Índex

1. Introducció

El present treball de recerca l'he realitzat amb la col·laboració i el suport de la Universitat Autònoma de Barcelona a través del programa Argó. Des de la universitat se'm van proposar una sèrie de temes entre els quals aquest em va semblar molt interessant per diverses raons. Primer perquè uneix dues matèries que m'agraden molt, com són les matemàtiques i el dibuix tècnic. I, a més a més, el fet de plantejar-me un treball en el que hagués de partir de zero, perquè mai abans havia treballat en aquest tema, em va semblar molt interessant i encoratjador.

La construcció amb regle i compàs ha resultat ser un tema més ampli i teòric del que a priori m'havia semblat. Des d'un bon principi em va atraure molt que els tres problemes clàssics que es van plantejar ja a l'Antiga Grècia no siguin resolubles amb regle i compàs; estic parlant de la quadratura del cercle, la duplicació del cub i la trisecció d'un angle. També em va sorprendre el fet de que no es pogués demostrar la seva irresolubilitat fins al segle XIX, quan es van poder determinar quins nombres són construïbles amb regle i compàs. Per aquest motiu, he plantejat com a objectiu principal del meu treball de recerca la caracterització dels nombres construïbles, és a dir, arribar a saber quins nombres són construïbles amb regle i compàs i per què. I, a més a més, aplicar els resultats obtinguts per demostrar la irresolubilitat dels tres problemes clàssics i per determinar quins polígons regulars són construïbles amb regle i compàs.

El treball comença amb una breu introducció històrica per centrar quan apareixen les construccions geomètriques amb regle i compàs i per quin motiu, i també quan es van plantejar els tres problemes clàssics. A part d'aquesta introducció històrica, el meu treball de recerca consta de quatre parts.

La primera part és un apartat sobre àlgebra, que aparentment no està relacionat amb les construccions amb regle i compàs, però que quan em vaig introduir en aquest treball em vaig adonar que em faltaven un sèrie de coneixements d'àlgebra per poder entendre molts conceptes i demostracions.

La segona part del meu treball és la demostració del teorema de Wantzell, que determina quins números són construïbles, però per arribar a demostrar aquest teorema he hagut de començar explicant el concepte de construcció amb regle i compàs i de número construïble.

En la tercera part del treball he aplicat la caracterització dels nombres construïbles per demostrar la irresolubilitat dels tres problemes clàssics i per determinar quins polígons regulars són construïbles. Com a exemple, he donat un mètode de construcció amb regle i compàs d'un pentàgon regular i l'he demostrat matemàticament.

L'última part del treball és una part pràctica, l'elaboració d'una pàgina web. Aquesta web és interactiva i permet comprovar algunes de les construccions amb regle i compàs fetes en el treball.

2. Història

Des dels seus orígens l'home ha intentat representar el món i podem considerar que aquestes representacions són l'origen de la geometria. Es pot dir que l'home primitiu, en intentar representar el medi on vivia, reflectia en forma de figures esquemàtiques la realitat que observava, és a dir, les pintures rupestres poden ser considerades l'origen de la geometria.

La geometria per als egipcis, babilonis i altres pobles antics orientals, com els indis o els xinesos, consistia en un conjunt de regles i coneixements pràctics obtinguts experimentalment, però no era una ciència estructurada. No va ser fins el segle VII a.C, quan es va introduir la geometria a Grècia des d'Egipte, que no va desenvolupar-se i començar a estructurar-se com una ciència deductiva.

La geometria grega parteix dels coneixements pràctics de les civilitzacions anteriors i fa un pas cap a l'abstracció. Així, van arribar a les formes geomètriques perfectes a través de l'observació de la naturalesa. Euclides és el màxim representant, és considerat el pare de la geometria. En la seva obra *Els elements* agrupa tot el coneixement i formalitza la geometria com una ciència deductiva. Aleshores necessiten crear instruments per poder representar les figures que s'imaginaven i van crear, entre d'altres, el regle i el compàs.

Els grecs no podien fer càlculs aritmètics, perquè el seu sistema de numeració només representava els nombres naturals, no tenia el zero, els negatius, ni els decimals. Això significa que, per exemple, ells no podien dividir cinc entre dos i obtenir 2'5, perquè 2'5 no és un nombre natural o "sencer". Per tant, quan es van trobar amb el problema de trobar el punt mig d'un segment no van recorre al càlcul aritmètic i dividir la longitud entre dos, sinó que es van ajudar de la geometria. Com que la recta i la circumferència eren considerades les figures ideals, es van basar en el regle i el compàs per fer totes les construccions. Aquesta també és la raó per la qual el regle no té marques, si no tenien aritmètica no els hi servia de res, simplement l'utilitzaven per traçar rectes. Els grecs solucionaven els problemes gràficament, fent construccions amb regle i compàs, com a substitució de l'aritmètica.

Durant la segona meitat del segle V a.C. es va produir un gran desenvolupament de la geometria, aquest període s'anomena "l'època heroica de les matemàtiques" perquè en tota la història mai s'ha enfrontat l'home amb problemes tant fonamentals, amb tan poques eines. En aquesta època els pensadors grecs es dediquen a l'estudi de qüestions purament teòriques, un canvi respecte les matemàtiques anteriors que sempre s'havien dedicat a resoldre problemes pràctics de la vida ordinària. És en aquest període quan es plantegen els tres problemes clàssics:

- La quadratura del cercle. Consisteix en construir amb regle i compàs un quadrat que tingui la mateixa àrea que un cercle donat.

  La primera referència històrica que es té respecte aquest problema és d'Anàxàgores, un dels matemàtics de l'època heroica, als voltants del 450 a.C.

- La duplicació del cub. Donada l'aresta d'un cub, consisteix en construir amb regle i compàs l'aresta d'un altre cub que tingui el doble de volum que el primer. Existeix una llegenda grega que explica l'origen del problema de la duplicació del cub. Explica que el 427 aC, quan una epidèmia assolava la ciutat d'Atenes, els atenencs van demanar ajuda a l'oracle de Delfos i aquest els hi va dir que construïssin un altar cúbic el doble de gran que l'actual. Els habitants van construir un que tenia el doble de costat, però l'epidèmia no es va acabar perquè n'havien construït un vuit vegades més gran.

- La trisecció d'un angle. Donat un angle arbitrari, consisteix en construir amb regle i compàs un angle que tingui un terç de l'obertura de l'angle donat.

  D'aquest problema no se'n coneix l'origen, només se sap que també data de l'antiga Grècia, possiblement de la mateixa època que els altres dos.

Més de 2200 anys després es va demostrar que aquests tres problemes són irresolubles utilitzant només regle i compàs. Tot i això, l'estudi d'aquests problemes ha contribuït de forma molt important en el desenvolupament de les matemàtiques gràcies als esforços fets per resoldre'ls, tant per part de la matemàtica grega com per pensadors matemàtics molt posteriors.

La impossibilitat de duplicar el cub i trisecar un angle va ser demostrada per Pierre Wantzel (1814-1848) l'any 1837 i la impossibilitat de quadrar el cercle es va demostrar quan Lindemann (1852-1939) va demostrar l'any 1882 que el número π és transcendent.

3. Conceptes algebraics

Per poder fer el meu treball de recerca he necessitat molts conceptes d'àlgebra nous, que no he treballat al batxillerat, i he decidit posar aquest apartat d'àlgebra.

3.1 Grup

Sigui G un conjunt en el qual hi ha definida una *operació interna* "$\circ$", és a dir, una operació que compleix que $\forall a, b \in G \quad a \circ b \in G$. Diem que ($G$, $\circ$), el conjunt G amb aquesta operació $\circ$, és un *grup* si compleix les següents propietats:

Associativa: $a \circ (b \circ c) = (a \circ b) \circ c \quad \forall a, b, c \in G$

Existeix element neutre: $\forall a \in G$ existeix $e \in G \mid a \circ e = e \circ a = a$

Existeix l'element simètric: $\forall a \in G$ existeix $a' \in G \mid a \circ a' = e$

(G, $\circ$) és un *grup commutatiu* si, a més a més, compleix la propietat:

Commutativa: $a \circ b = b \circ a \quad \forall a, b \in G$

Si l'operació interna té notació additiva "+" l'element neutre es denota 0; i si té notació de multiplicació "$\cdot$"es denota 1.

Exemple: El conjunt dels nombres enters amb l'operació suma és un grup commutatiu ($\mathbb{Z}$,+). En canvi, no ho és amb l'operació producte perquè no existeix l'element simètric.

3.2 Anell

Sigui A un conjunt en el qual hi ha definides dues operacions internes, "+" i "$\cdot$". El conjunt A amb aquestes dues operacions és un *anell* (A,+,$\cdot$) si amb l'operació "+" és un grup commutatiu (A,+) i amb l'operació "$\cdot$" verifica les següents propietats:

Associativa: $a \cdot (b \cdot c) = (a \cdot b) \cdot c \quad \forall a, b, c \in A$

Distributiva respecte de la suma $a \cdot (b + c) = a \cdot b + a \cdot c \quad \forall a, b, c \in A$

(A,+,$\cdot$) és un anell commutatiu si, a més a més, compleix la propietat:

Commutativa: $a \cdot b = b \cdot a \quad \forall a, b \in A$

Exemple: El conjunt dels nombres enters amb les operacions suma i producte és un anell commutatiu $(\mathbb{Z},+,\cdot)$.

3.3 Cos algebraic

Sigui K un conjunt en el que hi ha definides dues operacions internes "+", "$\cdot$". El conjunt K amb aquestes dues operacions és un *cos algebraic*, també anomenat simplement cos, si $(K,+,\cdot)$ si verifica les següents propietats:

Associativa: $a+(b+c)=(a+b)+c \quad a\cdot(b\cdot c)=(a\cdot b)\cdot c \quad \forall a,\, b,\, c\in K$

Element neutre: $\forall a\in K \quad a+0=a \quad a\cdot 1=a$

Element simètric: $\forall a\in K$ existeix $-a\in K \mid a+(-a)=0$ i

$$\forall a\in K,\ a\neq 0 \quad \text{existeix } a^{-1}\in K \mid a\cdot a^{-1}=1$$

Commutativa: $a+b=b+a \quad a\cdot b=b\cdot a \quad \forall a,\, b\in K$

Distributiva respecte a la suma: $a\cdot(b+c)=a\cdot b+a\cdot c \quad \forall a,b,c\in K$

Podem observar que si $(K,+,\cdot)$ és un cos, aleshores $(K,+)$ i $(K,\cdot)$ són grups commutatius.

Exemple: El conjunt dels nombres racionals amb les operacions suma i producte és un cos $(\mathbb{Q},+,\cdot)$.

Un exemple interessant és el cos $(\mathbb{Z}/\text{p}\mathbb{Z},+,\cdot)$ on p és un número primer. El conjunt d'elements del cos són $\mathbb{Z}/\text{p}\mathbb{Z}=\{0,1,2...\text{p-1}\}$. Les operacions internes del cos "+" i "$\cdot$" són la suma i el producte dels enters, sota la relació de equivalència $\text{a}\equiv\text{b}$ si $\frac{\text{b - a}}{\text{p}}$ és un nombre enter, o el que és el mateix, a i b son equivalents si donen el mateix residu al dividir-los entre p. Els elements d'aquest cos són el residu de dividir un nombre natural entre el nombre primer p.

3.4 Espai vectorial

Sigui $(K,+,\cdot)$ un cos i E un conjunt en el qual hi ha definida una operació interna "$\oplus$" i una operació externa "$\otimes$", és a dir, $\forall\lambda\in K \quad i \quad \forall v\in E \quad \lambda\otimes v\in E$. $(E,\oplus,\ \otimes)$ és un *espai vectorial* sobre el cos K si verifica les següents propietats:

$(E,\oplus)$ és un grup commutatiu.

$\forall\lambda,\mu\in K \quad i \quad \forall v,w\in E \qquad \lambda\otimes(\mu\otimes v)=(\lambda\cdot\mu)\otimes v$

$\forall v\in E \quad 1\otimes v=v$

$\forall\lambda\in K \quad i \quad \forall v,w\in E \qquad \lambda\otimes(w\oplus v)=(\lambda\otimes w)\oplus(\lambda\otimes v)$

$\forall\lambda,\mu\in K \quad i \quad \forall v\in E \qquad (\lambda+\mu)\otimes v=(\lambda\otimes v)\oplus(\mu\otimes v)$

Quan treballem amb espais vectorials, als elements de *E* se'ls acostuma a dir *vectors* i als elements del cos *K escalars*. La notació que es fa sevir per les operacions vectorials "$\oplus$" i "$\otimes$" sol ser la mateixa que la que s'utilitza per la suma i el producte del cos *K*. L'operació externa $\otimes$ es diu producte per un escalar i també es diu que E és un *K-espai vectorial*.

Exemple: $\mathbb{R}^2$, el conjunt de vectors del pla, és un $\mathbb{R}$-espai vectorial.

3.4.1 Combinació lineal de vectors

En un espai vectorial *E* sobre un cos *K*, una *combinació lineal* de n vectors $v_1,v_2,.....v_n\in E$ és una expressió de la forma $\lambda_1\cdot v_1+\lambda_2\cdot v_2+.......+\lambda_n\cdot v_n$ on $\lambda_1,\lambda_2,.....\lambda_n\in K$.

3.4.2 Vectors linealment dependents

En un espai vectorial E sobre un cos *K*, diem que n vectors $v_1,v_2,.....v_n\in E$ són *linealment dependents* si existeixen $\lambda_1,\lambda_2,.....\lambda_n\in K$, no tots nuls, que compleixen $\lambda_1\cdot v_1+\lambda_2\cdot v_2+.......+\lambda_n\cdot v_n=0$ (0 és l'element neutre respecte de la suma).

3.4.3 Vectors linealment independents

En un espai vectorial E sobre un cos K, diem que n vectors $v_1, v_2, ... v_n \in E$ són *linealment independents*, si l'única solució de $\lambda_1 \cdot v_1 + \lambda_2 \cdot v_2 + ... + \lambda_n \cdot v_n = 0$ és $\lambda_1 = \lambda_2 = ... = \lambda_n = 0$

3.4.4 Bases d'un espai vectorial

En un espai vectorial E sobre un cos K, diem que n vectors $v_1, v_2, ... v_n \in E$ són una *base* de l'espai vectorial si són linealment independents i compleixen que tot vector $u \in E$ és combinació lineal de $v_1, v_2, ... v_n$.

3.4.5 Dimensió d'un espai vectorial

En un espai vectorial totes les bases tenen el mateix nombre de vectors, això és el teorema de la base[1]. Anomenem *dimensió* d'un espai vectorial sobre un cos al número de vectors que formen una base qualsevol de l'espai vectorial.

3.5 Extensió d'un cos

Si $(L,+,\cdot)$ és un cos algebraic i K un subconjunt de L, $K \subset L$, i es compleix que les operacions internes de L són també operacions internes de K, aleshores $(K,+,\cdot)$ és un cos algebraic contingut en L. Es diu que L és una *extensió del cos K* i que K és un *subcòs* de L.

Si L és una extensió del cos K, aleshores és fàcil verificar que L és un K-espai vectorial, perquè a l'operar un element de L per un element de K el resultat serà un element de L i, per tant, tindrem una operació externa definida en L. Com que L és un espai vectorial podem parlar de la seva dimensió. La dimensió de l'espai vectorial L sobre el cos K s'expressa com $[L:K]$.

Exemple: El cos dels nombres complexos $\mathbb{C}$ és una extensió del cos dels nombres reals $\mathbb{R}$, i per tant és un $\mathbb{R}$-espai vectorial. Una base d'aquest espai vectorial és $\{1, i\}$ i, per tant, la dimensió de l'espai vectorial $\mathbb{C}$ sobre el cos $\mathbb{R}$ és 2. $[\mathbb{C}:\mathbb{R}]=2$.

[1] Podreu trobar una demostració d'aquest teorema al llibre [5] de la bibliografia.

Més endavant s'utilitza un teorema d'extensió de cossos[2] que no es demostra, perquè no forma part de l'objectiu del treball, però sí que l'explicaré en un cas particular.

Teorema[3]: donats tres cossos $K \subset F \subset H$, es compleix que $[H:K] = [H:F] \cdot [F:K]$.

Per al nostre treball necessitem estudiar un cas particular d'extensió de cossos. Donat un número $\alpha \in \mathbb{R}$ definim $\mathbb{Q}(\alpha)$ com el cos extensió de $\mathbb{Q}$ més petit que conté α. Ara estudiarem diversos exemples d'extensions de cossos.

Exemple 1: Si $\alpha = \sqrt{3}$, aleshores $\mathbb{Q}(\sqrt{3}) = \{x + y\sqrt{3} \mid x, y \in \mathbb{Q}\}$. $\mathbb{Q}(\sqrt{3})$ és un $\mathbb{Q}$−espai vectorial, i $\{1, \sqrt{3}\}$ és una base, per tant, $[\mathbb{Q}(\sqrt{3}):\mathbb{Q}] = 2$.

Exemple 2: Ara veurem $\mathbb{Q}(\sqrt{3},\sqrt{7})$ com una extensió del cos $\mathbb{Q}(\sqrt{3})$. Aleshores, $\mathbb{Q}(\sqrt{3},\sqrt{7}) = \{x + y\sqrt{7} \mid x, y \in \mathbb{Q}(\sqrt{3})\}$. $\mathbb{Q}(\sqrt{3},\sqrt{7})$ és un $\mathbb{Q}(\sqrt{3})$-espai vectorial, i $\{1, \sqrt{7}\}$ és una base, per tant, $[\mathbb{Q}(\sqrt{3},\sqrt{7}):\mathbb{Q}(\sqrt{3})]=2$.

Exemple 3: Ara veurem $\mathbb{Q}(\sqrt{3},\sqrt{7})$ com una extensió del cos $\mathbb{Q}$. Aleshores, $\mathbb{Q}(\sqrt{3},\sqrt{7}) = \{x + y\sqrt{3} + z\sqrt{7} + t\sqrt{21} \mid x, y, z, t \in \mathbb{Q}\}$. $\mathbb{Q}(\sqrt{3},\sqrt{7})$ és un $\mathbb{Q}$-espai vectorial, i $\{1, \sqrt{3}, \sqrt{7}, \sqrt{21}\}$ és una base, per tant, $[\mathbb{Q}(\sqrt{3},\sqrt{7}):\mathbb{Q}] = 4$.

Amb aquest exemple es pot veure que es compleix el teorema:

$$[\mathbb{Q}(\sqrt{3},\sqrt{7}):\mathbb{Q}] = [\mathbb{Q}(\sqrt{3},\sqrt{7}):\mathbb{Q}(\sqrt{3})] \cdot [\mathbb{Q}(\sqrt{3}):\mathbb{Q}]$$

[2] Podreu trobar una demostració d'aquest teorema al llibre [4] de la bibliografia, concretament està explicat a la pàg.192.
[3] Teorema: és una proposició molt important o bé central d'una teoria.

4. Concepte de construcció amb regle i compàs

Les construccions amb regle i compàs consisteixen en el traçat de punts, segments de recta i arcs de circumferència emprant única i exclusivament un sol regle i compàs. El regle i compàs de les construccions geomètriques no són instruments físics reals, són conceptes matemàtics abstractes, amb diferències notables amb el regle i compàs del món real. Es considera que el regle té longitud infinita i que no té cap marca que permeti mesurar o traslladar distàncies. També es considera que només té una vora, ja que dues vores paral·leles permetrien traçar rectes paral·leles. És a dir, que un regle només es pot utilitzar per traçar una recta que passi per dos punts prèviament existents, o bé prolongar un segment donat. El compàs pot traçar circumferències de qualsevol radi, però sempre partint de dos punts coneguts, un que sigui el centre i l'altre que determini el radi. Amb un compàs no es pot traslladar una distància, és com si a l'aixecar el compàs s'ajuntessin automàticament els dos braços. Aquest aspecte sembla molt molest, però matemàticament és irrellevant, ja que es poden traslladar distàncies indirectament, com més endavant s'explicarà.

4.1 Punts construïbles

Partint d'un conjunt inicial de n punts del pla $S_0=\{q_1, q_2,...q_n\}$ amb regle i compàs podem traçar rectes i circumferències:

- Una recta és *traçable* a partir de S_0 si passa per, al menys, dos punts de S_0.
- Una circumferència és traçable a partir de S_0 si té per centre un punt de S_0 i passa per altre punt de S_0.

Perquè un punt sigui construïble amb regle i compàs a partir de un conjunt de punts S_0 del pla ha de complir una, o més, de les següents condicions:

- Ser un punt del conjunt S_0.
- Ser un punt d'intersecció de dues rectes traçables a partir de S_0.
- Ser un punt d'intersecció de dues circumferències traçables a partir de S_0.
- Ser un punt d'intersecció d'una recta i una circumferència traçables a partir de S_0.

Partint d'un cert conjunt de punts S_0 del pla obtenim el conjunt S_1, format per tots els punts del pla construïbles amb regle i compàs a partir de S_0. De la mateixa manera, construïm S_2 a partir de S_1, i repetint aquest procés obtenim una successió de conjunts S_n, en la qual cada conjunt conté als anteriors, és a dir: $S_0 \subset S_1 \subset S_2 \subset ... \subset S_n$

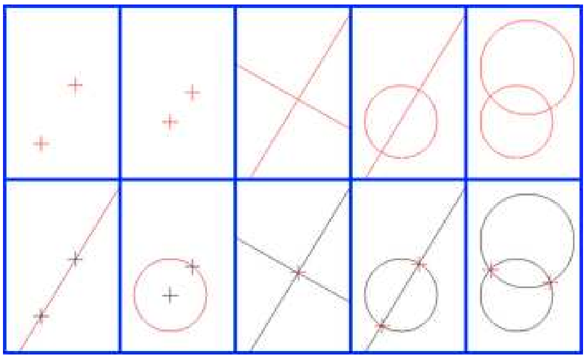
El límit superior d'aquests conjunts s'anomena $\overline{S}$ i s'expressa com $\overline{S} = \lim_{n \to \infty} S_n$.

$\overline{S}$ està format per tots els punts construïbles a partir de S_0. Per tant, un punt del pla és *construïble* amb regle i compàs a partir de S_0 si, i només si, pertany a $\overline{S}$.

Els punts del pla $\{(x,y)\ \forall x, y \in \mathbb{R}\}$ s'identifiquen amb els números complexos $\mathbb{C} = \{x + yi \quad \forall x, y \in R\}$. Els nombres reals són els nombres complexos de la forma $x + 0i$, és a dir, els nombres reals s'identifiquen amb els punts del pla de la forma $\mathbb{R} = \{(x, 0)\ \forall x \in \mathbb{R}\}$ i per tant $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{R} \subset \mathbb{C}$

4.2 Construccions bàsiques amb regle i compàs

Tota construcció amb regle i compàs es basa en la realització de només tres accions bàsiques:



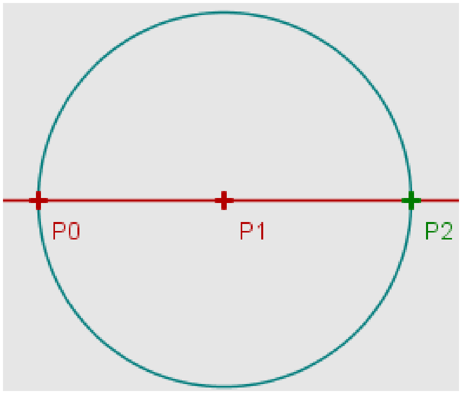
- Traçar la recta que uneixi dos punts.
- Traçar la circumferència que tingui de centre un punt donat i passi per un altre punt donat.
- Determinar el punt d'intersecció de dues rectes, una recta i una circumferència, o bé dues circumferències.

En aquest treball determinaré quins punts del pla són construïbles a partir de dos punts qualsevol, o sigui, el cas $S_0=\{q_1, q_2\}$. Establim un sistemes de coordenades al pla prenent q_1 com l'origen d'aquest sistema de coordenades i la distància entre q_1 i q_2 com la unitat. La recta determinada pels punts q_1 i q_2 és l'eix d'abscisses. En aquest sistema els punts q_1=(0,0) i q_2=(1,0).

Ara veurem algunes construccions senzilles que podem fer amb regle i compàs. A partir dels punts que es van obtenint mitjançant les construccions bàsiques amb regle i compàs arribaré a deduir alguns conjunts de nombres que són construïbles amb regle i compàs a partir de dos punts.

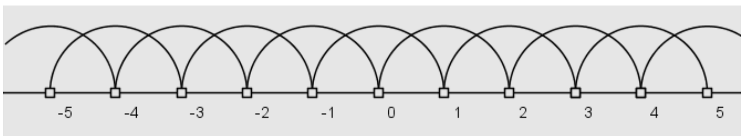
Definim S com el conjunt de punts del pla construïbles a partir de S_0.

4.2.1 Simètric d'un punt respecte un altre

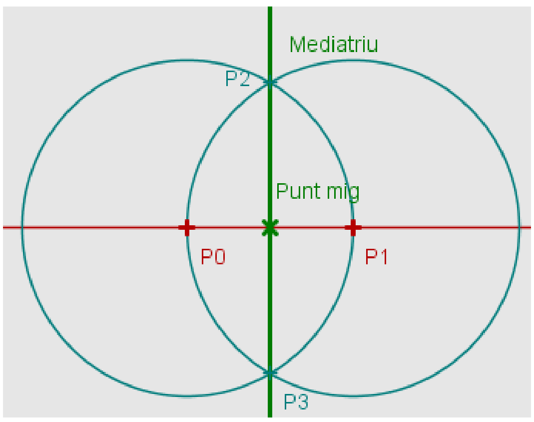


Donats dos punts qualsevol del pla p_0, p_1 tracem la recta que els uneix. Després, amb el compàs, dibuixem la circumferència de centre p_1 i que passi per p_0. Anomenem p_2 al punt d'intersecció de la recta i la circumferència, i és el simètric de p_0 respecte p_1.

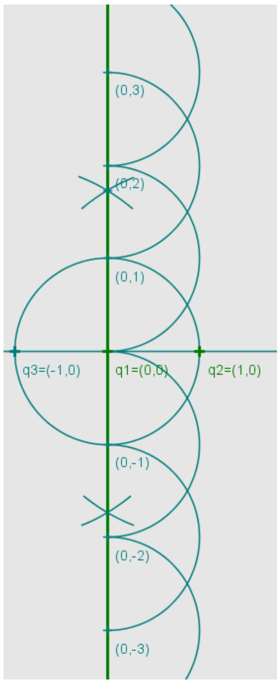
Aplicat al nostre cas, el simètric de q_1 (0,0) respecte de q_2 (1,0) és el punt (2,0), que per tant és construïble. Repetint aquest procés podem demostrar que tots els nombres naturals de la forma (n,0) són construïbles. Realitzant el mateix procés en sentit oposat, obtenim que tots els punts (-n, 0) també són construïbles. Per tant, tenint en compte la identificació dels punts del pla amb els nombres complexos que hem explicat anteriorment, hem demostrat que els naturals i els enters són construïbles $\mathbb{N} \subset \mathbb{Z} \subset S$



4.2.2 Mediatriu d'un segment i obtenció del punt mig



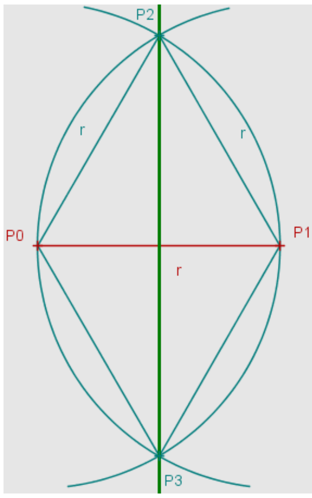
Donats dos punts del pla p_0, p_1 tracem el segment que els uneix. A continuació tracem la circumferència de centre p_0 que passa per p_1 i la circumferència de centre p_1 que passa per p_0. D'aquesta forma construïm dos nous punts, p_2 i p_3, que són els punts d'intersecció de les dues circumferències. Unint aquests dos punts obtenim la mediatriu del segment inicial.

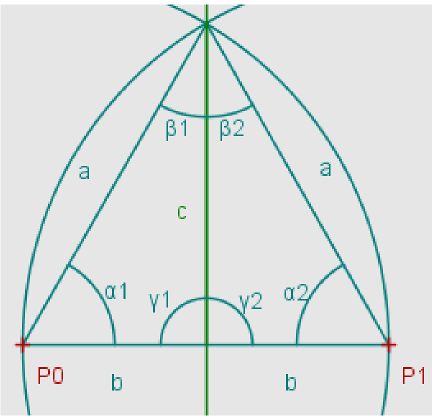


La intersecció de la mediatriu amb el segment inicial determina el punt mig del segment.

Aplicat al nostre cas, partint dels punts $q_1=(0,0)$ i $q_2=(1,0)$, podem trobar el simètric de q_2 respecte q_1 que serà $q_3=(-1,0)$. Tracem la mediatriu entre q_2 i q_3, que passarà per q_1, aquesta recta serà l'eix OY d'ordenades del sistema de referència. Si tracem la circumferència de centre q_1 i que passi per q_2 determinem els punts (0,1) i (0,-1). Repetint el procés de l'apartat anterior en l'eix d'ordenades construïm tots els punts (0,n) $\forall n \in \mathbb{Z}$.

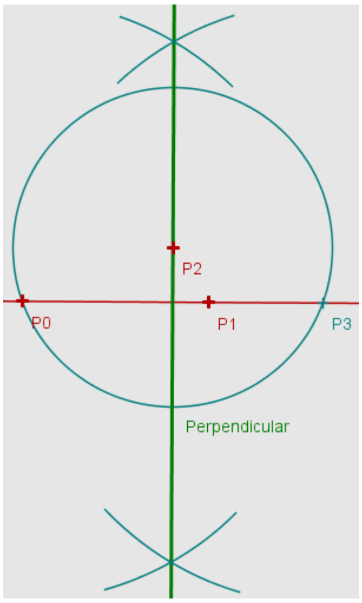
Ara comprovarem que la recta obtinguda mitjançant el mètode anterior és realment la mediatriu del segment inicial. Els dos radis de circumferència de centre p_0, p_1 són els punts que es troben a distància r de p_0 o p_1. Per tant, la intersecció dels dos arcs de circumferència, els punts p_2 *i* p_3, són punts que equidisten de p_0, p_1. La recta determinada per aquests dos punts són tots els punts que equidisten de p_0, p_1, és a dir, la mediatriu. El punt on talla amb el segment inicial és el punt mig, ja que és el punt que equidista de p_0, p_1.





Com que els dos triangles tenen els tres costats iguals a,b,c; això implica que són triangles idèntics i que, per tant, els angles també seran iguals $\alpha_1=\alpha_2$; $\beta_1=\beta_2$; $\gamma_1=\gamma_2$. Els angles γ_1, γ_2 estan determinats sobre una mateixa recta, és a dir, són suplementaris i per tant sumen 180º. Si sabem que els dos angles són iguals i sumats valen 180º, $\gamma_1=\gamma_2=90$º. Això demostra que la mediatriu és perpendicular a la recta inicial determinada per p_0, p_1.

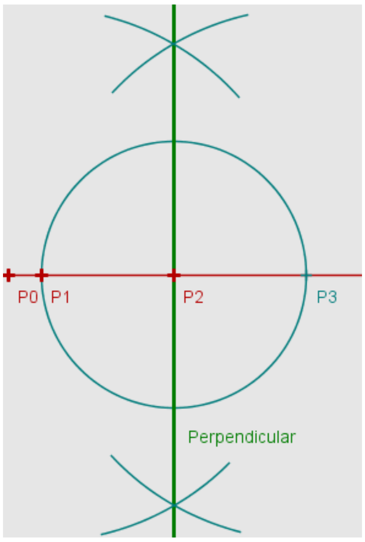
4.2.3 Perpendicular a una recta per un punt exterior[4]



Partim de tres punts p_0, p_1, p_2 no alineats. Dos punts p_0, p_1 determinen una recta i p_2 és un punt exterior a la recta. Tracem la circumferència de centre p_2 i radi la distància entre p_2 i p_0. Obtenim un altre punt p_3 de la recta, que podria coincidir amb p_1, en tal cas el seguiríem anomenant p_3. Si no obtenim cap punt, és a dir, si la circumferència és tangent a la recta en el punt p_0, hauríem de traçar una altre circumferència de centre p_2 i radi la distància entre p_2 i p_1, per tal d'obtenir p_3. Tracem la mediatriu entre p_0 i p_3, tal i com ja hem explicat en l'apartat anterior, aquesta mediatriu passarà per p_2 i, per tant, és la recta perpendicular a la recta determinada per p_0, p_1 que passa per p_2.

Aplicat al nostre cas, això ens permet demostrar que si un punt (x,y) és construïble, les seves projeccions sobre els eixos de coordenades també ho seran, és a dir, que (x,0) i (0,y) també seran construïbles.

4.2.4 Perpendicular a una recta per un punt de la pròpia recta

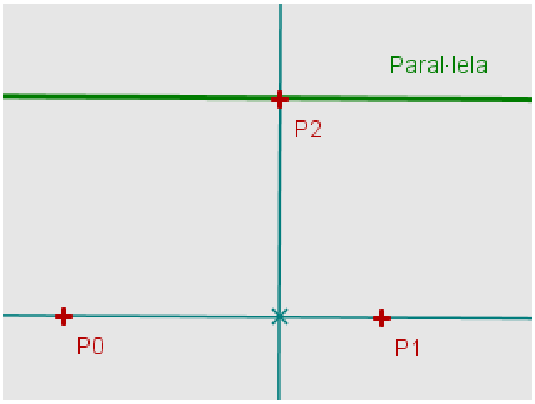


Partim de tres punts p_0, p_1, p_2 alineats. Dos punts p_0, p_1 determinen una recta i p_2 és un punt de la mateixa recta. Tracem el simètric de p_1 respecte p_2 i obtenim p_3. Després tracem la mediatriu entre p_1 i p_3. Aquesta mediatriu passarà per p_2 i serà la recta perpendicular a la recta determinada p_0, p_1.

Aplicat al nostre cas, això ens demostra que si els punts (x,0) i (0,y) són construïbles, aleshores també ho serà el punt de coordenades (x,y), ja que si tracem les perpendiculars als eixos que passen per aquests punts, la intersecció de les dues rectes serà el punt (x,y). Per tant, un punt (x,y) és construïble si, i només si, els punts (x,0) i (0,y) són construïbles.

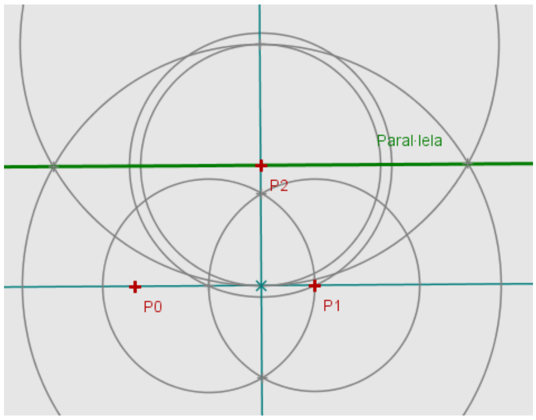
[4] En els annexos he inclòs un altre mètode per traçar la perpendicular a una recta per un punt exterior.

4.2.5 Paral·lela a una recta per un punt exterior[5]



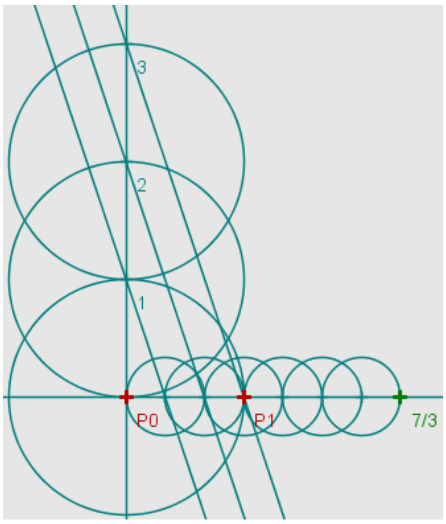
Partim de tres punts p_0, p_1, p_2 no alineats. Dos punts p_0, p_1 determinen una recta i p_2 és un punt exterior a la recta. Tracem la recta perpendicular a la recta determinada per p_0 i p_1 que passi per p_2. Després tracem la perpendicular a la recta obtinguda i que passi per p_2, seguint els passos indicats anteriorment. La recta resultant és la recta paral·lela a la inicial que passa per p_2.

Aplicat al nostre cas, això ens permet traçar totes les rectes horitzontals i verticals de coordenades enteres; i així demostrar que a partir de dos punts qualsevol del pla podem construir amb regle i compàs tots els punts de la forma (m,n) $\forall m,n \in \mathbb{Z}$.



Construcció seguint tots els passos necessaris

4.2.6 Divisió d'un segment en n parts iguals



A partir de dos punts p_0, p_1 tracem el segment que els uneix. Tracem la perpendicular a aquest segment que passa per p_0. Sobre aquesta perpendicular tracem n circumferències de radi la longitud del segment $\overline{p_0 p_1}$ i centre el punt d'intersecció de la circumferència anterior amb la perpendicular. Després tracem la recta que uneixi l'últim punt obtingut amb p_1 i tracem n paral·leles a la recta obtinguda que passin per les n divisions de la perpendicular. Els n punts de tall d'aquestes

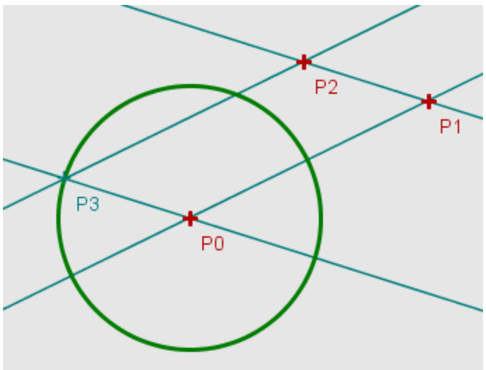
[5] En els annexos he inclòs un altre mètode per traçar la paral·lela a una recta per un punt exterior.

paral·leles amb el segment inicial són punts equidistants de longitud $\frac{\overline{p_0 p_1}}{n}$, on $\overline{p_0 p_1}$ és la longitud del segment.

Aplicat al nostre cas, per construir un racional de la forma (m/n,0) podem dividir el segment unitat en n parts iguals de longitud 1/n i, mitjançant el mateix procés que hem fet servir per trobar el punt simètric, tracem m circumferències consecutives de radi 1/n, i obtenim el punt (m/n,0). Per tant, $\forall x \in \mathbb{Q}\ (x,0) \in S$. És a dir, els racionals també són construïbles $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset S$

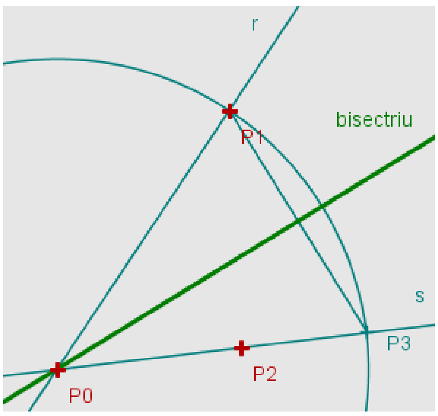
Ara ja sabem construir tots els números racionals partint, únicament, de dos punts donats.

4.2.7 Circumferència de radi la distància entre dos punts



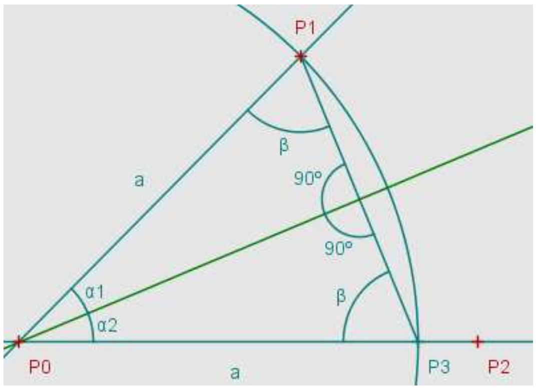
Donats tres punts p_0, p_1, p_2 no alineats volem traçar la circumferència de centre p_0 i radi la distància entre p_1 i p_2, és a dir, traslladar una distància. Com hem dit anteriorment, el compàs perd l'obertura en aixecar-se del full, per tant, no es pot traslladar una distància de forma directa. Hem de traçar la recta que uneix p_1 i p_2 i la recta que uneix p_0 i p_1. Després hem de traçar les rectes paral·leles a les anteriors que passen per p_0 i p_2 respectivament. El punt d'intersecció de les dues rectes l'anomenarem p_3 i la circumferència de centre p_0 i que passi per p_3 és la circumferència buscada.

4.2.8 Bisectriu d'un angle



Donats tres punts p_0, p_1, p_2 no alineats, tracem la recta que uneix p_0 i p_1 (recta r) i la recta que uneix p_0 i p_2 (recta s). Tracem una circumferència de centre p_0 i radi la distància entre p_0 i p_1, el punt d'intersecció d'aquesta circumferència amb la recta s l'anomenem p_3. Tracem el segment que uneix p_1 i p_3 i fem la mediatriu d'aquest segment. La recta obtinguda serà la bisectriu de l'angle determinat per p_1, p_0 i p_2.

Ara comprovarem que la recta obtinguda mitjançant el mètode anterior és realment la bisectriu de l'angle. Els punts p_1 i p_3 equidisten de p_0, ja que són punts d'una mateixa circumferència de centre p_0. Per tant, la mediatriu de p_1 i p_3 passarà pel vèrtex de l'angle, és a dir, per p_0. Com que el triangle determinat per p_0, p_1 i p_3 és isòsceles, els dos angles determinats pel costat diferent són iguals i com que els angles d'un triangle sumen 180º, podem determinar que:



$$\begin{cases} \alpha_1 + \beta + 90^\circ = 180^\circ \\ \alpha_2 + \beta + 90^\circ = 180^\circ \end{cases} \rightarrow \quad \alpha_1 = \alpha_2$$

Per tant, la mediatriu de p_1, p_3 és la bisectriu de l'angle determinat per p_1, p_0 i p_2.

4.3 Números construïbles

Un número real x és un número construïble si és una de les coordenades d'un punt construïble. Anomenarem $\mathcal{C}$ al conjunt de números construïbles. Dit d'una altra manera, $\forall\, x \in \mathbb{R}$, $x \in \mathcal{C}$ si existeix un punt $p \in S$ tal que $p=(x,a)$ o $p=(a,x)$.

4.3.1 Relació entre punts construïbles i números construïbles

Ara veurem que $S = \mathcal{C} \times \mathcal{C}$ (producte cartesià).

Proposició[6]: un punt del pla (x,y) és construïble si, i només si, x,y són números construïbles.

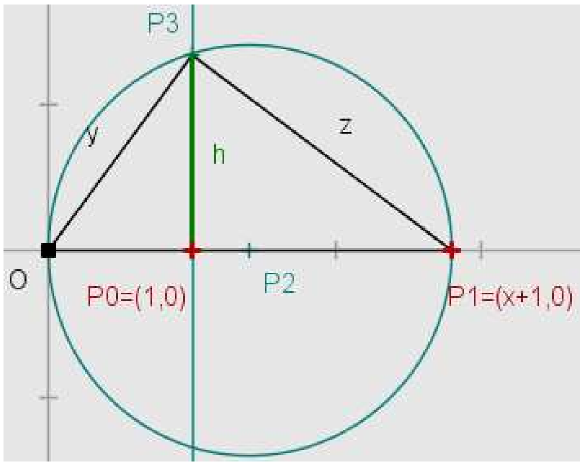
Demostració: per definició, si un punt és construïble les seves coordenades son números construïbles, és a dir, si $p=(x,y) \in S \Rightarrow x,y \in \mathcal{C}$.

[6] Proposició: és un enunciat que afirma una veritat partint d'una hipòtesi i aquesta veritat es demostra dins d'un marc lògic.

Recíprocament, si x és un número construïble, existeix un punt construïble *p* amb coordenades *p*=(x,a) o (a,x). Si *p*=(x,a) tracem la recta paral·lela a l'eix d'ordenades que passa per *p*. Aquesta recta talla a l'eix d'abscisses en el punt (x,0). Si fos *p*=(a,x), tracem la recta paral·lela a l'eix d'abscisses per construir el punt (0,x). A continuació, tracem la circumferència de centre (0,0) i que passa per (0,x), el punt d'intersecció d'aquesta circumferència amb l'eix d'abscisses és el punt (x,0). Podem fer el mateix raonament amb y per construir el punt (0,y). El punt (x,y) serà la intersecció de les rectes perpendiculars als eixos que passen pels punts (x,0) i (0,y). Per tant, si $x,y \in \mathcal{C} \Rightarrow q=(x,y)$ és construïble.

4.3.2 Arrel quadrada d'un número construïble positiu

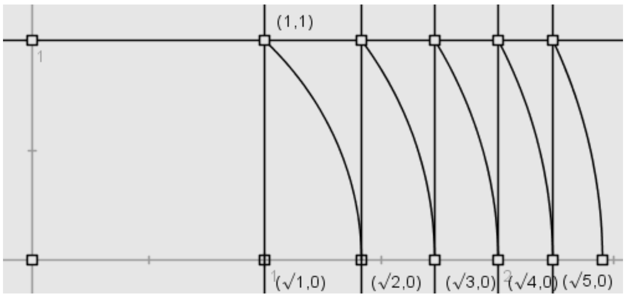
Si x és un nombre construïble positiu, per trobar la seva arrel quadrada, dibuixarem en els eixos de coordenades els punts $p_0(1,0)$ i $p_1(x+1,0)$. Trobem p_2, el punt mig de O i p_1. Traçarem la circumferència de centre p_2 i que passa per O i p_1. Després traçarem la perpendicular a l'eix OX que passa per p_0. Així trobarem p_3, el punt d'intersecció de la circumferència amb aquesta recta. L'angle format per O, p_3 i p_1 és de 90º, ja que la unió de qualsevol punt de la circumferència amb els extrems d'un diàmetre sempre forma un angle de recte. Els triangles de vèrtexs O,p_0,p_3; p_0,p_3,p_1; O,p_3,p_1 són rectangles. Si apliquem el teorema de Pitàgores obtenim que:



$$\begin{cases} y^2 = 1^2 + h^2 \\ z^2 = x^2 + h^2 \\ (x+1)^2 = y^2 + z^2 \end{cases}$$

$$(x+1)^2 = 1 + h^2 + x^2 + h^2 \rightarrow \; x^2 + 2x + 1 = 1 + h^2 + x^2 + h^2 \;\rightarrow\; 2x = 2h^2 \;\rightarrow\; h = \sqrt{x}$$

Un bon exemple de com construir les arrels quadrades dels nombres naturals és el següent. Tracem les perpendiculars als eixos pels punts (1,0) i (0,1), el punt d'intersecció serà (1,1). Tracem una circumferència de centre (0,0) i que passa per (1,1). Aplicant el teorema de Pitàgores podem determinar que el radi de la circumferència és

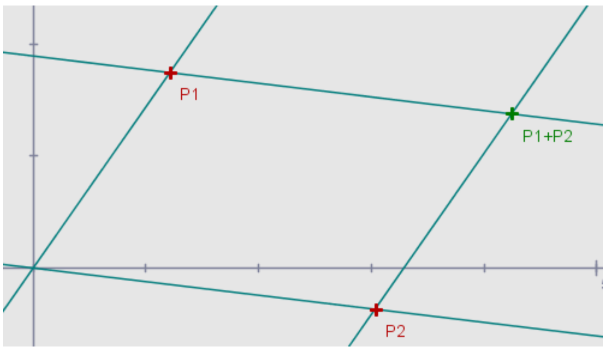


$\sqrt{2}$ i que, per tant, el punt d'intersecció d'aquesta circumferència amb l'eix d'abscisses és el punt ($\sqrt{2}$,0). Si ara tracem la perpendicular a l'eix d'abscisses per aquest punt, tallarà la perpendicular a l'eix d'ordenades en el punt ($\sqrt{2}$,1). Tornem a traçar una circumferència de centre (0,0) i que ara passi pel punt ($\sqrt{2}$,1). El radi d'aquesta circumferència serà $\sqrt{3}$ i, per tant, la intersecció de la circumferència amb l'eix d'abscisses serà el punt ($\sqrt{3}$,0). Repetint aquest procés obtenim les arrels quadrades de tots els nombres naturals.

4.4 Els cossos dels punts construïbles i dels números construïbles

4.4.1 Suma de punts construïbles

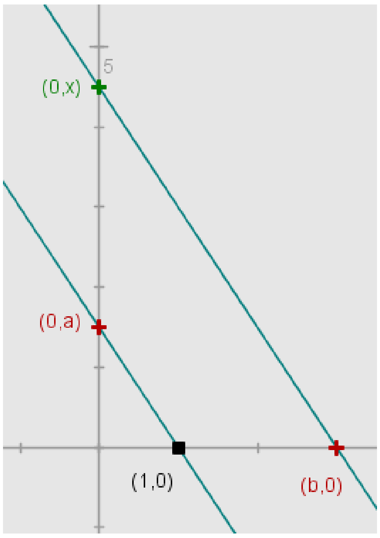
Coneixent la identificació dels nombres complexos amb els punts del pla, podem considerar l'operació suma de nombres complexos restringida als punts construïbles del pla *S*. Per sumar dos punts construïbles del pla $p_1(x_1,y_1)$ i $p_2(x_2,y_2)$ cal sumar les seves coordenades $p_3=p_1+p_2=(x_1+x_2, y_1+y_2)$. Per tal de que aquesta operació sigui una operació interna de S, cal que p_3 també sigui construïble.



En efecte, si unim p_1 i p_2 amb l'origen de coordenades i tracem les paral·leles a aquestes dues rectes que passin per p_1 i p_2, el punt de tall serà $p_3=p_1+p_2$. Per tant, la suma de dos punts construïbles és també un punt construïble. Tot punt p(x,y) té el seu oposat respecte a la suma $-p=(-x,-y)$, que és construïble ja que és el simètric de p respecte l'origen de coordenades. En la suma, també es compleixen les propietats associatives i commutatives dels complexos; i també té un element neutre construïble, el punt (0,0). Així que (S,+) és un grup commutatiu.

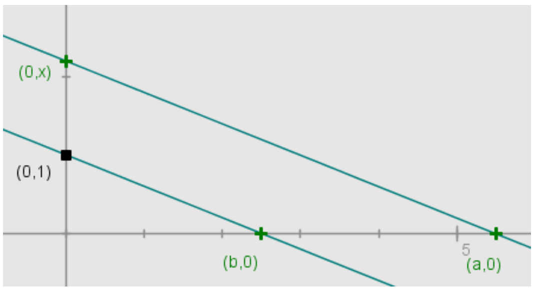
4.4.2 El cos dels números construïbles

Si a, b són números construïbles (a,b∈ $\mathcal{C}$) aleshores ja hem demostrat abans que els punts (a,0), (b,0) i (-b,0) són construïbles. Aplicant l'apartat anterior de suma de punts construïbles podem determinar que (a,0)+(b,0)=(a+b,0) i que, per tant, el punt (a+b,0) és construïble. Ja que és la coordenada d'un punt construïble, el número a+b també és construïble (a+b∈ $\mathcal{C}$). Podem aplicar el mateix raonament a l'operació (a,0)+(-b,0)=(a-b,0) i, per tant, demostrar que a-b també és un número construïble (a-b∈ $\mathcal{C}$).



Per demostrar que a·b és construïble, primer ens centrarem en demostrar que |a·b| és construïble, que és el mateix que considerar |a|·|b|, és a dir, considerarem a>0 i b>0. Després podrem generalitzar aquest cas a qualsevol a i b, ja que a·b pot tenir com a resultat |a·b| o -|a·b| i si |a·b| és construïble -|a·b| també ho serà perquè és el seu simètric respecte l'origen de coordenades.

Per demostrar-ho partirem dels punts construïbles (1,0), (b,0) i (0,a). Unim els punts (0,a) i (1,0) amb una recta i tracem una paral·lela que passi per (b,0). Pel teorema de Tales es determina que el punt de tall d'aquesta recta en l'eix OY és (0,a·b). Ja que per triangles semblants sabem que $\frac{a}{1}=\frac{x}{b} \to x=a\cdot b$



Pel mateix mètode podem obtenir a/b. Igual que en el cas del producte, podem considerar a i b positius. Construïm els punts (0,1), (a,0) i (b,0). A continuació, unim els punts (0,1) i (b,0) i tracem una paral·lela a aquesta recta per (a,0). El punt d'intersecció de la recta amb l'eix OY és el punt (0,a/b). Ja que pel teorema de Tales determinem que $\frac{1}{b}=\frac{x}{a} \to x=\frac{a}{b}$

Això fa que la suma i el producte siguin una operació interna de $\mathcal{C}$. Com que ja havíem vist que $\mathbb{N}\subset\mathbb{Z}\subset\mathbb{Q}\subset\mathcal{C}\subset\mathbb{R}\subset\mathbb{C}$, ara obtenim que ($\mathcal{C}$,+,·) és un cos algebraic.

Hem vist que els racionals són números construïbles i que la suma, resta, producte, divisió i arrel quadrada d'un número construïble és construïble. Per exemple, una expressió de la forma $\frac{3}{7}\sqrt{2+\sqrt{\frac{13}{3}-\sqrt{3}}}$ és construïble.

4.4.3 Producte de punts construïbles

De la mateixa manera que amb la suma, podem considerar l'operació producte de nombres complexos restringida als punts del pla *S*. Donats dos punts construïbles del pla $p_1(x_1,y_1)$ i $p_2(x_2,y_2)$ la aplicació del producte de nombres complexos estableix que $p_3=p_1\cdot p_2=(x_1x_2-y_1y_2,\ x_1y_2+y_1x_1)$. Com que els dos punts (p_1,p_2) són construïbles, les seves coordenades seran números construïbles i, per tant, el punt $p_1\cdot p_2$ també serà construïble ja que està determinat per la suma i producte de números construïbles i ja hem demostrat en el punt anterior que són construïbles. La multiplicació de complexos aplicada a *S* és correcte i compleix la propietat associativa, commutativa i té un element neutre, el punt (1,0). Tots els punts, excepte el (0,0), tenen un element simètric. Donat un punt $p=(x,y)$, el seu simètric respecte del producte és $\overline{p}=\left(\frac{x}{x^2+y^2},\frac{-y}{x^2+y^2}\right)$.

D'aquesta manera determinem que $(S,+,\cdot)$ també és un cos algebraic.

5. Caracterització dels nombres construïbles

Per demostrar la forma que tenen els nombres construïbles necessitem un seguit de conceptes algebraics que explicarem a continuació.

5.1 Números algebraics i transcendents

Sigui $(L,+,\cdot)$ un cos algebraic i K un subcòs de L, un element $\alpha \in L$ diem que és un *número algebraic* sobre K si α és arrel d'un polinomi amb coeficients en K, és a dir, si existeixen $\lambda_i \in K$ tals que $\lambda_0+\lambda_1\alpha+\lambda_2\alpha^2+...+\lambda_n\alpha^n=0$ amb $\lambda_n \neq 0$. En cas contrari, direm que α és un *número transcendent* sobre K.

Un número real a es diu algebraic si és un número algebraic sobre $\mathbb{Q}$, és a dir, si existeix un polinomi P(x) amb coeficients en $\mathbb{Q}$ tal que $P(a)=0$. Per exemple, el número $\sqrt{2}$ és algebraic sobre $\mathbb{Q}$, perquè és arrel del polinomi $P(x)= x^2-2$.

Actualment es coneixen molt pocs nombres transcendents i és molt difícil demostrar que un número és transcendent. Hermite (1822-1901), l'any 1873, va demostrar que el número e és transcendent sobre $\mathbb{Q}$ i l'any 1882 Ferdinand Lindemann (1852-1939) va demostrar que també π és transcendent[7].

El conjunt de números reals algebraics és numerable[8], o sigui que es pot posar en correspondència bijectiva amb els números naturals. Si tenim en compte que el conjunt de nombres reals no és numerable, podem deduir que el conjunt de nombres transcendents és no numerable, i per tant, hi ha molts més nombres reals transcendents que no pas algebraics. Un altre exemple de número transcendent molt coneguts, a part de π i e ja citats anteriorment, és $2^{\sqrt{2}}$.

5.2 Proposició sobre extensió de cossos

Donat un cos $(L,+,\cdot)$ i K un subcòs de L, per qualsevol $\alpha \in L$ definim $K(\alpha)$ com el menor subcòs de L que conté a K i a α. Aleshores $K \subseteq K(\alpha) \subseteq L$. Ja que $K(\alpha)$ és un cos,

[7] Podreu trobar la demostració al llibre [6] de la bibliografia, concretament està explicat a les pàg.72 i 74
[8] Podreu trobar més informació sobre nombres numerables i no numerables al llibre [7] de la bibliografia.

necessariament ha de contenir a α, α^2, α^3… i totes les seves combinacions lineals sobre el cos *K*, és a dir, ha de contenir $\lambda_0+\lambda_1\alpha+\lambda_2\alpha^2+...+\lambda_n\alpha^n$ per tot $\lambda_i \in K$.

Un polinomi P(x) amb coeficients en un cos *K* es diu un *polinomi irreductible* si no es pot expressar com a producte de dos polinomis amb coeficients en *K* de menor grau. A continuació demostrarem la següent proposició, que necessitarem en el següent apartat.

Proposició: $K(\alpha)$ és una extensió de dimensió finita sobre *K* si, i només si, α és algebraic sobre *K*. Si α és algebraic sobre *K*, la dimensió de $[K(\alpha):K]$ és el grau del polinomi irreductible P(x) tal que $P(\alpha)=0$.

Demostració: Si α és algebraic sobre *K*, aleshores existeix un polinomi a coeficients en *K*, P(x), tal que $P(\alpha)=0$. Podem considerar que P(x) és un polinomi irreductible, ja que si no ho fos podríem expressar P(x) com a producte de dos polinomis de grau més petit que el grau de P(x); $P(x)=S(x)\cdot R(x)$. Sabem que $P(\alpha)=0$, per tant, $S(\alpha)=0$ i/o $R(\alpha)=0$. Repetint el raonament sobre S(x) i R(x) anirem reduint el grau dels polinomis fins obtenir un polinomi irreductible del qual α serà una arrel, aquest polinomi el podríem anomenar P(x). Suposem que P(x) té grau n, aleshores $P(\alpha)=\mu_0+\mu_1\alpha+\mu_2\alpha^2+...+\mu_n\alpha^n=0$ amb $\mu_n\neq 0$, i aïllant α^n obtenim que $\alpha^n=-\frac{1}{\mu_n}(\mu_0+\mu_1\alpha+\mu_2\alpha^2+...+\mu_{n-1}\alpha^{n-1})$.

Veurem que $\{1,\alpha,\alpha^2,...,\alpha^{n-1}\}$ és una base de l'espai vectorial $K(\alpha)$ sobre *K*. Sabem que els elements de $K(\alpha)$ són de la forma $\lambda_0+\lambda_1\alpha+\lambda_2\alpha^2+...+\lambda_i\alpha^i$ $\forall i\in\mathbb{N}$. Si $i<n$ ja és una combinació lineal de $\{1,\alpha,\alpha^2,...,\alpha^{n-1}\}$. I si $i\geq n$ aleshores $\lambda_0+\lambda_1\alpha+\lambda_2\alpha^2+...+\lambda_n\alpha^n+\lambda_{n+1}\alpha^{n+1}+...+\lambda_i\alpha^i=\lambda_0+\lambda_1\alpha+\lambda_2\alpha^2+...+\lambda_{n-1}\alpha^{n-1}+\alpha^n(\lambda_n+\lambda_{n+1}\alpha+...+\lambda_i\alpha^{i-n})$ Si substituïm α^n per $-\frac{1}{\mu_n}(\mu_0+\mu_1\alpha+\mu_2\alpha^2+...+\mu_{n-1}\alpha^{n-1})$ aconseguim un polinomi de grau i-1. Repetint aquest raonament i-n vegades podem reduir el grau de la combinació lineal fins a n-1. Per tant, tot element de $K(\alpha)$ és de la forma $\lambda_0+\lambda_1\alpha+\lambda_2\alpha^2+...+\lambda_{n-1}\alpha^{n-1}$, és a dir, és combinació lineal de $\{1,\alpha,\alpha^2,...,\alpha^{n-1}\}$.

Per altre banda, sabem que P(x) és irreductible i que $P(\alpha)=\mu_0+\mu_1\alpha+\mu_2\alpha^2+...+\mu_n\alpha^n=0$. Si $\{1,\alpha,\alpha^2,...,\alpha^{n-1}\}$ fossin linealment dependents, és a dir, $\mu_0+\mu_1\alpha+\mu_2\alpha^2+...+\mu_{n-1}\alpha^{n-1}=0$ amb algun $\mu_j\neq 0$ aleshores existiria un polinomi de grau menor que n que tindria com arrel α, però sabem que P(x) és irreductible i de grau n, per tant, $\mu_0+\mu_1\alpha+\mu_2\alpha^2+...+\mu_{n-1}\alpha^{n-1}=0$ només si $\mu_0=\mu_1=\mu_2=...=\mu_{n-1}=0$, és a dir, $\{1,\alpha,\alpha^2,...,\alpha^{n-1}\}$ són linealment independents.

Amb això acabem de demostrar que $\{1,\alpha,\alpha^2,...,\alpha^{n-1}\}$ és una base de $K(\alpha)$, $K(\alpha)=\{\lambda_0+\lambda_1\alpha+\lambda_2\alpha^2+...+\lambda_{n-1}\alpha^{n-1}\}$, i que $[K(\alpha):K]=n$.

Recíprocament, si la dimensió de $K(\alpha)$ sobre K és finita, l'anomenarem r, les bases d'aquest espai vectorial tindran r elements i $\{1,\alpha,\alpha^2,...,\alpha^{r-1}\}$ és una base. Ja que $\alpha^r\in K(\alpha)$ es pot expressar com una combinació lineal $\alpha^r=\lambda_0+\lambda_1\alpha+\lambda_2\alpha^2+...+\lambda_{r-1}\alpha^{r-1} \Rightarrow \lambda_0+\lambda_1\alpha+\lambda_2\alpha^2+...+\lambda_{r-1}\alpha^{r-1}-\alpha^r=0$. Per tant, α és algebraic ja que és arrel del polinomi $P(x)=\lambda_0+\lambda_1x+\lambda_2x^2+...+\lambda_{r-1}x^{r-1}-x^r$.

Exemple: els números complexos $\mathbb{C}$ són una extensió dels nombres reals $\mathbb{C}=\mathbb{R}(i)$. L'extensió de $\mathbb{R}(i)$ sobre $\mathbb{R}$ és finita ja que i és algebraic sobre $\mathbb{R}$ i el polinomi irreductible sobre $\mathbb{R}$ del que i és una arrel és $x^2+1=0$, per tant, $[\mathbb{R}(i):\mathbb{R}]=2$. Una base de $\mathbb{C}$ és $\{1,i\}$.

5.3 Teorema de Wantzell

Ara farem un resum ràpid de tot el que ja hem definit en aquest treball per tal d'abordar el teorema que ho relaciona i determina quins són "tots" els números construïbles.

El problema original que havíem abordat en aquest treball és determinar quins punts del pla són construïbles a partir de dos punts inicials qualsevol $S_0=\{q_1, q_2\}$ amb regle i compàs. Mitjançant el traçat de rectes i circumferències anem determinant nous punts del pla a partir dels punts ja coneguts, i així anem creant una successió de conjunts de punts en que cadascun conté l'anterior $S_0\subset S_1\subset S_2\subset...\subset S_n$ que acabaran determinant el conjunt S de tots els punts construïbles. També hem establert la relació entre punt i número, sent el conjunt dels números construïbles $\mathcal{C}$ el conjunt de números que són coordenades d'un punt construïble.

Teorema de Wantzell: si un número real x és construïble amb regle i compàs, aleshores x és algebraic sobre $\mathbb{Q}$ i el polinomi irreductible amb coeficients en $\mathbb{Q}$ del que x és una arrel té com a grau una potència de dos. És a dir, $[\mathbb{Q}(x):\mathbb{Q}]=2^t$ amb $t\in\mathbb{N}$.

Demostració: definim el cos K_0 com el cos extensió de $\mathbb{Q}$ més petit que conté les coordenades de q_1 i q_2. Cada punt nou que obtenim mitjançant regle i compàs $p=(x,y)$ és la intersecció de dues rectes, una recta i una circumferència o bé dues circumferències. En general, definim el cos K_{n+1} com l'extensió més petita del cos K_n que conté la primera coordenada del nou punt p i K_{n+2} com l'extensió més petita de K_{n+1} que conté la segona coordenada del punt p. És a dir, $K_{n+1}=K_n(x)$ i $K_{n+2}=K_{n+1}(y)$. Per tant, a mesura que anem construint nous punts obtenim una successió de cossos $K_0\subseteq K_1\subseteq K_2\subseteq \ldots\subseteq \mathcal{C}$ (on $\mathcal{C}$ és el cos dels números construïbles).

Així, a cada operació que fem amb regle i compàs obtenim un nou punt $p=(x,y)$ (encara que és possible que aquest punt ja l'haguéssim obtingut en un pas anterior) aquest punt determinarà dos nous números construïbles (encara que potser ja els teníem) i determinarem dues noves extensions de $\mathbb{Q}$, $K_{n+1}= K_n(x)$ i $K_{n+2}= K_{n+1}(y)$ (que potser no aporten res, si $x,y\in K_n$).

A partir d'un conjunt de punts S_m definirem K_m com el cos extensió de $\mathbb{Q}$ més petit que conté les coordenades dels punts de S_m. Sigui $p=(x,y)$ un nou punt construïble a partir de S_m en una única operació elemental i sigui $K_{m+1}=K_m(x)$ i $K_{m+2}=K_{m+1}(y)$, aleshores demostrarem que $[K_{m+1}: K_m]$ i $[K_{m+2}: K_{m+1}]=1$ o 2.

Com ja hem indicat anteriorment per trobar un nou punt construïble, aquest ha de ser la intersecció de dues rectes, una recta i una circumferència, o bé, de dues circumferències.

Considerem el primer cas, que $p=(x,y)$ sigui la intersecció de dues rectes construïbles. L'equació de la recta que passa per dos punts construïbles (x_1,y_1) i (x_2,y_2) és de la forma:

$$(x,y)=(x_1,y_1)+t\cdot(x_2-x_1,y_2-y_1)\rightarrow\frac{x-x_1}{x_2-x_1}=\frac{y-y_1}{y_2-y_1}\rightarrow$$
$$(y_2-y_1)x-(x_2-x_1)y-x_1y_2+x_1y_1+x_2y_1-x_1y_1=0\rightarrow$$
$$Ax+By+C=0 \quad \text{on } A,B,C\in K_m$$

A, B, C pertanyen a K_m ja que K_m és un cos amb les operacions internes suma i producte definides, per tant, el resultat de sumar i multiplicar elements del cos dóna com a resultat altres elements del cos. Per calcular la intersecció hem de resoldre el sistema.

$$\begin{cases}Ax+By+C=0\rightarrow y=\dfrac{-Ax-C}{B} \\ A'x+B'y+C'=0\end{cases}\rightarrow A'x+B'\left(\frac{-Ax-C}{B}\right)+C'=0$$
$$(A'\text{-}AB')x-\frac{B'C+BC'}{B}=0 \qquad \text{on } A,B,C,A',B',C'\in K_m$$

Aquest mateix raonament es pot aplicar a la segona coordenada del punt. És a dir, que per p=(x,y) tant x com y són números arrels d'un polinomi de primer grau amb coeficients en K_m. Això implica, utilitzant la proposició explicada anteriorment, que $[K_m(x): K_m]=1$ i $[K_m(y): K_m(x)]=1$, és a dir, $K_m= K_m(x)= K_m(y)$.

Considerem el segon cas, que p=(x,y) sigui la intersecció d'una recta i una circumferència construïbles. La recta passarà per dos punts de S_m (x_1,y_1) i (x_2,y_2) i es podrà expressar, com ja hem demostrat en l'apartat anterior, com $Ax+By+C=0$ on $A,B,C\in K_m$. La circumferència tindrà de centre el punt construïble (x_3,y_3) i radi r construïble. Els punts de la circumferència compleixen l'equació:

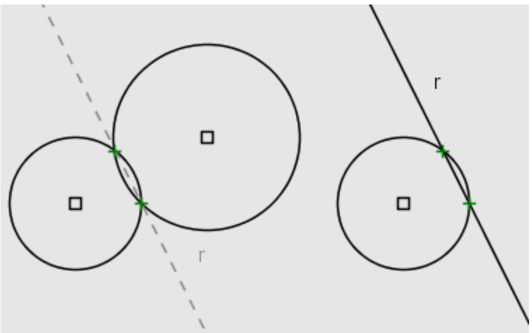
$$(x-x_3)^2+(y-y_3)^2=r^2\rightarrow x^2+y^2+x_3^2+y_3^2-2xx_3-2yy_3-r^2=0\rightarrow$$
$$x^2+y^2+A'x+B'y+C'=0 \qquad \text{on } A',B',C'\in K_m$$

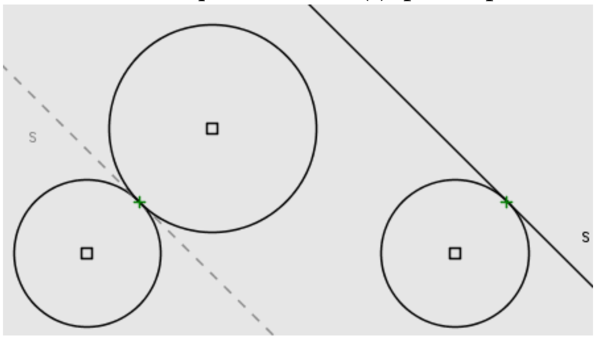
El punt (x,y) serà solució del sistema:

$$\begin{cases}Ax+By+C=0\rightarrow y=\dfrac{-Ax-C}{B} \\ x^2+y^2+A'x+B'y+C'=0\end{cases}\rightarrow x^2+\left(\frac{\text{-}Ax\text{-}C}{B}\right)^2+A'x+B'\left(\frac{\text{-}Ax\text{-}C}{B}\right)+C'=0$$
$$\left(\frac{B^2+A^2}{B^2}\right)x^2+\left(\frac{2AC+A'B^2\text{-}ABB'}{B^2}\right)x+\left(\frac{C^2\text{-}BB'C+B^2C'}{B^2}\right)=0 \quad \text{on } A,B,C,A',B',C'\in K_m$$

És a dir, que per p=(x,y) tant x com y són arrels d'un polinomi de segon grau amb coeficients en K_m. Això implica, utilitzant la proposició explicada anteriorment, que [K_m(x): K_m] i [K_m(y): K_m(x)] seran 1 o 2. Si el polinomi és irreductible en K_m la dimensió serà 2 i si es pot reduir l'extensió serà 1.

Si considerem el tercer cas, que p=(x,y) sigui la intersecció de dues circumferències, podem arribar a veure que es pot reduir al segon cas, és a dir, a la intersecció d'una circumferència i una recta. Si expressem les equacions de les dues circumferències d'aquesta forma, $\begin{cases} x^2 + y^2 + Ax + By + C = 0 \\ x^2 + y^2 + A'x + B'y + C' = 0 \end{cases}$ hem demostrat anteriorment que els coeficients pertanyen a K_m. Podem restar una equació a l'altre i així desapareixen els termes de segon grau i ens queda un polinomi de primer grau, és a dir, l'equació d'una recta. Els punts d'intersecció d'aquesta recta amb una de les circumferències són els mateixos que els punts d'intersecció de les dues circumferències. Gràficament això es demostra sabent que la recta (r) passa pels dos





punts de tall de les circumferències o en el cas de que siguin tangents és la recta (s) que passa pel punt de tangència i també és tangent a la circumferència.

Tot aquest raonament ens permet arribar a la conclusió de que quan obtenim un nou número construïble a només el podem haver obtingut com a resultat d'un dels tres casos anteriors i, per tant, podem afirmar que sempre [$K_m(a)$: K_m] = 1 o 2. Aplicant un teorema ja explicat en l'apartat d'àlgebra podem observar que: [$K_m(a)$:$\mathbb{Q}$] = [$K_m(a)$: K_m]$\cdot$[K_m: K_{m-1}]$\cdot \ldots \cdot$[K_0: $\mathbb{Q}$]. Aquesta expressió serà una sèrie de productes de 1 i 2, per tant, [$K_m(a)$:$\mathbb{Q}$] = 2^t amb $t \in \mathbb{N}$. Sabem que $\mathbb{Q} \subseteq \mathbb{Q}(a) \subseteq K_m$; utilitzant el mateix teorema d'àlgebra podem afirmar que [$K_m(a)$:$\mathbb{Q}$] = [$K_m(a)$:$\mathbb{Q}(a)$]$\cdot$[$\mathbb{Q}(a)$:$\mathbb{Q}$] = 2^t. La dimensió de $\mathbb{Q}(a)$ sobre $\mathbb{Q}$ és un divisor de 2^t, per tant, també haurà de ser una potència de dos.

Segons la proposició sobre extensió de cossos explicada en l'apartat 5.2, la dimensió d'una extensió d'un cos $\mathbb{Q}(a)$ sobre el propi cos $\mathbb{Q}$ és el grau del polinomi irreductible amb coeficients en $\mathbb{Q}$ del que a és una arrel.

És a dir, amb tot això hem demostrat que si un número a és construïble amb regle i compàs, aleshores a és una arrel d'un polinomi irreductible de grau una potència de dos amb coeficients en $\mathbb{Q}$.

Recíproc del teorema del Wantzell:

Ja hem demostrat que per tal que un número real x sigui construïble amb regle i compàs és necessari que la dimensió de l'extensió de $\mathbb{Q}$ que genera x sobre el propi cos $\mathbb{Q}$ sigui una potència de 2, és a dir, que $[\mathbb{Q}(x):\mathbb{Q}]=2^r$. Però això no és una condició suficient, ja que existeixen arrels de polinomis irreductibles amb coeficients en $\mathbb{Q}$ de grau una potència de dos que no són construïbles amb regla i compàs.

Per tal que x sigui construïble amb regle i compàs s'ha d'afegir una altra condició. També han d'existir r extensions de $\mathbb{Q}$, anomenades K_i, de manera que $\mathbb{Q}=K_0\subset K_1\subset\ldots\subset K_r=\mathbb{Q}(x)$, on $[K_i:K_{i-1}]=2$. [1]

Demostració: sigui P(x) el polinomi irreductible amb coeficients en $\mathbb{Q}$ de grau 2^r on $r\in\mathbb{N}$ del que x és una arrel.

La demostració es fa per inducció sobre r. És a dir, demostrarem que si per un valor de r, x és construïble, aleshores també serà construïble per r+1. Demostrarem que per $r=0$ x és construïble, per tant, x serà construïble per qualsevol valor de r.

Si $r=0$, el polinomi irreductible amb coeficients en $\mathbb{Q}$ del que x és una arrel serà de grau $2^0=1$ i tindrà la forma $P(x)=ax+b=0$ amb $a,b\in\mathbb{Q}$. Això implica que $x=-b/a$. Ja hem demostrat que tots els racionals són construïbles, per tant, x serà construïble.

Ara demostrarem que si x és construïble per r, també ho serà per r+1. Si $\mathbb{Q}=K_0\subset K_1\subset\ldots\subset K_{r+1}=\mathbb{Q}(x)$, amb $[K_i:K_{i-1}]=2$, aleshores $[\mathbb{Q}(x):\mathbb{Q}]=2^{r+1}$. Que

$[K_{r+1}:K_r]=2$ vol dir que existeix un polinomi de grau 2 irreductible sobre K_r de la forma $P(x)=ax^2+bx+c=0$ amb $a,b,c\in K_r$. Aleshores, $x=\dfrac{-b\pm\sqrt{b^2-4ac}}{2a}$. Com que $[K_r:\mathbb{Q}]=2^r$, pel raonament de inducció podem dir que tots els elements de K_r són construïbles. Sabem que la suma i el producte de números construïbles també és construïble, per tant, -b, 2a, b^2, -4ac també seran construïbles. Com que x és un número real b^2-4ac ha de ser positiu, ja hem demostrar anteriorment que l'arrel d'un número construïble positiu és construïble.

Una condició equivalent a [1] és que el grup de Galois del polinomi irreductible de x sigui un 2-grup[9]. Però fa servir conceptes de Teoria de Galois no definits en aquest treball.

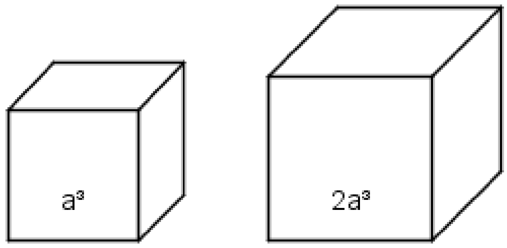
[9] Podeu veure la condició expressada d'aquesta forma al lloc web [14] de la bibliografia.

6. La irresolubilitat dels problemes clàssics

Els problemes clàssics són un grup de tres problemes sobre les construccions amb regle i compàs coneguts des de l'època de l'antiga Grècia. Concretament són la duplicació del cub, la quadratura del cercle i la trisecció d'un angle, utilitzant només regle i compàs amb les restriccions vistes anteriorment. Cap de les tres construccions és possible en general utilitzant només regle i compàs. A continuació donarem les raons de perquè no és possible cadascuna d'aquestes construccions.

6.1 La duplicació del cub

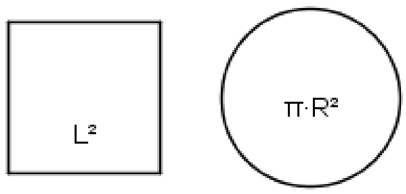
El problema consisteix en construir a partir d'un cub donat un altre cub que tingui el doble de volum, és a dir, donat un cub de costat a i conseqüentment volum a^3, construir un cub de volum $2a^3$.



Prenem com a unitat la longitud de l'aresta del cub inicial. Aleshores el volum del cub també serà 1. El costat del cub que hem de construir haurà de complir que $a^3=2$ i, per tant, $a^3-2=0$. Com que $x^3-2=0$ és un polinomi de grau 3 irreductible amb coeficients en $\mathbb{Q}$, sabem que $[\mathbb{Q}(a):\mathbb{Q}]=3$. En l'apartat anterior hem demostrat que tot número construïble ha de ser arrel d'un polinomi irreductible amb coeficients en $\mathbb{Q}$ de grau una potència de 2, per tant, a no és un número construïble amb regle i compàs, és a dir, no podem duplicar el volum d'un cub amb regle i compàs.

6.2 La quadratura del cercle

És el problema grec més conegut i, de fet, s'utilitza l'expressió "quadrar el cercle" per designar una cosa impossible o extremadament difícil. El problema consisteix en construir amb regle i compàs un quadrat que tingui la mateixa àrea que un cercle donat.

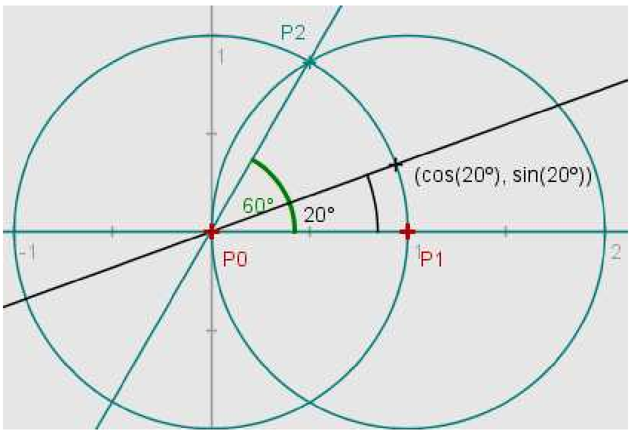


Partim d'un cercle de radi R, per tant, la seva àrea serà πR^2. Anomenarem al costat del quadrat que volem construir L, per tant, podem determinar que

$L^2 = \pi R^2$. Podem deduir que $\frac{L}{R} = \sqrt{\pi}$. Sabem que R és construïble (és la dada inicial del problema) si L fos construïble aleshores $\sqrt{\pi}$ també seria construïble, ja que la divisió de nombres construïbles és construïble, com ja hem determinat abans. El matemàtic alemany Ferdinand Lindemann (1852-1939) va demostrar l'any 1882 que π és un número transcendent, és a dir, que no és solució de cap polinomi amb coeficients en $\mathbb{Q}$ i, per tant, no és construïble. Si π no és construïble la seva arrel tampoc ho serà, perquè si $\sqrt{\pi}$ fos construïble, com ja hem demostrat que el producte de nombres construïbles és construïble, podríem multiplicar $\sqrt{\pi}$ per sí mateix i construir π. Per tant, L no pot ser construïble i no podem quadrar un cercle amb regle i compàs.

6.3 Trisecció d'un angle qualsevol

Consisteix en trobar un mètode per dividir un angle qualsevol en tres angles iguals amb regle i compàs. Certs angles sí que es poden trisecar, com per exemple el de 90º, però per demostrar que el cas general és impossible ho demostrarem en un cas particular, l'angle de 60º. Per construir un angle de 60º amb regle i compàs podem seguir els següents passos: donats dos punts p_0, p_1 tracem la recta que els uneix, a continuació tracem dues circumferències de radi la distància entre p_0 i p_1 de centre p_0 i p_1. Aquestes dues circumferències es tallaran en dos punts, un qualsevol d'aquests punts l'anomenarem p_2. La recta determinada per p_0 i p_2 forma un angle de 60º amb la recta determinada per p_0 i p_1. Considerem el punt p_0 com l'origen d'un sistema de coordenades, la recta determinada per p_0 i p_1 com l'eix d'abscisses i la distància entre p_0 i p_1 com la unitat. Trisecar l'angle de 60º suposaria trobar una recta que formés un angle de 20º amb l'eix d'abscisses. Si tracem una circumferència de radi unitat i centre p_0, tallaria amb la recta anterior en el punt de



coordenades (cos20º, sin20º). Per tant, el número cos20º hauria de ser construïble, ara demostrarem que no ho és.

$$\frac{1}{2}=\cos(60^o)=\cos(20^o+40^o)=\cos(20^o)\cdot\cos(40^o)-\sin(20^o)\cdot\sin(40^o)=$$

$$=\cos(20^o)\cdot\left(\cos^2(20^o)-\sin^2(20^o)\right)-\sin(20^o)\cdot\left(2\cdot\sin(20^o)\cdot\cos(20^o)\right)=$$

$$=\cos^3(20^o)-\cos(20^o)\cdot\sin^2(20^o)-2\cdot\cos(20^o)\cdot\sin^2(20^o)=$$

$$=\cos^3(20^o)-3\cdot\cos(20^o)\cdot\left(1-\cos(20^o)\right)=4\cos^3(20^o)-3\cos(20^o)=\frac{1}{2}\rightarrow$$

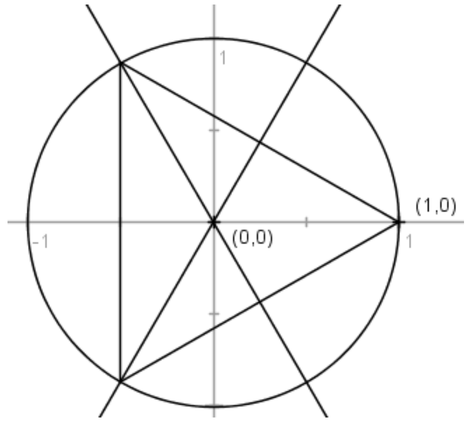
$$\rightarrow\cos^3(20^o)-\frac{3}{4}\cos(20^o)-\frac{1}{8}=0$$

Aleshores $\cos(20^o)$ és una arrel del polinomi $x^3-\frac{3}{4}x-\frac{1}{8}=0$ que és un polinomi de grau 3 irreductible amb coeficients en $\mathbb{Q}$. Com ja hem demostrat, el grau hauria de ser una potència de 2 perquè fos construïble, per tant, no és construïble i podem concloure que en general no es pot trisecar un angle amb regle i compàs.

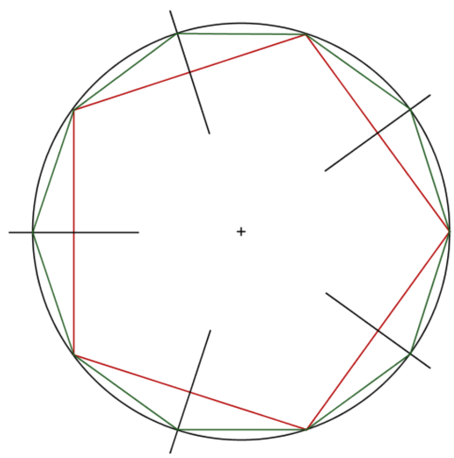
7. Polígons regulars

La nova pregunta que volem respondre és: quins polígons regulars es poden construir amb regle i compàs?. Per fer-ho primerament haurem de considerar diverses característiques dels polígons regulars, que ens permetran simplificar el problema.

Tots els polígons regulars es poden inscriure en una circumferència, que tindrà per centre la intersecció de les mediatrius dels costats del polígon. És a dir, en tots els polígons regulars podem traçar una circumferència exterior al polígon que passi per tots els vèrtexs.



Si podem construir un polígon regular de n costats de qualsevol grandària, també el podrem inscriure en una circumferència de radi 1. Unim tots els vèrtexs del polígon amb el centre de la circumferència circumscrita (el punt d'intersecció de les mediatrius) i tracem una circumferència de centre aquest punt i de radi la unitat. La intersecció de la circumferència amb totes les rectes traçades anteriorment determinen els vèrtex del polígon inscrit en la circumferència de radi 1. Podem considerar el centre de la circumferència el punt (0,0) i, com que l'orientació d'un polígon no té importància podem considerar un vèrtex del polígon el punt (1,0). Això ens permet simplificar el problema a construir un n-polígon, és a dir, un polígon de n costats, inscrit en una circumferència de radi 1 i centre (0,0).

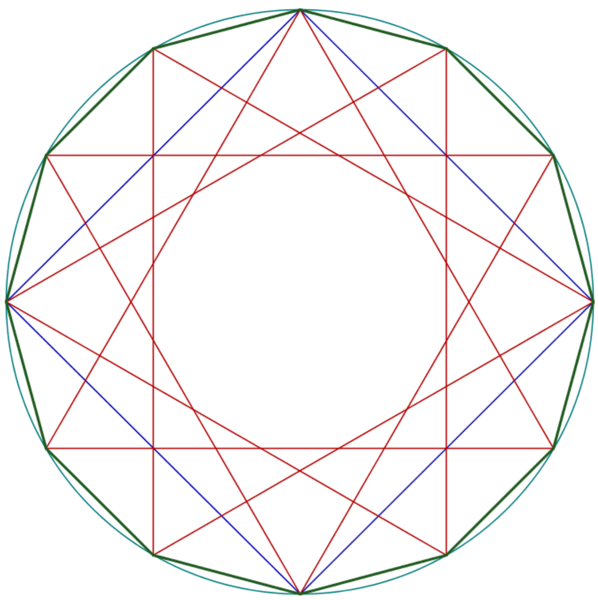


Proposició: Si sabem construir un n-polígon, aleshores podrem construir un polígon que tingui el doble de costats.

Demostració: Tracem les mediatrius dels seus costats del n-polígon. El punt d'intersecció de cadascuna de les mediatrius amb la circumferència circumscrita és un nou vèrtex del polígon de $2 \cdot n$ costats. Això implica que tots els polígons que tinguin un número de costats que sigui una potència de dos seran construïbles.

Proposició: Si sabem construir un polígon regular de n costats i un de m costats i si m i n són primers entre sí, és a dir, si el m.c.d.(m,n) = 1; aleshores també sabrem construir el polígon de m·n costats.

Demostració: Això es pot observar gràficament de la següent forma. Si inscrivim un n-polígon en una circumferència unitat i, a continuació, inscrivim en la mateixa circumferència n polígons de m costats, cadascun amb un vèrtex comú al n-polígon. Aleshores en la circumferència hi haurà m·n vèrtexs, que ens permetran dibuixar el (m·n)-polígon. Això és així ja que cada m-polígon inscrit afegirà m-1 vèrtexs, ja que tindrà un en comú amb n. I com que n'afegim n, podrem afirmar que $n + (m-1) \cdot n = n + m \cdot n - n = m \cdot n$

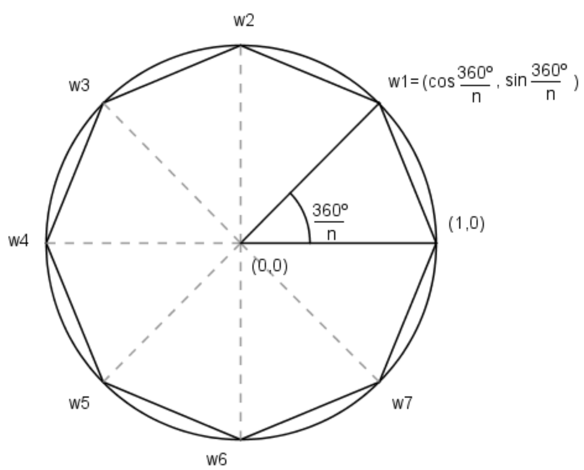


La condició de que m i n siguin coprimers és necessària per tal d'obtenir m·n vèrtexs diferents.

Exemple: donats els polígons de 3 i 4 costats, mitjançant el procés explicat anteriorment podem construir el polígon de 12 costats.

Recíprocament, si tenim un s-polígon tal que s = m·n, aleshores podrem construir el m-polígon i el n-polígon. Podem construir el m-polígon a partir del s-polígon unint un vèrtex de cada n, i si unim un vèrtex de cada m, obtindrem el n-polígon.

Exemple: donat el polígon de dotze costats (com el dibuix de l'exemple anterior) si unim un de cada tres vèrtexs que té el polígon obtindrem un quadrat. I si del polígon de dotze costats unim un vèrtex de cada quatre, obtindrem un triangle equilàter.



Per poder construir un polígon regular amb regle i compàs n'hi ha prou amb saber construir el vèrtex següent a l'inicial (1,0). Traçant circumferències de radi un costat i de centre cada vèrtex del polígon determinarem en les interseccions amb la circumferència circumscrita al polígon la resta de vèrtexs del polígon.

Recordant la analogia entre el pla i els números complexos, observem que els vèrtexs d'un n-polígon inscrit en una circumferència unitat amb un vèrtex en el punt (1,0) són les arrels complexes del polinomi $x^n-1=0$, és a dir, els punts $w_i=\left(\cos\left(\frac{360\cdot i}{n}\right), \sin\left(\frac{360\cdot i}{n}\right)\right)$ on $i=0,1,...,n-1$.

7.1 La funció phi de Euler:

La funció $\varphi(n)$ es defineix com la quantitat de números naturals menors que n que són primers entre sí amb n. És a dir, el cardinal (#), el nombre de números naturals d que compleixin que el m.c.d.$(d,n)=1$ on $d\in\mathbb{N}$.

$$\varphi(n)=\#\{d\in\mathbb{N}\ \text{amb}\ 1\le d<n \mid \text{m.c.d.}(d,n)=1\}$$

Exemples:

$\varphi(4)=\#\{1,3\}=2$ $\varphi(6)=\#\{1,5\}=2$

$\varphi(5)=\#\{1,2,3,4\}=4$ $\varphi(12)=\#\{1,5,7,11\}=4$

Propietats:

1) $\varphi(p)=(p-1)$ si p és primer

2) $\varphi(p^i)=(p-1)\cdot p^{i-1}$ on p és primer, $i\in\mathbb{N}$

3) $\varphi(m\cdot n)=\varphi(m)\cdot\varphi(n)$ si m.c.d.$(m,n)=1$

Pel teorema de Wantzell sabem que per tal de que un n-polígon sigui construïble amb regle i compàs haurà de complir que $[\mathbb{Q}(\cos\frac{360}{n}):\mathbb{Q}]=2^t$ per algun $t\in\mathbb{N}$.

Gauss va demostrar que el polinomi irreductible de les arrels unitàries de grau n (les arrels complexes del polinomi $x^n-1=0$) té grau φ(n), on φ(n) és la *funció phi de Euler*[10]. És a dir, que $[\mathbb{Q}(\cos\frac{360}{n}):\mathbb{Q}]=\varphi(n)$.

Per qualsevol n-polígon, n serà un nombre natural i es podrà expressar com $n = p_1^{i_1}\cdot p_2^{i_2}\cdot\ldots\cdot p_m^{i_m}$, la descomposició de n en factors primers. Aplicant les propietats anteriors, obtenim que per a que un n-polígon sigui construïble, haurà de complir que:

$$[\mathbb{Q}(\cos\tfrac{360}{n}):\mathbb{Q}]=2^t=\varphi(n)=\varphi(p_1^{i_1}\cdot p_2^{i_2}\cdot\ldots\cdot p_m^{i_m})=\varphi(p_1^{i_1})\cdot\varphi(p_2^{i_2})\cdot\ldots\cdot\varphi(p_m^{i_m}) =$$

$$=(p_1-1)p_1^{i_1-1}\cdot(p_2-1)p_2^{i_2-1}\cdot\ldots\cdot(p_m-1)p_m^{i_m-1}$$

Per tal de que l'última expressió sigui una potència de 2, cada factor haurà de ser una potència de 2. En el cas de que el nombre primer sigui 2, per a qualsevol potència serà construïble. En canvi, per a un nombre primer diferent de 2, p_k, elevat a una potència mai donarà una potència de 2, per tant, l'exponent haurà de ser 0, per tant, $i_k=1$. També haurà de complir que p_k-1 sigui una potència de 2, és a dir, que p_k haurà de ser un número primer de la forma $p_k=2^t+1$ per algun t natural. Per tant, per que un n-polígon sigui construïble ha de tenir la forma $n=2^r\cdot p_1\cdot\ldots\cdot p_m$, amb p_i primer de la forma $p_i=2^t+1$

Podem obtenir una condició encara més forta. Sabem que si n es senar x^n+1 és divisible per x+1, donant $x^n+1=(x+1)(x^{n-1}-x^{n-2}+x^{n-3}-\ldots-x+1)$. Si factoritzem t en factors primers $t=2^s\cdot q$ amb q senar (q és el producte de la resta de factors primers).

Aleshores,

$$p=2^t+1=2^{2^s q}+1=(2^{2^s})^q+1=[(2^{2^s})+1]\cdot[(2^{2^s})^{q-1}-(2^{2^s})^{q-2}+\ldots(2^{2^s})+1]$$

Com que *p* és un número primer, aleshores el segon factor ha de ser igual a 1, i això només és possible si $q=1$ perquè en aquest cas només hi haurà un terme del segon factor. Per tant, *p* haurà de ser de la forma $p=2^{2^s}+1$ i primer.

Els números d'aquesta forma es diuen números de Fermat. Fermat va conjecturar que sempre eren números primers, però no és cert:

$F_0 = 2^1 + 1 = 3$

$F_1 = 2^2 + 1 = 5$

[10] Podreu trobar aquesta teoria explicada als llocs web [12], [13] de la bibliografia.

$F_2 = 2^4 + 1 = 17$

$F_3 = 2^8 + 1 = 257$

$F_4 = 2^{16} + 1 = 65.537$

$F_5 = 2^{32} + 1 = 4.294.967.297 = 641 \times 6.700.417$

$F_6 = 2^{64} + 1 = 18.446.744.073.709.551.617 = 274.177 \times 67.280.421.310.721$

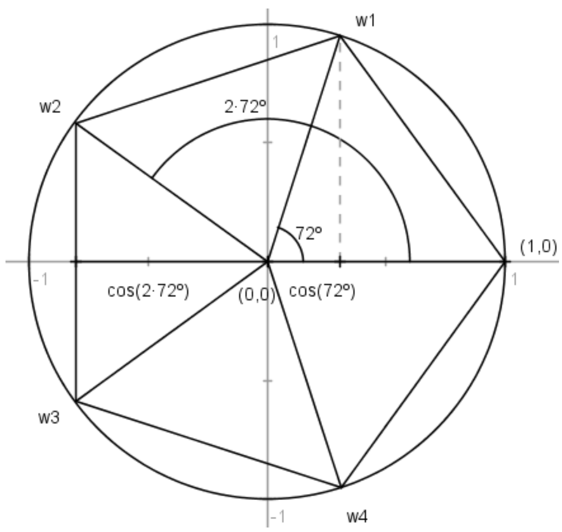
Només s'ha pogut determinar que son números primers $F_{0,}$ F_1 F_2 F_3 F_4 i es desconeix si hi ha més números de Fermat primers, però s'ha pogut validar que si existeixen algun altre número de Fermat primer ha de tenir més de 40.000 xifres.

Amb tot això podem concloure que per tal de que un n-poligon sigui construïble amb regle i compàs és necessari que $n=2^t \cdot p_1 \cdot p_2 \cdot \ldots \cdot p_m$, a on cada p_i ha de ser un número primer de Fermat de la forma $p = 2^{2^s} + 1$. És a dir que $n=2^t \cdot 3^a \cdot 5^b \cdot 17^c \cdot 257^d \cdot 65637^e$, a on $t \in \mathbb{N}$ i a,b,c,d,e$=$0 o 1. Sempre i quan no hi hagi més nombres de Fermat primers.

Els únics n-polígons construïbles amb regle i compàs menors de 1.000 son: n=3, 4, 5, 6, 8, 10, 12, 15, 16, 17, 20, 24, 30, 32, 34, 40, 48, 51, 60, 64, 68, 80, 85, 96, 102, 120, 128, 136, 160, 170, 192, 204, 240, 255, 256, 257, 272, 320, 340, 384, 408, 480, 510, 512, 514, 544, 640, 680, 768, 771, 816 i 960.

7.2 Construcció del Pentàgon

Farem un exemple de construcció d'un polígon regular, el pentàgon, i demostrarem matemàticament que el mètode emprat determina veritablement un pentàgon regular.



Els vèrtexs del pentàgon són les arrels complexes de $x^5-1=0$. Per tant són els punts del pla $\left(\cos\left(\frac{360\cdot k}{5}\right), \sin\left(\frac{360\cdot k}{5}\right)\right)$ on k=0, 1, 2, 3 o 4.

Si anomenem w a la primera arrel o vèrtex del polígon, podem determinar que w = (cos72º, sin72º) i que w és arrel de $x^5-1 = (x-1)(x^4+x^3+x^2+x+1)$, per tant, $w^4+w^3+w^2+w^1+1=0$.

Com es pot veure gràficament w^1 i w^4 tenen el mateix cosinus i el mateix valor de sinus, però de signe oposat, per tant, podem determinar que $w^1+w^4 = 2\cos(72)$. Podem aplicar el mateix raonament a w^2 i w^3 i determinar que $w^2+w^3 = 2\cos(2\cdot 72)$.

Substituint en el polinomi anterior obtenim que $2\cos(72) + 2\cos(2\cdot 72) + 1 = 0$. Aplicant la formula de l'angle doble i operant obtenim que:

$$2\cos(72) + 2(\cos^2(72) - \text{sen}^2(72)) + 1 = 0 \rightarrow$$

$$2\cos(72) + 2\cos^2(72) - 2(1 - \cos^2(72)) + 1 = 0 \rightarrow$$

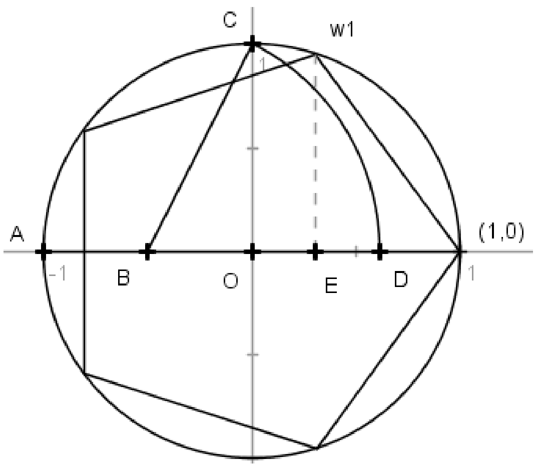
$$2\cos(72) + 2\cos^2(72) - 2 + 2\cos^2(72) + 1 = 0 \rightarrow$$

$$4\cos^2(72) + 2\cos(72) - 1 = 0 \rightarrow$$

$$\cos(72) = \frac{-2 \pm \sqrt{4+4\cdot 4}}{8} = \frac{-\frac{1}{2}+\sqrt{\frac{5}{4}}}{2}$$ a on hem eliminat la solució negativa ja que sabem que cos(72) és positiu.

Mètode de construcció del pentàgon:

Un cop determinat matemàticament el valor del cos(72º) com una expressió de números construïbles amb regle i compàs, podem obtenir un mètode de construcció del pentàgon.



En una circumferència de radi unitat i centre O = (0,0) trobem el punt mig del radi $\overline{OA}$, que anomenem B. El segment $\overline{OB}$ mesura $\frac{1}{2}$ i $\overline{OC}$ 1, aplicant el teorema de Pitàgores es determina que $\overline{BC}$ val $\sqrt{\frac{1}{4}+1} = \sqrt{\frac{5}{4}}$. Fem una circumferència de centre B i radi $\overline{BC}$, en la intersecció amb l'eix d'abscisses trobem el punt D. La longitud de $\overline{BD}$ és la mateixa que la de $\overline{BC}$.

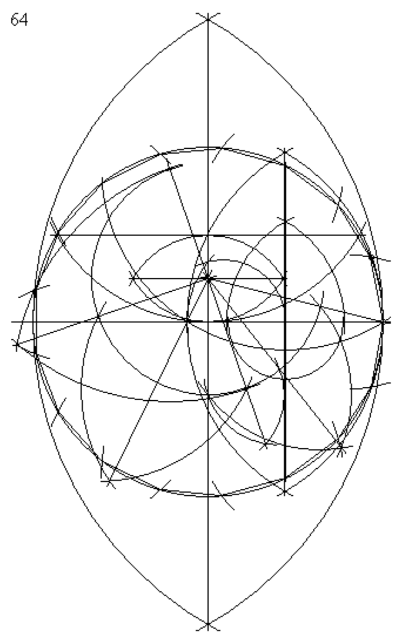
Com que la longitud de $\overline{OB}$ és $\frac{1}{2}$, la longitud de $\overline{OD}$ serà $-\frac{1}{2}+\sqrt{\frac{5}{4}}$. Trobem el punt mig de $\overline{OD}$ i anomenem el punt E. $\overline{OE}$ valdrà $\frac{-\frac{1}{2}+\sqrt{\frac{5}{4}}}{2}=\cos\left(\frac{360}{5}\right)$. Per tant, si tracem una recta perpendicular a l'eix d'abscisses per aquest punt determinarem en la intersecció amb la circumferència de radi unitat el punt de coordenades $(\cos(72),\sin(72))$. Aquest punt serà w_1, el segon vèrtex del pentàgon. Traslladant la distància del costat del pentàgon trobarem la resta de vèrtexs.

D'aquesta manera hem determinat matemàticament un mètode de construcció del pentàgon.

Anàlogament al mètode que hem seguit per elaborar un algorisme de construcció del pentàgon amb regle i compàs, Gauss va demostrar a l'edat de 19 anys que:

$$\cos\left(\frac{2\pi}{17}\right)=-\frac{1}{16}+\frac{1}{16}\sqrt{17}+\frac{1}{16}\sqrt{34-2\sqrt{17}}+\frac{1}{8}\sqrt{17+3\sqrt{17}-\sqrt{34-2\sqrt{17}}-2\sqrt{34+2\sqrt{17}}}$$

i va elaborar un mètode per construir un segment d'aquesta longitud. La construcció de l'heptadecàgon regular consta de 64 passos.



8. Pàgina web

Com a part pràctica del treball de recerca he elaborat una pàgina web[11] interactiva que consta de diverses parts. En una primera pantalla s'explica el concepte de construcció amb regle i compàs i les normes que s'han de seguir a l'hora de fer construccions. També es pot accedir a un apartat d'història on s'explica els inicis de la construcció amb regle i compàs i com van sorgir els tres problemes clàssics. A més a més, la pàgina web té una part interactiva molt important on es poden realitzar algunes construccions amb regle i compàs explicades en el meu treball de recerca. La web permet realitzar aquestes construccions utilitzant regle i compàs a partir d'unes dades inicials i, si ho desitges, permet visualitzar les seves respectives solucions mostrant-les pas per pas. Des de la pàgina principal es pot visualitzar i descarregar la part teòrica del meu treball de recerca.

El programa que he utilitzat per fer les construccions amb regle i compàs que apareixen a la web també l'he fet servir per realitzar totes les construccions que explico en el meu treball i m'ha permès acompanyar les explicacions amb la construcció corresponent, per tal de fer-les més entenedores.

Per arribar a elaborar la pàgina web i les construccions del treball he hagut d'introduir-me en el món del disseny gràfic que era completament desconegut per a mi. He après a manejar dos programes d'ordinador que no coneixia, el *Zirkel* (CaR) que m'ha permès fer totes les construccions i el *Macromedia Dreamweaver* que m'ha permès realitzar el disseny gràfic de la web. També he utilitzat altres programes d'edició d'imatges per elaborar diversos efectes de la web. Finalment, també he hagut d'aprendre a penjar arxius a Internet mitjançant un *hosting*.

He tingut problemes amb el domini de la pàgina web, finalment l'adreça del meu lloc web és: http://raulweb.webcindario.com

[11] En els annexos he inclòs dues pantalles de la pàgina web.

9. Conclusió

L'objectiu inicial del meu treball de recerca era determinar quins nombres són construïbles amb regle i compàs i posteriorment, aplicar els resultats obtinguts per demostrar la irresolubilitat dels tres problemes clàssics i per determinar quins polígons regulars són construïbles amb regle i compàs. Tot i les dificultats, penso que he aconseguit assolir els objectius plantejats, encara que alguna afirmació no l'he pogut demostrar degut a la seva dificultat.

La dificultat principal amb la que m'he trobat a l'hora de desenvolupar el meu treball ha estat el nivell de matemàtiques necessari per poder entendre la bibliografia. A causa de la falta de coneixements matemàtics previs, la primera part del meu treball ha consistit en un aprenentatge d'àlgebra del qual he inclòs un resum en el treball. Una altra dificultat que he trobat ha estat que moltes explicacions en llibres i principalment en webs eren incompletes. Es mostraven els resultats dels teoremes i es donaven indicacions[12] per arribar a entendre les demostracions però no estaven explicades detalladament enlloc. Jo he intentat que el meu treball fos ordenat i entenedor i que no apareguessin afirmacions sense raonar-les i demostrar-les, la qual cosa m'ha resultat força complicada, perquè he hagut d'elaborar gran part de les demostracions per mi mateix. També he tingut dificultats a l'hora d'escriure la memòria. El meu treball té un gran nombre de fórmules matemàtiques i escriure-les ha resultat molt lent i desesperant, ja que es desplaçaven amb les imatges. Una cosa que m'ha sorprès ha estat descobrir que molts llibres de text i pàgines web mostren com fer una construcció geomètrica, però no demostren que la figura obtinguda sigui realment la indicada. Per exemple, he trobat diversos mètodes per construir la bisectriu d'un angle o una mediatriu, indicant una sèrie de passos a realitzar per obtenir la construcció. Però, enlloc es demostrava que la recta obtinguda fos realment la bisectriu o la mediatriu, com si el fet de que visualment ho sembli fos suficient per haver demostrat que realment ho és. Per aquest motiu he hagut de elaborar jo mateix la demostració.

Per altra banda, he gaudit molt pensant com fer les construccions bàsiques amb regle i compàs utilitzant els coneixements de dibuix tècnic. I també m'ha agradat molt la utilització del programa de dibuix per fer construccions.

[12] Llibre [1], pàg.216 "Vamos a intentar ofrecer una meditación intuitiva sobre este resultado"

Per poder fer la part pràctica he hagut d'aprendre a fer pàgines web i he tingut moltes dificultats. Principalment amb els problemes de format entre el programa de dibuix i el programa per elaborar la web. Hauria volgut fer una pàgina web més atractiva, però encara que vaig treballar molt a l'estiu, el temps sempre resulta insuficient i no he pogut aprofundir tant com m'hagués agradat en la part pràctica. També m'hagués agradat aprofundir molt més en l'apartat de polígons regulars, però el treball ja era molt extens i només he fet la construcció d'un polígon regular, el pentàgon. La construcció del pentàgon m'ha semblat molt interessant i, sabent que Gauss va aconseguir fer la del polígon de disset costats m'hagués agradat continuar per aquí la meva recerca, però el tema és tan extens que dóna per fer un altre treball de recerca..

Vull agrair la col·laboració tant del tutor de l'institut, Rafa Martínez, per les seves orientacions per millorar el treball, com al tutor de l'Argó, Eduard Gallego, per la seva dedicació i ajut. També vull agrair l'ajut de l'Edgar Carretero, que m'ha ensenyat a utilitzar els programes per fer la pàgina web i sense el qual m'hagués resultat impossible fer-la. Però especialment, vull agrair la col·laboració del meu pare, sense el qual hagués estat completament impossible realitzar aquest treball, ja que m'ha ajudat a entendre la bibliografia i a elaborar algunes de les demostracions.

En definitiva, la realització d'aquest treball de recerca m'ha resultat molt interessant i positiva. M'ha sorprès que aquest treball m'ha donat una visió de les matemàtiques molt diferent de la que tenia fins ara, molt més abstracta i deductiva. Abans de la realització d'aquest treball no estava habituat a fer demostracions matemàtiques i he après a valorar la importància del rigor en les afirmacions i demostracions. Sobretot, he après a valorar la importància que té en la ciència la feina feta durant segles per poder aconseguir nous objectius.

10. Bibliografia

Llibres i monografies

[1] ALSINA, Claudi; TRILLAS, Enric. *Lecciones de Algebra y Geometria*. Ed. Gustavo Gili, 1984.

[2] CARREGA, Jean-Claude. *Théorie des Corps, La règle et le compas*. Ed. Hermann, 1981.

[3] TEBAR FLORES, Emilio. *Problemas de álgebra lineal*. Madrid, 1977.

[4] LANG, Serge. *Algebra*. Madrid: Ed. Aguilar, 1977.

[5] QUEYSANNE, Michel. *Algebra basica*. Barcelona: Ed.Vicens Vives, 1971.

[6] STEWART, Ian. *Galois Theory*. Mathematical Series, 1973.

[7] COURANT, Richard; ROBBINS, Herbert. *¿Qué es la matemática?*. Ed. Aguilar, 1964.

[8] BOYER B., Carl. *Historia de la matemática*. Ed. Alianza, Madrid, 1968.

Articles de pàgines i llocs web

[9] *Construcciones con regla y compàs* [en línia], actual 22-07-09. Disponible des d'Internet en: http://gaussianos.com/construcciones-con-regla-y-compas-i-introduccion-y-primeras-construcciones/ [consulta 29-07-09]

[10] *Regla y compàs* [en línia], actual 22-07-09. Disponible a:http://es.wikipedia.org/wiki/Construcciones_con_regla_y_comp%C3%A1s [consulta 21-07-09]

[11] *Math Open Reference* [en línia], actual 12-09-09. Disponible des d'Internet en: http://www.mathopenref.com/constructions.html [consulta 17-09-09]

[12] *Physics daily, The Physics Encycplopedia* [en línia], actual 07-10-09. Disponible a http://www.physicsdaily.com/physics/Euler%27s_totient_function [consulta 7-10-09]

[13] *Physics daily, The Physics Encycplopedia* [en línia], actual 7-10-09. Disponible a: http://www.physicsdaily.com/physics/Cyclotomic_polynomial [consulta 9-10-09]

[14] *Àlgebra Abstracta, Teoria de Galois* [en línia], actual 7-10-09. Disponible a: http://www-ma2.upc.es/~quer/docencia/AA/galois.pdf

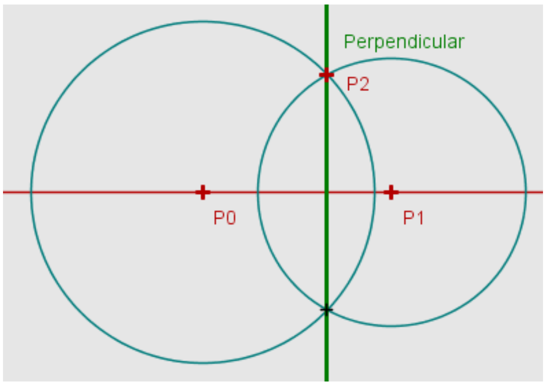
11. Referències

Annexos

Annex 1: Altres mètodes per realitzar construccions bàsiques

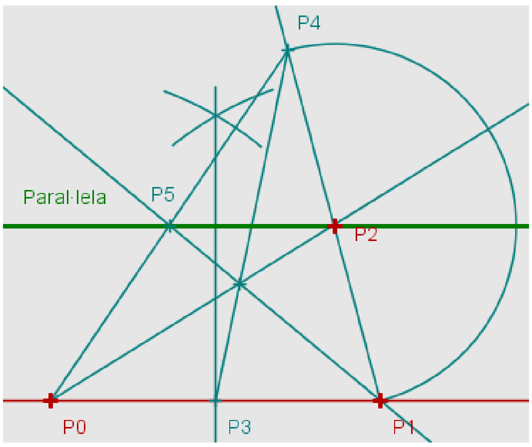
A continuació explicaré dos mètodes alternatius per traçar rectes perpendiculars i paral·leles en menys passos que els explicats anteriorment, però que no els he fet constar en l'apartat de construccions bàsiques perquè no estan demostrats matemàticament.

Perpendicular a una recta per un punt exterior



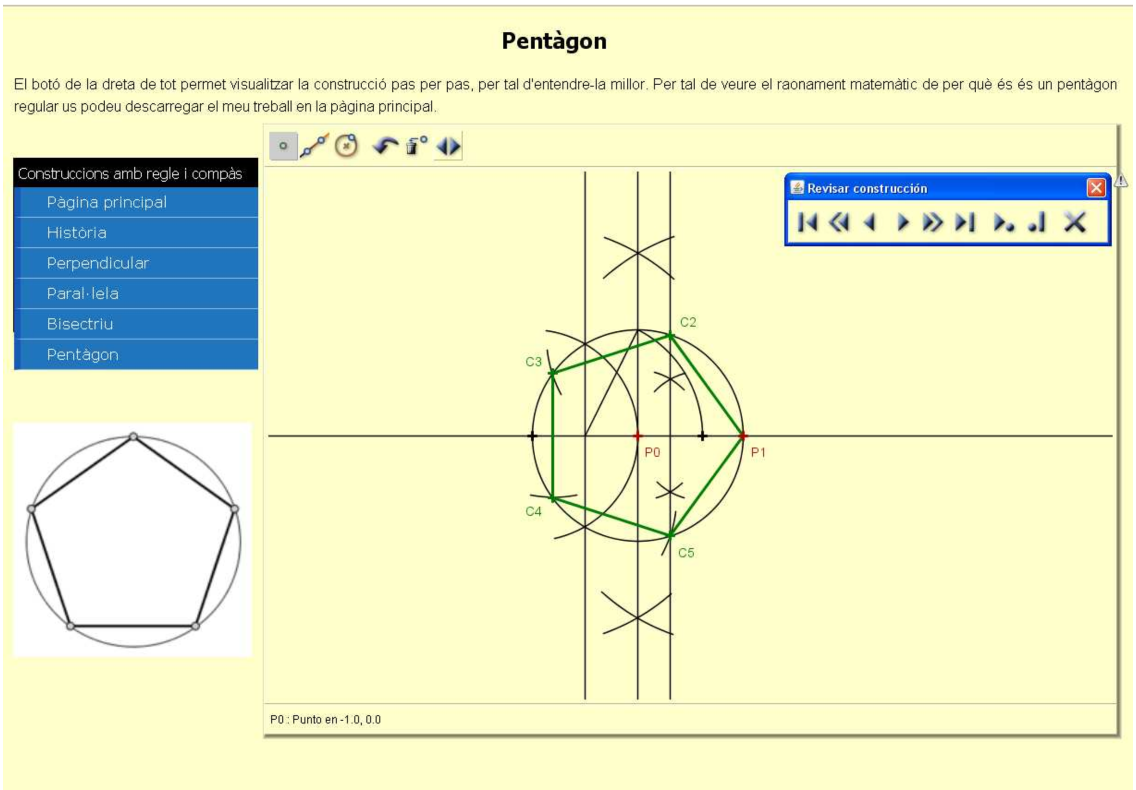
Partim de tres punts p_0, p_1, p_2 no alineats. Dos punts p_0, p_1 determinen una recta i p_2 és un punt exterior a la recta. Tracem la circumferència de centre p_1 i radi la distància entre p_1 i p_2. A continuació, tracem una altra circumferència de centre p_0 i radi la distància entre p_0 i p_2. La intersecció de les dues circumferències determina un nou punt, la recta que passa per aquest punt i per p_2 és la recta perpendicular a la recta determinada per p_0, p_1 que passa per p_2.

Paral·lela a una recta per un punt exterior:

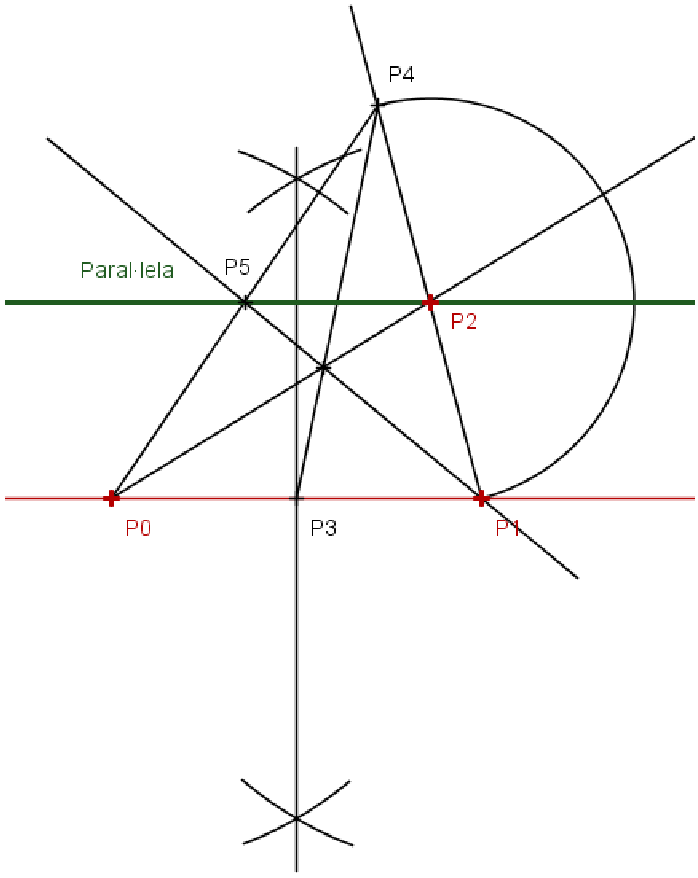


Partim de tres punts p_0, p_1, p_2 no alineats. Dos punts p_0, p_1 determinen una recta i p_2 és un punt exterior a la recta. Tracem la mediatriu de p_0 i p_1 per trobar el punt mig, p_3. Tracem una recta que uneixi p_1 i p_2 i trobem el simètric de p_1 respectep_2 que anomenem p_4. Tracem la recta que uneix p_3 i p_4 i la que uneix p_0 i p_2. La intersecció d'aquestes rectes determina un nou punt, tracem la recta que uneix aquest punt amb p_1. Aqueta recta tallarà la recta determinada per p_0 i p_4 en un nou punt que anomenarem p_5. La recta resultant d'unir p_2 i p_5 és la recta paral·lela a la recta determinada per p_0 i p_1 que passa per p_2.

Annex 2: Imatges de la pàgina web



Construccions amb regle i compàs



Autor: Raül Castrillo Gómez

Tutor del centre: Rafa Martínez

Tutor de l'Argó: Eduardo Gallego

IES Pere Calders

Data de lliurament: 09-11-2009