra). Acest cerc intersectează din nou axa Ox într-un punct B, a cărui abscisă este $-u$. Cum punctul B este, în mod evident, constructibil, rezultă că şi abscisa lui, $-u$ este în $\mathcal{C}$.

2) Fie $u, v \in \mathcal{C}$ şi fie A şi B punctele de pe axa Ox pentru care $\overline{OA} = u$ şi $\overline{AB} = v$. Punctul A este constructibil, conform propoziţiei 1.5, iar punctul B este constructibil conform propoziţiei 1.6, dacă utilizăm cercul de centru A şi de rază $|v|$. Prin urmare, avem $\overline{OB} = u + v$, ceea ce înseamnă că $u + v = \mathcal{C}$.

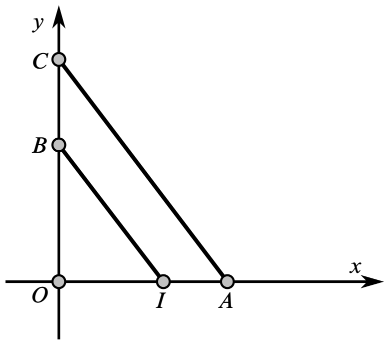

Figura 1.7

[1]Asta înseamnă că dacă un număr real pozitiv este constructibil, atunci şi rădăcina sa pătrată este constructibilă.

3) Fie $u, v \in \mathcal{C}$. Dacă $uv = 0$, atunci nu avem ce demonstra, deci presupunem că atât u, cât şi v sunt nenule. Fie A pe Ox astfel încât $\overline{OA} = u$ şi B pe Oy astfel încât $\overline{OB} = v$. Paralela la IB care trece prin A taie axa Oy într-un punct C. Din teorema lui Thales rezultă că
$$\frac{\overline{OC}}{\overline{OB}} = \frac{\overline{OA}}{\overline{OI}},$$
de unde rezultă că $\overline{OC} = uv$, adică $uv \in \mathcal{C}$ (vezi figura 1.7).

4) Fie $u \in \mathcal{C}$, $u \neq 0$. Fie, mai departe, A pe axa Ox astfel încât $\overline{OA} = u$. Paralela la AJ dusă prin I taie axa Oy într-un punct B. Din Teorema lui Thales, avem că
$$\frac{\overline{OB}}{\overline{OJ}} = \frac{\overline{OI}}{\overline{OA}},$$
de unde rezultă că $\overline{OB} = 1/u$, deci $1/u \in \mathcal{C}$ (vezi figura 1.8).

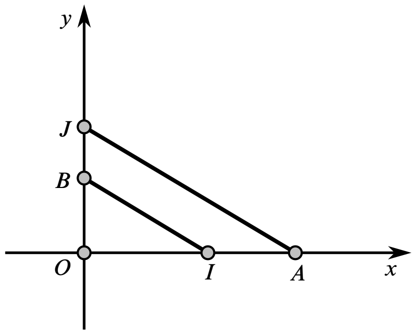

Figura 1.8

5) Dacă $u \in \mathcal{C}$, $u \geq 0$. Dacă $u = 0$, atunci $\sqrt{u}$ este tot 0, deci este constructibil. Presupunem, în cele ce urmează, că $u > 0$. Fie A punctul de pe axa Ox astfel încât $\overline{IA} = u$ şi M – mijlocul segmentului OA. Perpendiculara în I pe Ox taie cercul cu centrul în M şi de rază OM într-un punct B de ordonată pozitivă. Triunghiul OBA este dreptunghic în B, deci avem $IA^2 = OI \cdot IA$. Astfel, $IB = \sqrt{u}$, iar $\sqrt{u}$ este ordonata punctului constructibil B, adică $\sqrt{u} \in \mathcal{C}$ (vezi figura 1.9).

□

Observaţii. 1) Menţionăm, mai întâi, că $\mathbb{Q}$ este cel mai mic subcorp al lui $\mathbb{R}$. Întradevăr, fie K un subcorp oarecare al lui $\mathbb{R}$. Atunci, înainte de toate, $1 \in K$. Din stabilitatea lui K faţă de adunare, rezultă imediat că $\mathbb{N} \subset K$, în timp ce stabilitatea faţă de trecerea la opus implică $\mathbb{Z} \subset K$. În sfârşit, din stabilitatea faţă de produs şi trecerea la invers rezultă că $\mathbb{Q} \subset K$. Rezultă de aici că $\mathbb{Q} \subset \mathcal{C} \subset \mathbb{R}$.

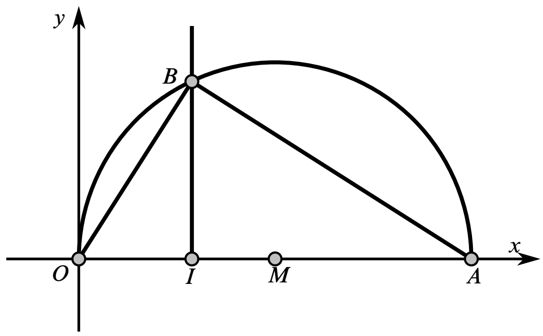

Figura 1.9

Aşadar, din moment ce corpul $\mathcal{C}$ este stabil faţă de rădăcina pătrată şi conţine numerele raţionale, se pot da multe exemple de numere constructibile, ca de exemplu:

$$-\frac{2}{3},\ \sqrt{2},\ \sqrt[4]{3},\ \frac{2+3\sqrt{2}+\sqrt{5}}{\sqrt{3}}.$$

Mai mult, folosind construcţiile din teorema 1.1, putem construi efectiv punctele de pe axa Ox care au ca abscise aceste numere.

1.4 Caracterizarea numerelor constructibile

1.4.1 Extinderi de corpuri

Ceea ce vom prezenta în acest paragraf este doar o trecere în revistă a noţiunilor şi rezultatelor de teoria extinderilor de corpuri care vor fi necesare în analiza ce urmează a constructibilităţii cu rigla şi compasul. Cititorul interesat poate găsi detalii şi demonstraţii detaliate în orice carte de teoria corpurilor. Reamintim că toate corpurile considerate de noi se presupune a fi comutative.

Definiţia 1.3. Fie K şi L două corpuri astfel încât K să fie un subcorp al lui L. Vom spune atunci despre corpul K că este *o extindere* a corpului K şi vom nota acest fapt cu $K \subset L$.

Evident, orice corp este o extindere a lui însuşi.

Dacă $a \in L$, vom nota cu $K(a)$ cel mai mic subcorp al lui L care conţine pe K şi pe a. Este uşor de constatat că acest corp există şi poate fi construit fie ca intersecţia tuturor subcorpurilor lui L care conţin a şi K fie (ceea ce este acelaşi lucru) ca fiind subcorpul lui L generate de a şi de K (mai precis, de a şi de *elementele* lui K). Mai general, dacă $a_1, a_2, \ldots, a_n \in L$, vom nota cu $K(a_1, \ldots, a_n)$ cel mai mic subcorp al lui L care conţine elementele lui K şi, în plus, elementele $a_1, \ldots, a_n$ şi vom spune că acest corp a fost obţinut din corpul K prin *adjuncţionarea* elementelor $a_1, \dots, a_n$. Iată câteva exemple:

- $\mathbb{Q}(1) = \mathbb{Q}\left(-\frac{2}{3}\right) = \mathbb{Q}$;
- $\mathbb{Q}(\sqrt{2}) = \left\{\alpha + \beta\sqrt{2} \,|\, \alpha, \beta \in \mathbb{Q}\right\}$;
- $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \left\{\alpha + \beta\sqrt{2} + \gamma\sqrt{3} + \delta\sqrt{6} \,|\, \alpha, \beta, \gamma, \delta \in \mathbb{Q}\right\}$;
- $\mathbb{Q}(i) = \left\{\alpha + \beta i \,|\, \alpha, \beta \in \mathbb{Q}\right\}$;
- $\mathbb{R}(i) = \left\{\alpha + \beta i \,|\, \alpha, \beta \in \mathbb{R}\right\} = \mathbb{C}$.

În cazul în care $K \subset L$ este o extindere de corpuri, atunci corpul mai mare, L în cazul nostru, poate fi privit ca fiind un spaţiu vectorial peste corpul mai mic (K, în cazul nostru). Aici adunarea în spaţiul vectorial L este adunarea în L (ca şi corp, de data aceasta), în timp ce înmulţirea cu scalari este restricţia la $K \times L$ a înmulţirii interne în corpul L. Dimensiunea lui L, privit ca şi corp peste K, joacă un rol foarte important în teoria extinderilor de corpuri, de aceea merită o poziţie şi o notaţie specială.

Definiţia 1.4. Fie $K \subset L$ o extindere de corpuri. Dimensiunea lui L, ca spaţiu vectorial peste K, se numeşte *gradul extinderii* şi se notează cu $[L : K]$.

Exemple. 1. Este clar că orice extindere trivială are gradul 1. Într-adevăr, dacă îl privim pe L ca şi corp peste L, în spiritul definiţie precedente, atunci mulţimea $\{1\}$ este, în mod evident, o bază a acestui spaţiu vectorial, deci $[L : L] = 1$. Astfel, de exemplu, dacă punem $K = \mathbb{Q}$ şi $L = \mathbb{Q}(2)(= \mathbb{Q})$, atunci $[L : K] \equiv [\mathbb{Q}(2) : \mathbb{Q}] = 1$.

2. $\left\{1, \sqrt{2}\right\}$ formează o bază a lui $\mathbb{Q}(\sqrt{2})$ peste $\mathbb{Q}$, deci $\left[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}\right] = 2$.

3. $\left\{1, \sqrt{3}\right\}$ formează o bază a lui $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ peste $\mathbb{Q}(\sqrt{2})$, deci
$$\left[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})\right] = 2.$$

Observaţia 5. Se poate demonstra uşor că dacă K, L, M sunt trei corpuri astfel încât $K \subset L \subset M$, atunci între grade există relaţia
$$[M : K] = [M : L] \times [L : K].$$

Astfel, de exemplu,
$$\left[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}\right] = \left[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})\right] \times \left[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}\right] = 2 \times 2 = 4.$$

Definiţia 1.5. Fie $K \subset L$ o extindere de corpuri. Dacă $a \in L$, atunci a se numeşte *algebric* peste K dacă există un polinom nenul $P \in K[X]$ astfel încât să avem $P(a) = 0$. Un element care nu este algebric peste K se numeşte *transcendent* peste K.

Este clar că toate elementele corpului K sunt algebrice peste K.

Elemente algebrice peste $\mathbb{Q}$ (adică *numere algebrice*) se pot construi cu uşurinţă. Ele sunt rădăcini ale polinoamelor cu coeficienţi întregi. De exemplu, $\sqrt{2}$ este o rădăcină a polinomului $X^2 - 2$, în timp ce i este o rădăcină a polinomului $X^2 + 1$.

Construirea unor numere transcendente (elemente transcendente peste $\mathbb{Q}$) este mai dificilă. De fapt primele exemple au fost date abia la sfârşitul secolului al XIX-lea. Astfel, în anul 1873 matematicianul francez Ch. Hermite a demonstrat că numărul e (baza logaritmilor naturali) este transcendent, iar în 1882, F. Lindemann a demonstrat că numărul π este transcendent.

Observaţia 6. Fie $K \subset L$ o extindere de corpuri şi $a \in L$ un element algebric peste K. Atunci există un polinom unic $P \in K[X]$ astfel încât:

- $P(a) = 0$;
- P este ireductibil în $K[X]$;
- P este unitar (coeficientul termenului de grad maxim este egal cu 1).

Acest polinom se numeşte *polinomul minimal al lui a peste K*.

Dacă a este un element algebric peste K, iar n este gradul polinomului său minimal, atunci vom spune că a este *algebric de grad n peste K*. Atunci avem $\big[K(a) : K\big] = n$, iar o bază a K-spaţiului vectorial $K(a)$ este formată din

$$\left\{1, a, a^2, \ldots, a^{n-1}\right\}.$$

De exemplu, $\sqrt{2}$ este algebric de gradul 2 peste $\mathbb{Q}$, polinomul său minimal peste $\mathbb{Q}$ este $X^2 - 2$, iar o bază a lui $\mathbb{Q}(\sqrt{2})$ este $\{1, \sqrt{2}\}$.

Dacă $K \subset L$ este o extindere de corpuri, mulţimea elementelor algebrice peste K ale lui L formează, după cum se poate constata cu uşurinţă, un subcorp al lui L care conţine K. Vom nota cu $\mathcal{A}$ corpul numerelor reale algebrice peste $\mathbb{Q}$. Se ştie despre acest corp că este numărabil.

1.5 Teorema (sau rezultatul) lui Wantzel

În anul 1837, matematicianul francez P.L. Wantzel a dat o caracterizare a numerelor reale constructibile. Mai precis, el a indicat o condiţie *necesară*, dar, după cum vom vedea, nu şi suficientă pentru ca un număr real să fie constructibil cu rigla şi compasul.

Pentru a putea expune rezultatul lui Wantzel, plecăm, din nou, de la punctele de bază O şi I, pe baza cărora vom construi reperul ortonormat (O, I, J). Dacă M este un punct din planul euclidian raportat la acest reper, punct care are coordonatele x şi y, atunci acest punct va fi notat cu $M(x, y)$.

Începem prin a demonstra următoarea lemă:

Lema 1.1. *1. Dacă D este o dreaptă din planul euclidian Π care trece prin punctele distincte $A(a_1, a_2)$ şi $B(b_1, b_2)$, atunci D are o ecuaţie de forma*

$$\alpha x + \beta y + \gamma = 0,$$

unde $\alpha, \beta, \gamma \in \mathbb{Q}(a_1, a_2, b_1, b_2)$.

2. Fie $A(a_1, a_2)$, $B(b_1, b_2)$ şi $C(c_1, c_2)$ trei puncte necoliniare din planul euclidian Π. Atunci cercul de centru A şi de rază BC are o ecuaţie de forma

$$x^2 + y^2 - 2\alpha x - 2\beta y + \gamma = 0,$$

cu $\alpha, \beta, \gamma \in \mathbb{Q}(a_1, a_2, b_1, b_2, c_1, c_2)$.

Demonstraţie. 1) Dacă $a_1 = b_1$, atunci ecuaţia dreptei D este

$$x - a_1 = 0,$$

care, în mod evident, este de forma cerută. Dacă $a_1 \neq b_1$, atunci ecuaţia dreptei se poate scrie sub forma

$$y - a_2 = \frac{b_2 - a_2}{b_1 - a_1}(x - a_1),$$

ecuaţie care este, de asemenea, de forma cerută.

2) Cercul de centru A şi de rază BC are ecuaţia

$$(x - a_1)^2 + (y - a_2)^2 = (c_1 - b_1)^2 + (c_2 - b_2)^2,$$

care se poate rescrie sub forma

$$x^2 + y^2 - 2\alpha x - 2\beta y + \gamma = 0,$$

cu $\alpha, \beta, \gamma \in \mathbb{Q}(a_1, a_2, b_1, b_2, c_1, c_2)$. □

Teorema 1.2. *Fie $t \in \mathbb{R}$. t este un număr constructibil dacă şi numai dacă există un întreg $p \geq 1$ şi un şir de subcorpuri ale lui $\mathbb{R}$, $L_1, L_2, \ldots, L_p$ astfel încât:*

- *$L_1 = \mathbb{Q}$;*
- *pentru $1 \leq j \leq p - 1$, $L_j \subset L_{j+1}$ şi $[L_{j+1} : L_j] = 2$;*

- $t \in L_p$.

Demonstraţie. Dacă t este constructibil, atunci t este abscisa unui punct M al axei Ox. Fie $M_1, M_2, \ldots, M_n = M$ şirul de puncte succesive construite pentru obţinerea lui M. Se poate presupune că M_1 şi M_2 sunt punctele de bază O şi I.

Pentru $i = 1, 2, \ldots, n$ vom nota cu x_i şi y_i coordonatele punctului M_i în reperul (O, I, J). Avem, în particular: $x_1 = y_1 = 0$, $x_2 = 1$, $y_2 = 0$, $x_n = t$, $y_n = 0$. Punem:

$$\begin{aligned}
K_1 &= \mathbb{Q}(x_1, y_1),\\
K_2 &= \mathbb{Q}(x_1, y_1, x_2, y_2),\\
&\cdots\\
K_i &= \mathbb{Q}(x_1, y_1, \ldots, x_i, y_i),\\
&\cdots\\
K_n &= \mathbb{Q}(x_1, y_1, \ldots, x_n, y_n).
\end{aligned}$$

Avem:

$$K_1 \subset K_2 \subset \cdots \subset K_i \subset K_{i+1} \subset \cdots \subset K_n,\ t = x_n \in K_n.$$

Vom demonstra că pentru $i = 1, 2, \ldots, n-1$, avem $K_{i+1} = K_i$ sau $[K_{i+1} : K_i] = 2$.

Rezultatul este evident pentru $i = 1$, deoarece $K_1 = K_2 = \mathbb{Q}$. Să presupunem, deci, că $i \geq 2$. Avem de examinat trei cazuri, după cum punctul M_{i+1} este intersecţia dintre două drepte, dintre o dreaptă şi un cerc sau dintre două cercuri definite prin punctele precedente, $M_1, M_2, \ldots, M_i$. Dar, potrivit lemei 1.1, aceste drepte şi cercuri au coeficienţi în $K_i = \mathbb{Q}(x_1, y_1, \ldots, x_i, y_i)$. Prin urmare,

1) Dacă M_{i+1} este la intersecţia a două drepte, atunci coordonatele sale, x_{i+1} şi y_{i+1} sunt soluţii ale unui sistem de forma

$$\begin{cases} \alpha x + \beta y + \gamma = 0,\\ \alpha' x + \beta' y + \gamma' = 0, \end{cases}$$

cu $\alpha, \beta, \gamma, \alpha', \beta', \gamma' \in K_i$. Rezolvând acest sistem de gradul întâi se constată că x_{i+1} şi y_{i+1} sunt, de asemenea, în K_i, de unde rezultă că avem

$$K_{i+1} = K_i(x_{i+1}, y_{i+1}) \equiv K_i.$$

2) Dacă M_{i+1} se află la intersecţia dintre o dreaptă şi un cerc, atunci atunci coordonatele sale, x_{i+1} şi y_{i+1} sunt soluţii ale unui sistem de forma

$$\begin{cases} \alpha x + \beta y + \gamma = 0,\\ x^2 + y^2 - 2\alpha' x - 2\beta' y + \gamma' = 0, \end{cases}$$

cu $\alpha, \beta, \gamma, \alpha', \beta', \gamma' \in K_i$. Avem mai multe situaţii posibile:

- Dacă $\beta \neq 0$, atunci avem
$$y = -\frac{1}{\beta}(\alpha x + \gamma).$$
Înlocuim în cea de-a doua ecuaţie pentru a obţine ecuaţia pentru abscise. Această ecuaţie este de gradul al doilea cu coeficienţi în K_i, iar x_{i+1} este o rădăcină a acestei ecuaţii.
  - Dacă $x_{i+1} \in K_i$, atunci
  $$y = -\frac{1}{\beta}(\alpha x_{i+1} + \gamma) \in K_i,$$
  iar $K_{i+1} = K_i$.
  - Dacă $x_{i+1} \notin K_i$, atunci x_{i+1} este algebric de gradul 2 peste K_i şi avem:
  $$K_{i+1} = K_i(x_{i+1}, y_{i+1}) = K_i(x_{i+1})$$
  şi $\left[K_{i+1} : K_i\right] = 2$.
- Dacă $\beta = 0$, atunci $\alpha \neq 0$ şi se poate proceda la fel ca mai sus, formând ecuaţia de gradul al doilea pentru ordonate.

3) Dacă M_{i+1} este la intersecţia dintre două cercuri, atunci coordonatele sale, x_{i+1} şi y_{i+1}, sunt soluţii ale unui sistem de forma
$$\begin{cases} x^2 + y^2 - 2\alpha x - 2\beta y + \gamma = 0, \\ x^2 + y^2 - 2\alpha' x - 2\beta' y + \gamma' = 0, \end{cases}$$
cu $\alpha, \beta, \gamma, \alpha', \beta', \gamma' \in K_i$. Acest sistem este echivalent cu sistemul
$$\begin{cases} x^2 + y^2 - 2\alpha x - 2\beta y + \gamma = 0, \\ 2(\alpha - \alpha')x + 2(\beta - \beta')y + (\gamma - \gamma') = 0, \end{cases}$$
deci problema se reduce la cazul precedent.

Am construit, astfel, un şir de subcorpuri ale lui $\mathbb{R}$:
$$K_1 \subset K_2 \subset \cdots \subset K_n$$
astfel încât $K_1 = \mathbb{Q}$, $t \in K_n$ şi pentru $1 \leq i \leq n-1$, să avem fie $K_{i+1} = K_i$, fie $\left[K_{i+1} : K_i\right] = 2$. Putem face în aşa fel încât acest şir să fie strict crescător, eliminând corpurile superflue. Se obţine atunci un şir
$$L_1 \subset L_2 \subset \cdots \subset L_p$$

astfel încât $L_1 = \mathbb{Q}$, $t \in L_p$ şi pentru $1 \leq i \leq p-1$, să avem $\left[L_{i+1} : L_i\right] = 2$.

Invers, să presupunem acum că

$$L_1 \subset L_2 \subset \cdots \subset L_p$$

este un şir de subcorpuri ale lui $\mathbb{R}$ care îndeplineşte condiţiile din enunţul teoremei. Vom demonstra, prin recurenţă după j, cu $1 \leq j \leq p$, că $L_j \subset \mathcal{C}$. Va rezulta atunci că t este un număr constructibil.

- $L_1 \subset \mathcal{C}$, deoarece $L_1 = \mathbb{Q}$ şi se ştie că $\mathbb{Q} \subset \mathcal{C}$.

- Presupunem că $L_j \subset \mathcal{C}$ şi vom demonstra că $L_{j+1} \subset \mathcal{C}$. Fie $a \in L_{j+1}$. Să demonstrăm că $a \in \mathcal{C}$. Familia $\left\{1, a, a^2\right\}$ este liniar dependentă peste L_j, deoarece $\left[L_{j+1} : L_j\right] = 2$. Prin urmare, există $\alpha, \beta, \gamma \in L_j$, nu toate nule, astfel încât

$$\alpha a^2 + \beta a + \gamma = 0.$$

  Sunt posibile două situaţii:

  – dacă $\alpha = 0$, atunci $a = -\frac{\gamma}{\beta} \in L_j \subset \mathcal{C}$;
  – dacă $\alpha \neq 0$, atunci
$$a = \frac{-\beta + \sqrt{\beta^2 - 4\alpha\gamma}}{2\alpha}$$
  şi $a \in \mathbb{C}$, deoarece corpul $\mathbb{C}$, după cum am văzut, este stabil faţă de rădăcina pătrată.

$\square$

Teorema de mai sus are o consecinţă remarcabilă, care este tocmai rezultatul demonstrat de către Wantzel.

Consecinţa 1 (Rezultatul lui Wantzel)**.** *Orice număr real constructibil este algebric peste $\mathbb{Q}$, iar gradul său este o putere a lui 2.*

Demonstraţie. Dacă $t \in \mathbb{R}$ este constructibil, atunci din teorema 1.2 rezultă că există un întreg $p \geq 1$ şi un şir de subcorpuri ale lui $\mathbb{R}$, $L_1, L_2, \ldots, L_p$ astfel încât:

- $L_1 = \mathbb{Q}$;

- pentru $1 \leq j \leq p-1$, $L_j \subset L_{j+1}$ şi $\left[L_{j+1} : L_j\right] = 2$;

- $t \in L_p$.

Pe de altă parte, utilizând o proprietate a extinderilor de corpuri pe care am mai menţionat-o mai sus, avem:

$$\left[L_p : \mathbb{Q}\right] = \left[L_p : L_{p-1}\right] \times \left[L_{p-1} : L_{p-2}\right] \times \cdots \times \left[L_2 : \mathbb{Q}\right] = 2^{p-1}.$$

Pe de altă parte, avem $\mathbb{Q} \subset \mathbb{Q}(t) \subset L_p$, de unde rezultă că

$$2^{p-1} = \left[L_p : \mathbb{Q}\right] = \left[L_p : \mathbb{Q}(t)\right] \times \left[\mathbb{Q}(t) : \mathbb{Q}\right].$$

Aşadar, $\left[\mathbb{Q}(t) : \mathbb{Q}\right]$ este un divizor al lui 2^{p-1}, adică este tot o putere a lui 2, pe care o vom nota cu 2^q. Considerăm familia $\left\{1, t, t^2, \ldots, t^{2^q}\right\}$. Această familie are $2^q + 1$ elemente, deci este liniar dependentă în $\mathbb{Q}$-spaţiul vectorial $\mathbb{Q}(t)$. Prin urmare, există numerele raţionale $\alpha_0, \alpha_1, \ldots \alpha_{2^q}$, nu toate nule, astfel încât

$$\alpha_0 + \alpha_1 t + \cdots + \alpha_{2^q} t^{2^q} = 0.$$

Ptin urmare, t este algebric peste $\mathbb{Q}$, iar gradul lui t peste Q este $\left[\mathbb{Q}(t) : \mathbb{Q}\right] = 2^q$. $\square$

Exemple. Rezultatul lui Wantzel este deosebit de util pentru a demonstra că un număr real *nu* este constructibil. Iată două exemple utile în cele ce urmează:

1) Unul dintre numerele ce joacă un rol esenţial în matematică este π. Noi vom demonstra în Anexa A că π nu este algebric peste $\mathbb{Q}$, deci el nu are cum să fie constructibil.

2) Să considerăm polinomul $X^3 - 2$, care este ireductibil peste $\mathbb{Q}$ (în caz contrar, polinomul ar trebui să aibă un factor de gradul întâi pe peste $\mathbb{Q}$, ceea ce înseamnă că el ar trebui să aibă o rădăcină raţională, ceea ce, în mod evident, nu este cazul). Prin urmare, polinomul $X^3 - 2$ este polinomul minimal peste $\mathbb{Q}$ al numărului real $\sqrt[3]{2}$. Aceasta înseamnă că $\sqrt[3]{2}$ este algebric de gradul 3 peste $\mathbb{Q}$. Din rezultatul lui Wantzel rezultă, atunci, că $\sqrt[3]{2}$ nu este un număr constructibil.

Observaţia 7. Am notat cu $\mathcal{A}$ corpul numerelor reale algebrice peste $\mathbb{Q}$. Atunci avem

$$\mathbb{Q} \subset \mathcal{C} \subset \mathcal{A} \subset \mathbb{R}.$$

Mai mult, folosind numerele $\sqrt{2}$, $\sqrt[3]{2}$ şi π, constatăm că toate incluziunile sunt stricte. În fine, întrucât corpul numerelor algebrice este numărabil, acelaşi lucru este valabil şi pentru corpul numerelor constructibile.

1.6 Aplicaţii ale rezultatului lui Wantzel

1.6.1 Cuadratura cercului

Reamintim că această problemă constă în construirea, cu rigla şi compasul, a unui pătrat de aceeaşi arie cu cea a unui cerc dat. A da un cerc este echivalent cu a indica centrul său, fie el O şi un punct al cercului, fie el I. Prin urmare, construcţia cerută este o construcţie cu rigla şi compasul plecând de la punctele de bază O şi I. Dacă raportăm planul la reperul (O, I, J) introdus mai devreme, atunci segmentul OI este de lungime 1, iar aria cercului dat este egală cu π.

În cazul în care cuadratura cercului ar fi posibilă, am putea construi cu rigla şi compasul un segment de lungime $\sqrt{\pi}$ (latura pătratului căutat). Or, noi ştim că numărul $\sqrt{\pi}$ este transcendent (dacă ar fi algebric, atunci şi pătratul său, adică π, ar fi algebric, ori noi demonstrăm în anexa A că este transcendent).

Prin urmare, problema cuadraturii cercului este imposibil de rezolvat cu rigla şi compasul.

1.6.2 Dublarea cubului

Reamintim că această problemă constă în construirea cu rigla şi compasul a laturii unui cub al cărui volum să fie egal cu volumul unui cub dat.

Faptul că un cub este dat este echivalent, din punctul nostru de vedere, că este dată una dintre laturile sale, fie ea OI. Ca şi în cazul cuadraturii cercului, raportăm planul la reperul ortonormat (O, I, J). Asta înseamnă că latura cubului dat este de lungime 1. De aici rezultă că volumul cubului dat este egal cu 1, în timp ce volumul cubului căutat trebuie să fie egal cu 2. Dacă dublarea cubului ar fi posibilă, am putea construi cu rigla şi compasul latura cubului cerut, adică am putea construi cu rigla şi compasul numărul real $\sqrt[3]{2}$. Dar, rezultatul lui Wantzel implică, după cum am remarcat deja la sfârşitul secţiunii precedente, rezultă că $\sqrt[3]{2}$ nu este un număr constructibil, deci dublarea cubului nu se poate efectua cu rigla şi compasul.

1.6.3 Trisecţiunea unghiului

Această problemă constă în construirea, cu rigla şi compasul, a semidreptelor care împart un unghi *oarecare* în trei unghiuri egale. Evident, este suficient să construim una dintre semidrepte, deoarece construirea celei de-a doua se reduce, atunci, la construirea bisectoarei unui unghi.

Înainte de a ademonstra că problema este imposibilă, o traducem într-un limbaj mai comod, folosind noţiunea de *unghi trisectabil*.

Unghiurile la care se referă problema sunt unghiuri neorientate, care se pot identifica cu măsura lor în radiani şi putem presupune că sunt cuprinse în intervalul $[0, \pi]$. Mai precis, $\widehat{ABC} = \theta$ înseamnă că θ este singurul număr real din intervalul $[0, \pi]$ pentru care

$$\cos\theta = \frac{\overrightarrow{BA} \cdot \overrightarrow{BC}}{\|\overrightarrow{BA}\| \cdot \|\overrightarrow{BC}\|}.$$

Punctele de bază O şi I fiind date, putem întotdeauna să considerăm că unghiurile sunt toate reprezentate prin semidrepte cu originea în O, iar una dintre ele este semidreapta OI. Notăm cu Γ cercul cu centrul în O şi care trece prin I şi cu Γ_1 semicercul închis al acestui cerc care este situat deasupra dreptei OI.

Dacă $\theta \in [0, \pi]$, vom spune că *unghiul θ este constructibil* dacă punctul M al semicercului Γ_1 pentru care $\measuredangle IOM = \theta$ este constructibil. Aceasta condiţie este, în mod evident, echivalentă cu condiţia ca numărul $\cos\theta$ să fie constructibil, deoarece $\cos\theta$ este abscisa lui M relativ la reperul ortonormat (O, I, J). De exemplu, unghiurile $\frac{\pi}{2}, \frac{\pi}{3}, \frac{\pi}{6}$ sunt constructibile, deoarece cosinusurile acestor unghiuri, egale, respectiv, cu $0, \frac{1}{2}, \frac{\sqrt{3}}{2}$ sunt numere reale constructibile. Dimpotrivă, unghiul θ al cărui cosinues este egal cu $\frac{\sqrt[3]{2}}{2}$ nu este constructibil, din moment ce cosinusul însuşi nu este constructibil.

Find dat un unghi $\theta = \measuredangle IOM$, unde M este un punct de pe semicercul Γ_1, vom spune că θ este *trisectabil* dacă punctul N de pe semicercul Γ_1 pentru care

$$\measuredangle ION = \frac{\theta}{3}$$

este un punct constructibil plecând de la punctele de bază O, I, M.

Problema trisecţiunii unghiului se referă, prin urmare, la construcţii care pleacă de la trei puncte de bază, nu doar de la două, ca în czul cuadraturii cercului sau al dublării cubului. Pe de altă parte, dacă unghiul $\measuredangle IOM = \theta$ este constructibil, atunci punctul M este constructibil plecând de la punctele de bază O şi I, prin urmare construcţiile ce se obţin plecând de la punctele O, I, M sunt exact acelea care se obţin plecând de la punctele O, I. Astfel, a spune că unghiul θ este trisectabil este totuna cu a spune că unghiul $\frac{\theta}{3}$ este constructibil sau, ceea ce este acelaşi lucru, că numărul real $\cos\frac{\theta}{3}$ este constructibil. Astfel, unghiurile π şi $\frac{\pi}{3}$ sunt constructibile, deoarece $\cos\frac{\pi}{3} = \frac{1}{2}$ şi $\cos\frac{\pi}{6} = \frac{\sqrt{3}}{2}$ sunt numere reale constructibile.

Ceea ce dorim să demonstrăm este imposibilitatea trisecţiunii pentru un unghi oarecare. Va fi, deci, suficient să demonstrăm, de exemplu, că unghiul $\frac{\pi}{3}$ nu este trisectabil. Cum unghiul $\frac{\pi}{3}$ este constructibil, aceasta revine la a demonstra că $\cos\frac{\pi}{9}$ nu este un număr real constructibil.

Avem

$$\cos 3\theta = 4\cos^3\theta - 3\cos\theta,$$

prin urmare, $\cos\frac{\pi}{9}$ este o rădăcină a polinomului

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

Vom demonstra că acest polinom este ireductibil în $\mathbb{Q}[X]$. Dacă s-ar descompune în $\mathbb{Q}[X]$, unul dintre factori ar fi de gradul întâi, iar polinomul ar avea o rădăcină raţională, dar ne putem convinge cu uşurinţă că P nu are rădăcini raţionale.

Astfel, $P(X)$ este ireductibil în $\mathbb{Q}[X]$, prin urmare, polinomul minimal al lui $\cos\frac{\pi}{9}$ este

$$\frac{1}{4}P(X)$$

şi este de gradul 3. Prin urmare, $\cos\frac{\pi}{9}$ nu este constructibil, conform rezultatului lui Wantzel, ceea ce înseamnă că unghiul $\frac{\pi}{3}$ nu este trisectabil, ceea ce confirmă aşteptările noastre, adică faptul că nu orice unghi este trisectabil.

1.7 Caracterizarea corpurilor $\mathcal{C}$ şi $\mathcal{C}(i)$

Teorema 1.3. *$\mathcal{C}$ este cel mai mic subcorp al lui $\mathbb{R}$ care este stabil faţă de rădăcina pătrată.*

Demonstraţie. Am văzut, deja, că $\mathcal{C}$ este un subcorp al lui $\mathbb{R}$ stabil faţă de rădăcina pătrată. Fie K un alt subcorp al lui $\mathbb{R}$ stabil faţă de rădăcina pătrată. Scopul nostru este să demonstrăm că $\mathcal{C} \subset K$.

Fie $t \in \mathcal{C}$. Atunci există un şir de subcorpuri ale lui $\mathbb{R}$,

$$L_1 \subset L_2 \subset \cdots \subset L_p,$$

astfel încât $L_1 = \mathbb{Q}$, $t \in L_p$ şi, pentru $1 \leq j \leq p-1$, $\left[L_{j+1} : L_j\right] = 2$.

Pentru a demonstra că $t \in K$, este suficient să demonstrăm, prin recurenţă după j, că, pentru $1 \leq j \leq p$, $L_j \subset K$. Demonstraţia este perfect analogă cu sfârşitul demonstraţiei teoremei 1.2, în care se înlocuieşte $\mathbb{C}$ cu K. □

Observaţia 8. Rezultatul precedent are o interpretare intuitivă foarte simplă. El spune, pur şi simplu că toate numerele constructibile se pot obţine plecând de la numerele raţionale $\mathbb{Q}$, folosind operaţiile $+, -, \times, :, \sqrt{\ }$. În fapt, nici măcare nu trebuie să utilizăm toate numerele raţionale, numerele 0 şi 1 sunt suficiente.

Ne amintim că am spus că un punct este constructibil dacă ambele sale coordonate relativ la reperul $\{O, I, J\}$ sunt numere constructibile. Dacă identificăm planul cu corpul numerelor complexe, atunci este clar că mulţimea punctelor constructibile coincide cu subcorpul lui $\mathbb{C}$, $\mathcal{C}(i)$, unde i este, desigur, unitatea imaginară.

Corpul $\mathcal{C}(i)$ admite o caracterizare analogă caracterizării corpului $\mathcal{C}$. Mai precis, avem teorema care urmează.

Teorema 1.4. *$\mathcal{C}(i)$ este cel mai mic subcorp al lui $\mathbb{C}$ stabil relativ la rădăcina pătrată.*

Demonstraţie. Un subcorp K al lui $\mathbb{C}$ se numeşte *stabil relativ la rădăcina pătrată* dacă pentru orice $\alpha \in K$ rădăcinile polinomului $X^2 - \alpha$ sunt în K. Această afirmaţie este, în mod evident, echivalentă cu afirmaţia că orice polinom de gradul doi din $K[X]$ se descompune, în $K[X]$, în factori de gradul întâi.

Să demonstrăm, acum, că $\mathcal{C}(i)$ este stabil relativ la rădăcina pătrată. Cum $\mathcal{C}(i)$ este cel mai mic subcorp al lui $\mathbb{C}$ care conţine $\mathcal{C}$ şi i, este uşor de constatat că

$$\mathcal{C}(i) = \left\{a + ib \mid a, b \in \mathcal{C}\right\}.$$

Fie $\alpha \in \mathcal{C}(i)$. Atunci $\alpha = a + ib$, cu $a, b \in \mathcal{C}$. Trebuie să verificăm că, dacă

$$\alpha = (u + iv)^2,$$

atunci $u, v \in \mathcal{C}$. Dar $\alpha = (u + iv)^2$ dacă şi numai dacă

$$\begin{cases} a = u^2 - v^2, \\ b = 2uv. \end{cases}$$

u^2 şi $-v^2$ sunt rădăcinile polinomului

$$X^2 - aX - \frac{b^2}{4},$$

adică sunt egale cu

$$\frac{a \pm \sqrt{a^2 + b^2}}{2}.$$

Prin urmare,

$$u = \pm\sqrt{\frac{a + \sqrt{a^2 + b^2}}{2}},$$

de unde

$$v = \pm\sqrt{\frac{\sqrt{a^2 + b^2} - a}{2}}.$$

Semnele se aleg ţinând cont de faptul că $b = 2uv$. Oricum am alege semnele, $u, v \in \mathcal{C}$, deoarece $a, b \in \mathcal{C}$, iar $\mathcal{C}$ este stabil relativ la rădăcina pătrată.

Să demonstrăm, acum, că $\mathcal{C}(i)$ este cel mai mic subcorp al lui $\mathbb{C}$ stabil relativ la rădăcina pătrată.

Fie K un subcorp al lui $\mathbb{C}$ stabil relativ la rădăcina pătrată. Atunci $K \cap \mathbb{R}$ va fi un subcorp al lui $\mathbb{R}$, stabil relativ la rădăcina pătrată. Deducem, din teorema 1.3, că

$$\mathcal{C} \subset K \cap \mathbb{R} \subset K.$$

În plus, cum $-1 \in K$, iar K e stabil relativ la rădăcina pătrată, rezultă că $i \in K$, deci $\mathcal{C}(i) \in K$. □

1.8 Reciproca rezultatului lui Wantzel

După cum am văzut, rezultatul lui Wantzel ne dă doar o condiţie necesară pentru ca un număr să fie constructibil. Este natural să ne întrebăm dacă reciproca sa este adevărată. Cu alte cuvinte, dacă t este un număr real, algebraic peste $\mathbb{Q}$, iar gradul său este o putere a lui 2, este acest număr constructibil? Vom da mai jos un contraexemplu, care va dovedi că răspunsul la această întrebare este negativ.

Considerăm polinomul $P \in \mathbb{Q}[X]$,

$$P(X) = X^4 - X - 1.$$

Vom demonstra, mai întâi, că polinomul este ireductibil în $\mathbb{Q}[X]$. Asta va însemna că orice rădăcină a lui P este un număr algebric peste $\mathbb{Q}$, de gradul $4 = 2^2$. Pe de altă parte, vom arăta că acest polinom are o rădăcină reală, care nu este constructibilă. Polinomul P se poate descompune, în $\mathbb{R}[X]$, într-un produs de două polinoame de gradul doi, adică:

$$X^4 - X - 1 = (X^2 + aX + b)(X^2 + a'X + b'), \quad a, b, a', b' \in \mathbb{R}. \tag{1.1}$$

Identificând coeficienţii, obţinem:

$$\begin{cases} a + a' = 0, \\ b + b' + aa' = 0, \\ ab' + a'b = -1, \\ bb' = -1, \end{cases} \quad \text{sau} \quad \begin{cases} a = -a, \\ b + b' = a^2, \\ a(b' - b) = -1, \\ bb' = -1. \end{cases}$$

Din a doua şi a patra ecuaţie din cel de-al doilea sistem, deducem că b şi b' sunt rădăcinile ecuaţiei

$$T^2 - a^2 T - 1 = 0.$$

Cum a şi a' sunt opuse, putem presupyne, de exemplu, că $a > 0$, ceea ce înseamnă că $b' < b$, de unde rezultă că avem

$$\begin{cases} b = \dfrac{a^2 + \sqrt{a^4 + 4}}{2}, \\ b' = \dfrac{a^2 - \sqrt{a^4 + 4}}{2}, \end{cases}$$

prin urmare

$$\begin{cases} b - b' = -\sqrt{a^4 + 4}, \\ a\sqrt{a^4 + 4} = 1. \end{cases}$$

Polinomul $X^2 + aX + b$ are discriminantul

$$\Delta_1 = a^2 - 4b = a^2 - 2\left(a^2 + \sqrt{a^4 + 4}\right) = -a^2 - 2\sqrt{a^4 + 4} < 0,$$

ceea ce înseamnă că acest polinom are două rădăcini complexe conjugate. Polinomul $X^2 + a'X + b'$ are discriminantul

$$\Delta_2 = a'^2 - 4b' = a^2 - 2\left(a^2 - \sqrt{a^4 + 4}\right) = 2\sqrt{a^4 + 4} - a^2 > 0,$$

adică acest polinom are două rădăcini reale distincte, fie ele α şi β.

Plecând de la egalitatea $a\sqrt{a^4+4}=1$, deducem că $a^2(a^4+)=1$, ceea ce înseamnă că a^2 este rădăcină a ecuaţiei

$$T^3+4T-1=0.$$

Este uşor de verificat că această ecuaţie nu are rădăcini raţionale, deci polinomul T^3+4T-1 este ireductibil în $\mathbb{Q}[X]$. Dar asta înseamnă că a^2 este algebric peste $\mathbb{Q}$, iar gradul său este egal cu 3. Rezultatul lui Wantzel ne asigură, atunci, că a^2 nu este constructibil, prin urmare nici a nu este un număr constructibil.

Din prima formulă a lui Viète, avem

$$\alpha+\beta=-a'=a.$$

Cum a nu este constructibil, înseamnă că cel puţin una dintre rădăcinile lui P este neconstructibilă.

Ne-a mai rămas de demonstrat doar că P este ireductibil în $\mathbb{Q}[X]$. Cum a este neconstructibil, el nu este raţional, deci descompunerea (1.1) nu este o descompunere în $\mathbb{Q}[X]$. Cum, în plus, polinomul X^2+aX+b nu are rădăcini reale, nici o altă descompunere a lui P nu se poate face în $\mathbb{Q}[X]$. Aşadar, P este ireductibil în $\mathbb{Q}[X]$.

CAPITOLUL 2

Poligoane regulate

2.1 Poligoane regulate constructibile

În acest capitol, vom lucra cu *unghiuri orientate*, cu alte cuvinte, vom face distincţie, de exemplu, între un unghi $\widehat{ABC}$ şi unghiul $\widehat{CBA}$, măsura celui de-al doilea fiind considerată egală cu opusa măsurii celei dintâi.

Dacă $\theta \in \mathbb{R}$, vom nota cu $\widehat{\theta}$ unghiul orientat a cărui măsură în radiani este egală cu θ. Celelalte măsuri ale unghiului sunt $\theta + 2k\pi$, unde $k \in \mathbb{Z}$. $\widehat{\theta}$ posedă o unică măsură în radiani $\alpha \in (-\pi, \pi]$, care se numeşte *determinare principală* a unghiului dat.

Unghiul $\widehat{\theta}$ se numeşte *constructibil* dacă punctul M de pe cercul Γ (cu centrul în O şi care trece prin I) pentru care

$$\widehat{(\overrightarrow{OI}, \overrightarrow{OM})} = \widehat{\theta}$$

este un punct constructibil. A spune că $\widehat{\theta}$ este constructibil este echivalent cu a spune că numărul $\cos\theta$ este constructibil. Într-adevăr, dacă avem $\overline{OH} = \cos\theta$, atunci perpendiculara pe dreapta OI care trece prin H intersectează cercul Γ în două puncte, M şi M'. Alegem punctul care corespunde lui $\widehat{\theta}$, ţinând cont de determinarea principală a unghiului.

Dacă $n \geq 3$, vom spune că un poligon regulat cu n laturi este *constructibil* dacă unghiul de măsură $2\pi/n$ este constructibil, adică dacă numărul real $\cos\dfrac{2\pi}{n}$ este constructibil.

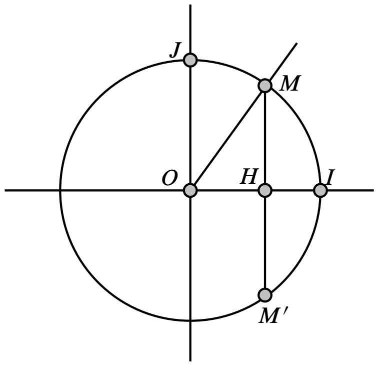

Figura 2.1

2.2 Teorema lui Gauss

Scopul acestei secţiuni este să prezentăm o caracterizare a poligoanelor regulate care sunt constructibile cu rigla şi compasul. Începem cu o lemă:

Lema 2.1. *Dacă m şi n sunt numere naturale prime între ele, atunci unghiul* $\dfrac{\widehat{2\pi}}{mn}$ *este constructibil dacă şi numai dacă sunt constructibile unghiurile* $\dfrac{\widehat{2\pi}}{n}$ *şi* $\dfrac{\widehat{2\pi}}{m}$.

Demonstraţie. ($\Longrightarrow$)Dacă $\dfrac{\widehat{2\pi}}{mn}$ este constructibil, atunci şi $\dfrac{\widehat{2\pi}}{n}$ şi $\dfrac{\widehat{2\pi}}{m}$ sunt constructibile, deoarece

$$\frac{\widehat{2\pi}}{n} = m\frac{\widehat{2\pi}}{mn},$$

iar

$$\frac{\widehat{2\pi}}{m} = n\frac{\widehat{2\pi}}{mn}$$

şi noi ştim cum să construim un multiplu întreg al unui unghi, purtând cu compasul de un anumit număr de ori coarda determinată de acest unghi în cercul de centru O şi care trece prin I[1].

($\Longleftarrow$) Dacă unghiurile $\dfrac{\widehat{2\pi}}{n}$ şi $\dfrac{\widehat{2\pi}}{m}$ sunt constructibile, atunci şi unghiul $\dfrac{\widehat{2\pi}}{mn}$ este constructibil, căci, conform relaţiei lui Bezout, există $\lambda, \mu \in \mathbb{Z}$, cu

$$\lambda n + \mu m = 1,$$

[1]Este de remarcat că în demonstrarea acestei implicaţii nu se foloseşte faptul că numerele m şi n sunt prime între ele.

de unde

$$\frac{\widehat{2\pi}}{mn} = \lambda \frac{\widehat{2\pi}}{n} + \mu \frac{\widehat{2\pi}}{m}.$$

Prin urmare, este suficient să ştim să construim suma a două unghiuri constructibile. Dar asta este foarte simplu, este suficient să aşezăm cele două unghiuri cu vârful în acelaşi punct, astfel încât ele să aibă o latură comună. □

Lema 2.2. *Dacă $n \geq 3$ are descompunerea în factori primi*

$$n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$$

atunci poligonul regulat cu n laturi este constructibil dacă şi numai dacă sunt constructibile unghiurile

$$\frac{\widehat{2\pi}}{p_1^{\alpha_1}}, \dots \frac{\widehat{2\pi}}{p_k^{\alpha_k}}.$$

Demonstraţie. Lema rezultă imediat din lema 2.1, prin inducţie după k. □

Lema 2.2 ne permite caracterizarea unghiurilor constructibile de forma $\frac{\widehat{2\pi}}{p^\alpha}$, unde p este un număr prim, iar α este un număr natural nenul.

Teorema 2.1. *1) Unghiurile de forma $\frac{\widehat{2\pi}}{2^\alpha}$ sunt constructibile.*

2) Dacă p este un număr prim mai mare sau egal cu 3, atunci $\frac{\widehat{2\pi}}{p^\alpha}$ este constructibil dacă şi numai dacă $\alpha = 1$, iar p este un număr Fermat, adică este de forma $1 + 2^{2^\beta}$, unde β este un număr natural.

Demonstraţie. 1) Este imediat că unghiurile de forma $\frac{\widehat{2\pi}}{2^\alpha}$ sunt constructibile. Este suficient să ştim să construim bisectoarea unui unghi, apoi folosim inducţia după α.

2) Fie $p \geq 3$ un număr prim.

($\Longrightarrow$) Să presupunem că unghiul $\frac{\widehat{2\pi}}{p^\alpha}$ este constructibil, cu $\alpha \in \mathbb{N}^*$. Atunci $\cos \frac{2\pi}{p^\alpha}$ este un număr constructibil şi atunci, din rezultatul lui Wantzel, obţinem că:

$$\left[\mathbb{Q}\left(\cos \frac{2\pi}{p^\alpha}\right) : \mathbb{Q}\right] = 2^m, \tag{2.1}$$

pentru un anumit număr natural m.

Pentru a simplifica scrierea, vom pune $q = p^\alpha$ şi fie

$$\omega = \cos \frac{2\pi}{q} + i \sin \frac{2\pi}{q}.$$

ω este o rădăcină de ordinul q a unităţii, rădăcină a polinomului $X^q - 1$, deci ω este algebric peste $\mathbb{Q}$. Admitem că polinomul minimal al lui ω peste $\mathbb{Q}$ este

$$P(X) = (X - \omega_1)(X - \omega_2) \cdots (X - \omega_h),$$

unde $\omega_1, \ldots, \omega_h$ sunt rădăcinile primitive de ordinul q ale unităţii, adică aceste rădăcini sunt de forma

$$\cos \frac{2k\pi}{q} + i \sin \frac{2k\pi}{q},$$

unde k este un număr întreg prim cu q, $1 \leq k \leq q$. Vom spune că $P(X)$ este *polinomul ciclotomic* de ordinul q.

Pentru a determina gradul h al lui $P(X)$ este suficient să cunoaştem numărul întregilor k, $1 \leq k \leq q$, astfel încât k să fie prim cu $q = p^\alpha$. Se obţine $h = p^{\alpha-1}(p-1)$, prin urmare

$$\left[\mathbb{Q}(\omega) : \mathbb{Q}\right] = p^{\alpha-1}(p-1). \tag{2.2}$$

Pe de altă parte, avem

$$\omega + \omega^{-1} = 2\cos\frac{2\pi}{p^\alpha},$$

de unde rezultă că

$$\cos\frac{2\pi}{p^\alpha} \in \mathbb{Q}(\omega) \quad \text{şi că} \quad \omega^2 - 2\omega\cos\frac{2\pi}{p^\alpha} + 1 = 0.$$

Astfel, ω este algebric de gradul 2 peste $\mathbb{Q}\left(\cos\frac{2\pi}{p^\alpha}\right)$, de unde rezultă că:

$$\left[\mathbb{Q}(\omega) : \mathbb{Q}\left(2\cos\frac{2\pi}{p^\alpha}\right)\right] = 2. \tag{2.3}$$

Plecând de la relaţiile (2.1), (2.2) şi (2.3) şi ştiind că

$$\left[\mathbb{Q}(\omega) : \mathbb{Q}\right] = \left[\mathbb{Q}(\omega) : \mathbb{Q}\left(2\cos\frac{2\pi}{p^\alpha}\right)\right] \times \left[\mathbb{Q}\left(2\cos\frac{2\pi}{p^\alpha}\right) : \mathbb{Q}\right],$$

se obţine

$$p^{\alpha-1}(p-1) = 2^{m+1}.$$

Cum p este un număr prim diferit de 2, rezultă că $\alpha = 1$ şi că $p = 1 + 2^{m+1}$.

Vom demonstra acum că $m+1$ este o putere a lui. Plecând de la descompunerea lui $m+1$ în factori primi, se obţine că

$$m + 1 = \lambda \cdot 2^\beta,$$

cu $\beta \in \mathbb{N}$ şi $\lambda \in \mathbb{N}^*$ – un număr impar. Prin urmare,

$$p = 1 + 2^{m+1} = 1 + 2^{\lambda \cdot 2^\beta} = 1 + \left(2^{2^\beta}\right)^\lambda .$$

λ fiind un număr impar, polinomul $1 + X^\lambda$ este divizibil cu $1 + X$. Rezultă că p este divizibil cu $1 + 2^{2^\beta}$. Cum p este un număr prim, rezultă că $p = 1 + 2^{2^\beta}$. □

Teorema 2.2 (Gauss)**.** *Poligoanele regulate constructibile cu rigla şi compasul sunt cele pentru care numărul n de laturi este fie de forma 2^α, cu $\alpha \geq 2$, fie de forma $2^\alpha p_1 p_2 \cdots p_r$, cu $\alpha \in \mathbb{N}$, unde p_i sunt numere prime distincte care sunt, în acelaşi timp, numere Fermat.*

Demonstraţie. Demonstraţia rezultă imediat din lema 2.2 şi teorema 2.1. □

2.3 Construcţii de poligoane regulate

2.3.1 Triunghiul echilateral, pătratul, pentagonul regulat

Construcţia *triunghiului echilateral* este foarte simplă, din moment ce ştim că avem

$$\cos \frac{2\pi}{3} = -\frac{1}{2}$$

(vezi figura 2.2).

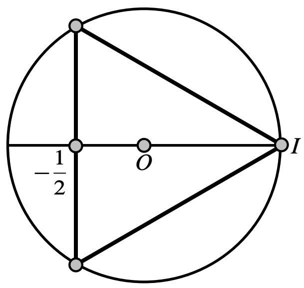

Figura 2.2

Construcţia *pătratului* este trivială, folosind punctele I şi J (vezi figura 2.3).

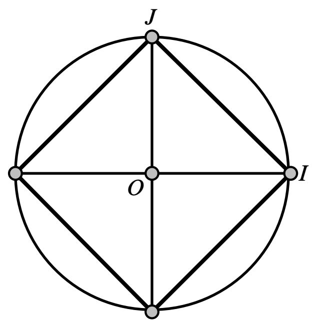

Figura 2.3

Construcţia *pentagonului regulat* este ceva mai complicată, deşi ea este cunoscută încă din antichitate, fiind prezentă în *Elementele* lui Euclid. O vom prezenta în cele ce urmează (vezi figura 2.4). În fapt, este suficient să exprimăm $\cos\frac{2\pi}{5}$ într-o formă care să permită construirea, efectivă, a punctului de pe axa Ox de abscisă $\cos\frac{2\pi}{5}$.

$$\cos\frac{2\pi}{5} + i\sin\frac{2\pi}{5}$$

este o rădăcină a polinomului

$$X^5 - 1 = (X-1)(X^4 + X^3 + X^2 + X + 1).$$

Avem, prin urmare,

$$\omega^4 + \omega^3 + \omega^2 + \omega + 1 = 0. \tag{2.4}$$

ω^4 este conjugatul lui ω, iar ω^3 este conjugatul lui ω^2, deci avem

$$\omega + \omega^4 = 2\cos\frac{2\pi}{5} \quad \text{şi} \quad \omega^2 + \omega^3 = \cos\frac{4\pi}{5}.$$

Din (2.4) rezultă atunci:

$$2\cos\frac{2\pi}{5} + 2\cos\frac{4\pi}{5} + 1 = 0. \tag{2.5}$$

Considerăm produsul

$$\cos\frac{2\pi}{5}\cdot\cos\frac{4\pi}{5},$$

egal cu

$$\frac{1}{2}\left(\cos\frac{6\pi}{5} + \cos\frac{2\pi}{5}\right) = \frac{1}{2}\left(\cos\frac{4\pi}{5} + \cos\frac{2\pi}{5}\right).$$

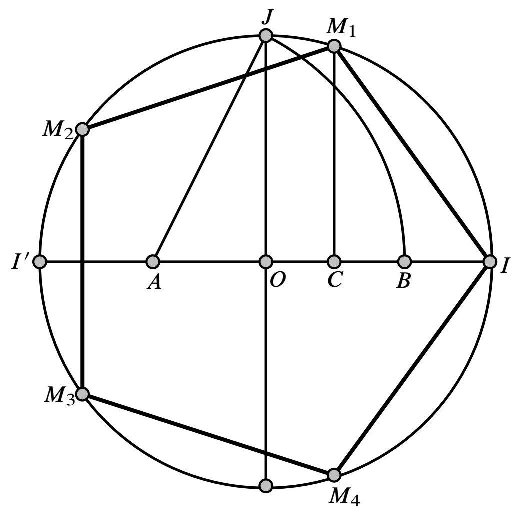

Figura 2.4

Dacă notăm cu p, respectiv s, produsul şi suma numerelor $\cos\dfrac{2\pi}{5}$ şi $\cos\dfrac{4\pi}{5}$, obţinem, ţinând cont de (2.5),

$$s = -\frac{1}{2} \quad \text{şi} \quad p = -\frac{1}{4}.$$

Astfel, $\cos\dfrac{2\pi}{5}$ şi $\cos\dfrac{4\pi}{5}$ sunt rădăcinile ecuaţiei

$$X^2 + \frac{1}{2}X - \frac{1}{4} = 0.$$

Remarcând faptul că

$$\cos\frac{4\pi}{5} < 0 < \cos\frac{2\pi}{5},$$

avem

$$\cos\frac{2\pi}{5} = \frac{-1+\sqrt{5}}{4} = \frac{-\frac{1}{2}+\sqrt{\frac{5}{4}}}{2}.$$

Fie A mijlocul segmentului OI'. Avem, prin urmare,

$$AJ = \sqrt{\frac{5}{4}}.$$

Folosind cercul de centru A şi de rază AJ, construim punctul B pe Ox astfel încât $\overline{AB} = AJ$. Avem, atunci,

$$\overline{OB} = -\frac{1}{2} + \sqrt{\frac{5}{4}}.$$

Dacă C este mijlocul lui OB, atunci avem

$$\overline{OC} = \cos\frac{2\pi}{5}.$$

Perpendiculara în C pe Ox permite obţinerea vârfului M_1. Cu ajutorul compasului, cu o deschidere egală cu coarda IM_1, construim celelalte patru vârfuri, M_2, M_3, M_4.

Observaţia 9. Graţie posibilităţii construirii bisectoarei unui unghi, putem dubla, tot timpul, numărul de laturi al unui poligon regulat constructibil. Astfel, plecând de la un triunghi echilateral, obţinem poligoane regulate cu 6, 12, 24, ... de laturi, iar plecând de la pătrat, se pot construi poligoane regulate cu 8, 16, 32, ... de laturi. De asemenea, plecând de la un pentagon regulat, se pot construi poligoane regulate cu 10, 20, 40, ... de laturi.

2.3.2 Poligonul cu 15 laturi

Deoarece 3 şi 5 sunt numere prime Fermat, rezultă câ poligonul regulat cu 15 laturi se poate construi cu rigla şi compasul.

Ideea construcţiei este să plecăm de la o relaţie Bezout între numerele 3 şi 5 şi, apoi, să exprimăm, folosind această relaţie, unghiul $\widehat{\frac{2\pi}{15}}$ în funcţie de unghiurile $\widehat{\frac{2\pi}{3}}$ şi $\widehat{\frac{2\pi}{5}}$.

Avem $2\cdot 3 + (-1)\cdot 5 = 1$ (relaţia Bezout pomenită mai sus), de unde

$$2\widehat{\frac{2\pi}{5}} - \widehat{\frac{2\pi}{3}} = \widehat{\frac{2\pi}{15}}.$$

Utilizând construcţiile pentru triunghiul echilateral şi pentagonul regulat, se pot construi pe cercul Γ punctele M şi N astfel încît

$$\widehat{(\overrightarrow{OI}, \overrightarrow{OM})} = 2\widehat{\frac{2\pi}{5}} \quad \text{şi} \quad \widehat{(\overrightarrow{OI}, \overrightarrow{ON})} = \widehat{\frac{2\pi}{3}}.$$

Avem atunci

$$\widehat{(\overrightarrow{ON}, \overrightarrow{OM})} = \widehat{\frac{2\pi}{15}}$$

şi, folosind compasul cu o deschidere egală cu coarda MN, se construieşte punctul P astfel încât

$$\widehat{(\overrightarrow{OI}, \overrightarrow{OP})} = \widehat{\frac{2\pi}{15}}.$$

ANEXA A

Transcendenţa numărului π

Teorema A.1 (Lindemann, 1882)**.** *Numărul real π este transcendent peste $\mathbb{Q}$.*

Demonstraţie. Presupunem că π ar fi algebric şi găsim o contradicţie. Deoarece şi i este algebric, iar numerele algebrice complexe formează un corp, rezultă că şi numărul πi este, de asemenea, algebric. Prin urmare, există o ecuaţie algebrică cu coeficienţi întregi

$$P_1(x) = 0, \tag{A.1}$$

ale cărei rădăcini sunt $\pi i = r_1, r_2, \ldots, r_n$. Cum

$$e^{r_1} \equiv e^{\pi i} = -1,$$

(relaţia lui Euler), obţinem

$$(e^{r_1} + 1)(e^{r_2} + 1) \cdots (e^{r_n} + 1) = 0. \tag{A.2}$$

Vom construi acum o ecuaţie algebrică cu coeficienţi întregi ale cărei rădăcini sunt exponenţii din dezvoltarea membrului stâng al ecuaţiei (A.2). Considerăm, mai întâi, exponenţii

$$r_1 + r_2, r_1 + r_3, \ldots, r_{n-1} + r_n. \tag{A.3}$$

Din ecuaţia (A.1) rezultă că funcţiile simetrice elementare de $r_1, r_2, \ldots, r_n$ sunt numere raţionale (tot ce se utilizează sunt formulele lui Viète). Prin urmare, funcţiile simetrice elementare de cantităţile (A.3) sunt, de asemenea, numere raţionale, aşadar aceste cantităţi sunt rădăcinile unei ecuaţii algebrice cu coeficienţi întregi

$$P_2(x) = 0. \tag{A.4}$$

În mod similar, sumele de câte trei r_i sunt cele C_n^3 rădăcini ale unei ecuaţii algebrice cu coeficienţi întregi

$$P_3(x) = 0. \tag{A.5}$$

Continuând procedeul, obţinem

$$P_4(x) = 0, P_5(x) = 0, \ldots, P_n(x) = 0, \tag{A.6}$$

ecuaţii algebrice cu coeficienţi întregi, ale căror rădăcini sunt sumele de câte 4, 5, ..., n rădăcini r_i ale ecuaţiei (A.1). Ecuaţia produs

$$P_1(x)P_2(x)\cdots P_n(x) = 0 \tag{A.7}$$

are ca rădăcini exact exponenţii dezvoltării membrului stâng al ecuaţiei (A.2).

Eliminarea rădăcinilor nule (dacă există) din ecuaţia (A.7) ne conduce la o ecuaţie de forma

$$P(x) = ax^m + a_{m-1}x^{m-1} + \cdots + a_1x + a_0 = 0 \tag{A.8}$$

ale cărei rădăcini $\alpha_1, \alpha_2, \ldots, \alpha_m$ sunt sunt exponenţii nenuli din dezvoltarea membrului stâng al ecuaţiei (A.2), iar coeficienţii sunt numere întregi. Prin urmare, relaţia (A.2) se poate scrie sub forma

$$e^{\alpha_1} + e^{\alpha_2} + \cdots + e^{\alpha_m} + k = 0, \tag{A.9}$$

unde k este un întreg (strict) pozitiv.

Introducem acum un polinom auxiliar,

$$f(x) = \frac{a^s x^{p-1}[P(x)]^p}{(p-1)!}, \tag{A.10}$$

unde $s = mp-1$, iar p este un număr prim a cărui valoare va fi precizată ulterior. Gradul lui f este

$$p - 1 + pm = pm - 1 + p = s + p.$$

Este de remarcat că polinomul $f(x)$ este un polinom cu coeficienţi complecşi, deci derivările pe care le vom face mai jos se referă la funcţii cu o variabilă complexă. Formal, însă, regulile sunt aceleaşi ca şi în cazul funcţiilor de o variabilă reală.

Definim, mai departe,

$$F(x) = f(x) + f'(x) + f^{(2)}(x) + \cdots + f^{(s+p)}(x). \tag{A.11}$$

Deoarece $f^{(s+p+1)}(x) = 0$, remarcăm că derivata funcţiei $e{-}xF(x)$ este $e{-}xf(x)$, fapt de care vom avea nevoie în cele ce urmează. Într-adevăr, avem

$$\frac{d}{dx}\left[e^{-x}F(x)\right] = e^{-x}\left[f'(x) + f^{(2)}(x) + \cdots + f^{(s+p)}(x)\right] -$$
$$- e^{-x}\left[f(x) + f'(x) + f^{(2)}(x) + \cdots + f^{(s+p)}(x)\right] = e^{-x}f(x).$$

În cele ce urmează, x va fi privit ca fiind un număr complex arbitrar, dar fixat şi considerăm funcţia dată de

$$\phi(u) = e^{-xu} F(xu),$$

unde u este o variabilă *reală*. Prin urmare, ϕ este o funcţie cu valori complexe, de o variabilă reală. Derivarea şi integrarea acestor funcţii sunt definite aplicând aceste operaţii separat părţii reale şi părţii imaginare, ambele fiind funcţii reale de o variabilă reală. Este foarte uşor de verificat că teorema Leibniz-Newton se extinde la acest gen de funcţii, sub forma:

$$\phi(b) - \phi(a) = \int_a^b \phi'(u) du.$$

Scopul nostru este să aplicăm această teoremă intervalului [0, 1]. În acest scop, trebuie să calculăm $\phi'(u)$. Folosind schimbarea de variabilă

$$z = ux,$$

putem scrie

$$\phi(u) = e^{-z} F(z).$$

Rezultă că

$$\phi'(u) = \frac{d}{dz}[e^{-z} F(z)] \cdot \frac{dz}{du} = -e^{-z} f(z) \cdot x = -xe^{-z} f(ux).$$

Aplicăm acum teorema Leibniz-Newton pe intervalul [0, 1] şi obţinem

$$\begin{aligned} \phi(1) - \phi(0) &= \int_0^1 \phi'(u) du, \\ e^{-x} F(x) - e^{-0} F(0) &= \int_0^1 -xe^{-ux} f(ux) du, \\ F(x) - e^{x} F(0) &= \int_0^1 -xe^{(1-u)x} f(ux) du \end{aligned}$$

Lăsându-l pe x să ia, pe rând, valorile $\alpha_1, \alpha_2, \ldots, \alpha_m$ şi însumând rezultatele, obţinem

$$\sum_{j=1}^{m} F(\alpha_j) + kF(0) = -\sum_{j=1}^{m} \int_0^1 e^{(1-u)\alpha_j} f(u\alpha_j) du. \tag{A.12}$$

Planul nostru de a obţine o contradicţie cu ipoteza că π este un număr algebric este să alegem numărul prim p astfel încât membrul stâng al ecuaţiei (A.12) să fie un număr întreg nenul, iar membrul drept să fie un număr arbitrar de mic (în particular, subunitar).

Începem prin a demonstra că $\sum_{j=1}^{m} F(\alpha_j)$ *este un întreg, divizibil cu* p. Într-adevăr, utilizând definiţia lui F, obţinem

$$\sum_{j=1}^{m} F(\alpha_j) = \sum_{j=1}^{m} \sum_{r=0}^{s+p} f^{(r)}(\alpha_j) = \sum_{r=0}^{s+p} \sum_{j=1}^{m} f^{(r)}(\alpha_j).$$

Pentru $0 \le r < p$,

$$\sum_{j=1}^{m} f^{(r)}(\alpha_j) = 0,$$

deoarece, prin definiţie lui f, $f^{(r)}(\alpha_j)$ are cel puţin un factor $P(\alpha_j)$, care este egal cu zero. Astfel,

$$\sum_{j=1}^{m} F(\alpha_j) = \sum_{r=p}^{s+p} \sum_{j=1}^{m} f^{(r)}(\alpha_j).$$

Fie acum r arbitrar, dar fixat, cu $p \le r \le s+p$. Întrucât $a^{-s}(p-1)!f(x)$ este o funcţie polinomială cu coeficienţi întregi, coeficientul fiecărui termen nenul al derivatei sale de ordinul r conţine un produs de r (deci, cel puţin p) întregi consecutivi. Prin urmare, coeficientul respectiv este divizivil cu $p!$. Astfel, fiecare coeficient al lui $f^{(r)}(x$ este divizibil cu $a^s p)$, aşadar expresia

$$\sum_{j=1}^{m} \frac{1}{pa^s} f^{(r)}(u_j)$$

este un polinom simetric cu coeficienţi întregi de variabilele $u_1, u_2, \ldots, u_m$, de aceea el poate fi exprimat ca un polinom cu coeficienţi întregi în funcţiile simetrice elementare. Înlocuim acum variabilele cu valorile $\alpha_1, \alpha_2, \ldots, \alpha_m$ şi ne reamintim că pentru fiecare funcţie simetrică elementară avem:

$$\sigma_i(\alpha_1, \alpha_2, \ldots, \alpha_m) = (-1)^i \frac{a_{m-i}}{a}.$$

Întrucât gradul polinomului în σ_i este cel mult egal cu s, fiecare termen are forma unui întreg împărţit la o putere a lui a, nu mai mare de s. Astfel,

$$\sum_{j=1}^{m} f^{(r)}(\alpha_j) = p \left[a^s \sum_{j=1}^{m} \frac{1}{pa^s} f^{(r)}(\alpha_j) \right],$$

unde termenul dintre parantezele drepte este un număr întreg. Deoarece această afirmaţie este adevărată pentru orice r astfel încât $p \le r \le s + r$, suma făcută după aceste valori ale lui r este un întreg divizibil cu p. Cum această sumă este egală cu expresia originală, demonstraţia afirmaţiei noastre este completă.

În continuare, vom demonstra că *pentru* p *suficient de mare,* $kF(0)$ *este, de asemenea, un număr întreg, dar* nedivizibil *cu* p.

Într-adevăr, termenii lui $F(0)$ sunt de trei tipuri:

- Termenii $f^{(r)}(x)$, pentru $0 \leq r \leq p-2$ conţin, cu toţii, un factor x, deci se anulează pentru $x = 0$.
- Termenii $f^{(r)}(x)$, pentru $p \leq r \leq s + p$ sunt polinoame cu coeficienţi întregi, fiecare coeficient fiind divizibil cu p, după cum s-a văzut mai sus. Astfel, $f^{(r)}(0)$, termenii constanţi, sunt întregi divizibili cu p.
- Pentru a ne asigura că numărul $kF(0)$ nu este divizibil cu p este, prin urmare, suficient să ne asigurăm că singurul termen rămas, adică $kf^{(p-1)}(0)$, nu este divizibil cu p.

  Din definiţia lui f, rezultă că singurul termen care contribuie la $f^{(p-1)}(0)$ este
  $$\frac{a^s a_0^p}{(p-1)!} x^{p-1}.$$
  Prin urmare,
  $$kf^{(p-1)}(0) = ka^s a_0^p.$$
  În consecinţă, dacă p este orice număr prim strict mai mare decât k, a şi a_0, atunci p nu poate să dividă produsul $ka^s a_0^p$.

Revenim acum la ecuaţia (A.12). Am reuşit să demonstrăm că, pentru p suficient de mare, membrul stâng este un întreg nenul (pentru că este suma dintre un întreg divizibil cu p şi unul nedivizibil cu p). Mai rămâne să demonstrăm că, din nou, pentru p suficient de mare, membrul drept al acestei egalităţi poate fi făcut subunitar, de unde va rezulta contradicţia căutată.

Avem
$$\left| -\sum_{j=1}^{m} \int_0^1 e^{(1-u)\alpha_j} f(u\alpha_j) du \right| =$$
$$= \left| -\sum_{j=1}^{m} \int_0^1 e^{(1-u)\alpha_j} \left[\frac{a^s (u\alpha_j)^{p-1} [P(u\alpha_j)]^p}{(p-1)!} \right] du \right| \leq$$
$$\leq \int_0^1 \sum_{j=1}^{m} \left| \frac{\left[a^m (u\alpha_j) P(u\alpha_j)\right]^{p-1}}{(p-1)!} \alpha_j e^{(1-u\alpha_j)} a^{m-1} P(u\alpha_j) \right| du,$$
deoarece
$$a^s = a^{mp-1} = (a^m)^{p-1} a^{m-1}.$$

Fie B o margine superioară uniformă pentru $1 \leq j \leq m$ a funcţiilor continue

$$\left| a^m (u\alpha_j) P(u\alpha_j) \right|$$

pe intervalul închis $0 \leq u \leq 1$ şi fie C o margine superioară a funcţiei continue

$$\sum_{j=1}^{m} \left| \alpha_j e^{(1-u\alpha_j)} a^{m-1} P(u\alpha_j) \right|$$

pe acelaŞi interval. Atunci expresia originală este mărginită superior de

$$\frac{CB^{p-1}}{(p-1)!}. \tag{A.13}$$

Cum această margine superioară este termenul de ordinul p în seria MacLaurin a funcţiei (de variabilă B) Ce^B, iar această serie se ştie că este convergentă, rezultă că expresia (A.13) trebuie să tindă la zero, atunci când $p \to \infty$. Dar asta înseamnă tocmai că membrul drept al relaţiei (A.12) poate fi făcut arbitrar de mic (şi, în particular, subunitar) dacă numărul prim p este suficient de mare. $\square$

Bibliografie

[1] Argunov, V.I., Balk, M.B. – *Construcţii geometrice în plan* (în limba rusă), ediţia a II-a, Moscova, 1957

[2] Alexandrov, I. – *Probleme de construcţii geometrice*, Ed. Tehnică, 1951

[3] Buicliu, Gh. – *Probleme de construcţii geometrice cu rigla şi compasul*, Ed. Tehnică, 1957

[4] Enriques, F. – *Questioni riguardanti le matematiche elementari*, ediţia a III-a, vol. II, Nicola Zanichelli, Bologna, 1900

[5] Fourrey, E. – *Curiosités géométriques*, 2e edition, Vuibert et Nony, Paris, 1910

[6] Gerwien, P. – *Zerschneidung jeder beliebigen Anzahl von gleichen geradlinigen Figuren in dieselben Stücke*, Journal für die reine und angewandte Mathematik, 1833

[7] Guitel, E. – *Propriétés relatives aux polygones équivalents*, Assoc. fr. p. l'av. des Sciences, 1895

[8] Hadlock, C.R., *Field Theory and its Classical Problems*, Mathematical Association of America, 1978

[9] Hurwitz, A. – *Beweis der Transzendenz der Zahl e*, Math. Ann., vol. **43** (1893), pp. 220-221

[10] Jones, A., Morris, S.A., Pearson, K.R., *Abstract Algebra and Famous Impossibilities*, Springer, 1991

[11] Lindemann, F., *Über die Zahl π*, Math. Ann., **20** (1882), pp. 213–225

[12] Niven, I. – *The transcendence of* π, Amer. Math. Monthly, vol. **46** (1939), pp. 469–471

[13] Tóth, A. – *Noţiuni de teoria construcţiilor geometrice*, Ed. Didactică şi Pedagogică, 1963