Butlletí de la Societat Catalana de Matemàtiques
Vol. 21, núm. 1, 2006. Pàg. 81–155

L'àlgebra de la papiroflèxia*

Josep Pla i Carrera

Resum Aquest article, seguint l'exemple de la construcció geomètrica amb regle i compàs, analitza allò que hom pot fer amb papiroflèxia. Ho fa en dos aspectes. Ofereix una definició general de construcció geomètrica amb papiroflèxia que, convenientment concretada, genera tres geometries del pla: la que s'aconsegueix amb un regle i un transportador de distàncies, la que s'obté amb regle i compàs, i la que s'obté amb regle, circumferències i còniques. Després observa que aquesta darrera correspon als nombres que s'aconseguixen resolent cúbiques i quàrtiques.

Paraules clau: geometria construïble, regle i compàs, papiroflèxia, àlgebra de la papiroflèxia.

Classificació MSC2000: 51-01.

1 Introducció

Qui entre nosaltres, en algun moment o un altre de la vida, no ha fet un plec en un full de paper? I qui no n'ha fet dos, de plecs, que, en tallar-se, generin un punt? Tots, en una ocasió o una altra, ho hem fet. Potser, fins i tot, moltes més vegades que no pas hem determinat un punt del pla tallant una recta i una circumferència.

Ara bé, ens hem preguntat mai, encara que només sigui per analogia, *quina és l'àlgebra que hi ha sota l'art de la papiroflèxia*? En tot cas, n'hi ha alguna? És fàcilment identificable? És clar que, per poder respondre aquestes preguntes amb rigor, abans hem d'establir amb precisió, formalment parlant, què és l'art de la papiroflèxia.

* Aquest article correspon a la conferència donada per l'autor a la Trobada Matemàtica de la SCM del maig de 2002.

Sabem que la geometria del regle i el compàs és força antiga, almenys tan antiga com la geometria grega. És a dir, remunta al segle VI aC. També sabem que alguns problemes, coneguts com els *problemes clàssics*, com ara la *trisecció de l'angle* i la *duplicació del cub*[1] no van poder ser reduïts a la *geometria plana*.[2]

Sabem també que el primer matemàtic que va posar les coses al seu lloc —en un joc genial d'interrelacions entre l'àlgebra i la geometria— va ser René Descartes (1596–1650). Va fer que la pregunta

Quina és l'àlgebra que hi ha sota la geometria plana?

comencés a tenir sentit.

Les seves paraules situen el nucli de la qüestió. Tot just abans d'enunciar els quatre preceptes del *seu mètode* que, «tot comprenent els avantatges d'aquestes tres [arts o ciències], estigués exempt dels seus defectes»,[3] diu:

> Quant a l'anàlisi dels antics i a l'àlgebra dels moderns, a més de no aplicar-se sinó a matèries molt abstractes i que no semblen de cap utilitat, la primera està sempre tan lligada a la consideració de les figures que no pot exercitar l'enteniment sense fatigar la imaginació, i, en la darrera, s'està tan lligat a certes regles i a certes xifres que se n'ha fet un art confús i obscur, que embarassa l'esperit, en comptes d'una ciència que el cultivi. Això em va fer pensar que calia buscar algun altre mètode que, tot comprenent els avantatges d'aquestes tres, estigués exempt dels seus defectes.[4]

Pel que fa a la geometria, cal posar cada cosa al lloc just perquè s'aclareixi tot el que és fosc i cal fer-ho sense fatigar la imaginació.[5] Per això, a l'inici del llibre primer de la *Géométrie*, exposa la *metodologia* de la geometria —de la manera nova d'entendre i fer geometria—, és a dir, la manera d'entendre-la en endavant.

> Tots els problemes de geometria es poden reduir amb facilitat a termes en què, en endavant, només sigui necessari conèixer la longitud d'algunes línies rectes per tal de poder-los construir.[6]

Aleshores s'adona que les *construccions geomètriques* —operacions entre segments rectilinis que generen segments rectilinis nous— admeten un *correlat*

1 Vegeu, per exemple, [9, 235–270].

2 Un problema geomètric és *pla* quan la seva resolució depèn de l'ús de rectes i circumferències. Vegeu [13, 926].

3 Les tres arts o ciències són la *lògica*, d'«entre les parts de la filosofia», i l'*anàlisi dels geòmetres* i l'*àlgebra*, d'«entre les matemàtiques», vegeu [3, 96 i 98].

4 Vegeu [3, 97–98].

5 «Després, en adonar-me que, per a conèixer les esmentades proposicions, a vegades em caldria considerar cadascuna d'elles en particular i altres vegades només retenir-ne o comprendre'n unes quantes conjuntament, vaig pensar que, per a considerar-les millor en particular, les havia de suposar entre línies, atès que no trobava res de més simple i que pogués presentar més distintament a la meva imaginació i als meus sentits; però que, per a retenir-ne o comprendre'n unes quantes conjuntament, em calia explicar-les per mitjà de xifres, tan curtes com fos possible; i que, d'aquesta manera, agafava el millor de l'anàlisi geomètrica i de l'àlgebra i corregia tots els defectes de l'una per mitjà de l'altra.» Vegeu [3, 101–102].

6 Vegeu [4, 13].

aritmètic —operacions entre els nombres reals que designen les longituds dels segments implicats en la construcció geomètrica. Això li permet plantejar-se la pregunta que suara ens fèiem nosaltres, i ho fa al llibre primer, el qual titula *Dels problemes que es poden construir fent ús exclusivament de les circumferències i de les línies rectes*. S'adona que, geomètricament, a la suma, la resta, la multiplicació, la divisió i l'extracció d'arrels quadrades de segments rectilinis —de les seves longituds— els correspon un segment rectilini —una *línia recta*— que és *construïble*, a partir dels segments donats i d'un segment unitat, amb l'ús exclusiu del regle i el compàs.[7]

En definitiva, René Descartes estableix *informalment* el que, en termes actuals, fóra el resultat següent:

TEOREMA DE DESCARTES *Fixada una unitat, la classe* $\mathbb{E}$ *dels nombres reals construïbles amb regle i compàs té l'estructura algèbrica d'un cos commutatiu i, a més, és tancada per l'extracció d'arrels quadrades dels seus elements positius.*[8]

El subcòs $\mathbb{E} \subseteq \mathbb{R}$ del teorema anterior —que és, de fet, el *més petit* subcòs de $\mathbb{R}$ tancat per arrels quadrades—[9] rep el nom de *cos pla* o de *cos euclidià* de $\mathbb{R}$.[10]

Tanmateix, Descartes va més lluny i, un cop ha deixat ben clar el que podem fer amb regle i compàs, diu:

> I si els problemes es poden resoldre mitjançant la geometria ordinària, és a dir, fent servir solament línies rectes i circumferències dibuixades sobre una superfície plana, quan la darrera equació hagi estat completament desentrellada, constarà, com a màxim, d'un únic quadrat desconegut, igual al producte de la seva arrel per una quantitat coneguda, més o menys alguna altra quantitat coneguda.[11]

És a dir, els problemes geomètrics resolubles amb regle i compàs menen finalment —i aquí la dificultat rau a comprendre el significat del terme *finalment*— a una equació de segon grau, la solució de la qual proporciona el *nombre construït*, entès sempre com la longitud del segment construït geomètricament. Amb això Descartes estableix que el cos $\mathbb{E}$ *és tancat per equacions de segon grau* en el sentit següent:

> Si $aX^2 + bX + c = 0$ és una equació de segon grau, amb $a, b, c \in \mathbb{E}$, no tots nuls, i amb $\Delta = b^2 - 4ac > 0$, aleshores les seves arrels α_1 i α_2 també pertanyen a $\mathbb{E}$.

7 Vegeu [4, XXXVI–XXXVII].

8 Naturalment, per *nombre real construïble* (amb el giny que sigui), entenem la longitud d'un segment rectilini, construïble amb el giny en qüestió, a partir d'un segment que considerem *el* segment unitat.

9 Tot avançant-nos a la secció 3, recordem que un cos $K \subseteq \mathbb{R}$ és *tancat per arrels quadrades* quan conté els nombres $\sqrt{\Delta}$, amb $\Delta \in K, \Delta > 0$.

10 Vegeu la definició 2.12.

11 Vegeu [4, 20].

Així, $\mathbb{E}$ és també el *més petit* subcòs de $\mathbb{R}$ que conté *totes les arrels reals* de les equacions de segon grau amb coeficients en $\mathbb{E}$.[12]

Aquest resultat, però, fou demostrat dos-cents anys més tard. Calgué esperar fins a l'any 1837 per disposar d'un article breu d'un jove estudiant de l'École Polytechnique de París, Pierre-Laurent Wantzel (1814–1848), on s'enuncia de manera precisa i es demostra amb rigor l'afirmació de Descartes.

> Suposem que un problema de geometria pot ser resolt per mitjà d'interseccions de línies rectes i de circumferències. Si hom uneix els punts obtinguts amb els centres dels cercles i amb els punts que determinen les rectes, tindrà una concatenació de triangles rectilinis els elements dels quals podran ser calculats per trigonometria. Tanmateix, aquestes fórmules són equacions algèbriques que només contenen els costats i les línies trigonomètriques dels angles en primer i segon grau. Així, doncs, la incògnita principal del problema s'obtindrà resolent una *sèrie* d'equacions de segon grau els coeficients de les quals seran funcions racionals de les dades del problema i de les arrels de les equacions precedents. A la vista de tot això, per saber si la construcció d'un problema de geometria es pot fer amb regle i compàs, cal mirar si és possible fer dependre les arrels de l'equació a la qual condueix el problema de les arrels d'un sistema d'equacions de segon grau formades tal com he indicat.[13]

De fet, Wantzel s'adona que, cada cop que construïm un nombre nou, usant el compàs, fem una extensió quadràtica del cos anterior. Això permet establir, com dèiem, que $\mathbb{E}$ és el més petit subcòs de $\mathbb{R}$ tancat per arrels quadrades dels elements positius. Wantzel va més lluny i estableix el famós teorema següent:

TEOREMA DE WANTZEL *Tot nombre construïble amb regle i compàs ha de ser la solució d'un polinomi irreductible sobre $\mathbb{Q}$ el grau del qual és una potència de 2, sent els seus coeficients les dades del problema.*[14]

Val la pena indicar que el recíproc és fals.[15] Sabem que les equacions cúbiques i quàrtiques són resolubles tallant una circumferència i una paràbola. Descartes és ben clar en el paràgraf «Manera general de construir tots els problemes sòlids reduïts a una equació de tres o quatre dimensions»:

> Quan un està segur que el problema és sòlid, tant si l'equació és un quadrat-quadrat com si és un cub, sempre és possible trobar-ne l'arrel per mitjà d'una de les tres seccions còniques, o fins i tot per una de les seves parts, per petita que sigui. La resta seran solament línies rectes i circumferències. M'acontentaré a donar una regla general per trobar-les totes mitjançant una paràbola perquè és, d'alguna manera, la més simple.[16]

Per tant les seves arrels, en principi, no són euclidianes.

12 A la secció 3, veurem l'equivalència de les tres presentacions alternatives informals del cos $\mathbb{E}$ d'aquesta introducció.
13 [22, 366]
14 [22, 367-368]
15 Vegeu la nota 3.
16 [4, 125].

Descartes va encara una mica més lluny quan estableix el resultat següent:

> Les arrels de les cúbiques i les quàrtiques s'aconsegueixen amb dues operacions geomètriques diferents: la *duplicació del cub* i la *trisecció de l'angle*.

Aquest resultat ja havia estat intuït per Rafael Bombelli (1526–1573)[17] i demostrat, amb tota mena de rigor, per l'il·lustre matemàtic francès François Viète (1540–1603).[18] Descartes l'aclareix i el sintetitza amb les paraules següents:

> *Tots els problemes sòlids es poden reduir a aquestes dues construccions.* Seria ben superflu que m'entretingués a donar uns altres exemples, perquè tots els problemes sòlids es poden reduir de manera que no calgui cap altra regla per construir-los que la que serveix per trobar dues mitjanes proporcionals, o bé dividir un angle en tres parts iguals. I això ho coneixereu si considereu que les dificultats del problema poden ser recollides en equacions que no passen del quadrat-quadrat, o del cub.[19]

Suposem, doncs, que, a més del regle i el compàs, disposéssim d'un giny —com ara el *mesolabum*— que permetés trobar dues mitjanes proporcionals i, de retruc, doblar el cub.[20] Amb aquest giny podríem extreure arrels cúbiques i, per tant, resoldre les equacions de tercer grau amb *discriminant positiu*. Aleshores, per analogia, podríem considerar $\mathbb{D}$ el més petit subcòs de $\mathbb{R}$ tancat per extracció d'arrels cúbiques. En canvi, si disposéssim d'un giny que permetés trisecar angles —per exemple, el *tomahawk*—, tindríem $\mathbb{T}$, el més petit subcòs de $\mathbb{R}$, tancat per trisecció d'angles. Amb aquest giny podríem resoldre les equacions de tercer grau amb *discriminant negatiu*. Són les cúbiques conegudes amb el nom de *cúbiques irreductibles*.[21] Els cossos $\mathbb{D}$ i $\mathbb{T}$ són diferents, atès que $\sqrt[3]{2} \notin \mathbb{T}$ i $\cos 20 \notin \mathbb{D}$.[22] Finalment podem considerar el més petit subcòs $\mathbb{V}$ del cos $\mathbb{R}$ tancat alhora per aquestes dues operacions geomètriques.[23] Òbviament, $\mathbb{V}$ és el més petit subcòs de $\mathbb{R}$ que conté els cossos $\mathbb{D}$ i $\mathbb{T}$.

Bé, doncs, la qüestió que es planteja ara és la següent:

> Si introduïm definicions adequades de *papiroflèxia*, podrem aconseguir construir els nombres reals dels cossos $\mathbb{E}$ i $\mathbb{V}$?

17 [1, 639–641]. Vegeu [15, II, 31–32].

18 [20, capítol VI, teorema 3, 90–91] i [21, 248–251]. Vegeu [10, 122–123].

19 [4, 133].

20 Per doblar el quadrat, cal determinar una mitjana proporcional MN entre dos segments AB i $AC = 2AB$ —és a dir, $\frac{AB}{MN} = \frac{MN}{AC}$—, quelcom que resol el teorema de l'alçada d'un triangle rectangle.

Hipòcrates de Quios (~460 aC) observà, per generalització del cas anterior, que el problema de *doblar el cub* era reduïble a cercar *dues mitjanes proporcionals* MN i PQ entre dos segments AB i $AC = 2AB$. És a dir, a determinar MN i PQ de manera que $\frac{AB}{MN} = \frac{MN}{PQ} = \frac{PQ}{AC}$. Vegeu [9, 200–201].

21 Vegeu [17, II, 461 i 464].

22 Ho podem veure consultant [12, 142].

23 Tenim la cadena següent:

$$\mathbb{Q} \subsetneq \mathbb{E} \begin{array}{c} \subsetneq \\ \subsetneq \end{array} \begin{array}{c} \mathbb{D} \\ \mathbb{T} \end{array} \subsetneq \mathbb{V}.$$

Veurem que la resposta és afirmativa. Aquest és, de fet, l'objectiu del treball que presentem. Abans, però, per qüestions de claredat expositiva donarem uns prerequisits i, després, farem un repàs breu de la *construcció amb regle i compàs* i de l'àlgebra subjacent. Veurem també que hi ha una papiroflèxia que permet construir els punts del cos $\mathbb{P}$, el més petit subcòs de $\mathbb{R}$ tancat pel teorema de Pitàgores.[24] És a dir, si $a, b \in \mathbb{P}$, aleshores $\sqrt{a^2+b^2} \in \mathbb{P}$.[25]

2 Prerequisits

Donat un subcòs $K \subseteq \mathbb{R}$,[26] parlarem d'una recta, una circumferència, una paràbola, etc., del cos K, quan els seus coeficients siguin elements del cos K. Així, doncs,

2.1 DEFINICIÓ *Siguin $a, b, c, d, e, f \in K$. Aleshores, fixada una referència cartesiana,*

- *el punt P de coordenades $\langle a, b\rangle$ és un* punt del cos K;
- *la recta ℓ d'equació $aX + bY + c = 0$ és una* recta del cos K;
- *la circumferència $\mathcal{O}$ d'equació $X^2 + Y^2 + 2bX + 2cY + d = 0$ és una* circumferència del cos K;
- *la paràbola $\mathcal{P}$ d'equació $aX^2 + bY^2 + 2cXY + 2dX + 2eY + f = 0$, amb $c^2 - ab = 0$, és una* paràbola del cos K.[27]

2.2 DEFINICIÓ *Una* extensió pitagòrica *o* mètrica *d'un cos K és un cos de la forma*

$$K\left(\sqrt{\Pi}\right) = \left\{k_1 + k_2\sqrt{\Pi} : k_1, k_2 \in K\right\},\ \textit{on}\ \Pi = a^2 + b^2,\ \textit{amb}\ a, b \in K.$$

Una extensió euclidiana, plana *o* quadràtica *d'un cos K és un cos de la forma*

$$K\left(\sqrt{\Delta}\right) = \left\{k_1 + k_2\sqrt{\Delta} : k_1, k_2 \in K\right\},\ \textit{on}\ \Delta \in K\ \textit{i}\ \Delta > 0.$$

Una extensió vietana *o* sòlida *d'un cos K és el més petit cos que conté K i les arrels reals d'una quàrtica $aX^4 + bX^3 + cX^2 + dX + e = 0$, amb $a, b, c, d, e \in K$.*

2.3 DEFINICIÓ *Un cos K és un* cos pitagòric *si, i només si, és tancat pel teorema de Pitàgores. És a dir, per a cada parella $a, b \in K$, $\sqrt{a^2+b^2} \in K$.*

2.4 DEFINICIÓ *Un cos K és un* cos euclidià *si, i només si, és tancat per arrels quadrades. És a dir, per a cada $\Delta \in K, \Delta > 0$, $\sqrt{\Delta} \in K$.*

24 És la papiroflèxia del text [2, 156–163].

25 Com veurem més endavant a la definició 3.16, hi ha una funció del compàs —*portar segments*— que és més feble que fer circumferències.

26 Si no fem cap especificació concreta, tots els cossos que considerarem seran subcossos de $\mathbb{R}$.

27 En endavant suposarem sobreentès que hem fixat una referència i, simplement, escriurem: $P := \langle a, b\rangle$, $\ell := aX + bY + c = 0$, $\mathcal{O} := X^2 + Y^2 + 2bX + 2cY + d = 0$, i $\mathcal{P} := aX^2 + bY^2 + 2cXY + 2dX + 2eY + f = 0$.

2.5 PROPOSICIÓ *Un cos K és euclidià si, i només si, conté les arrels reals de les equacions quadràtiques $aX^2 + bX + c = 0$, amb $a, b, c \in K$, i $\Delta = b^2 - 4ac > 0$; i si, i només si, és tancat per extensions quadràtiques.* □

2.6 DEFINICIÓ *Un cos K és un* cos vietà *si, i només si, conté les arrels reals de les equacions quàrtiques $aX^4 + bX^3 + cX^2 + dX + e = 0$, amb $a, b, c, d, e \in K$.*

2.7 PROPOSICIÓ *Un cos K és vietà si, i només si, és quadràtic*[28] *i conté les arrels reals de les equacions cúbiques $aX^3 + bX^2 + cX + d = 0$, amb $a, b, c, d \in K$; i si, i només si, és tancat per extensions sòlides.* □

2.8 DEFINICIÓ *Sigui K un subcòs de $\mathbb{R}$.*

K és tancat per arrels cúbiques *si, i només si, per a cada $a \in K$, tenim que $\sqrt[3]{a} \in K$.*

K és tancat per trisecció *si, i només si, per a cada $\cos\theta \in K$, tenim que $\cos\frac{\theta}{3} \in K$.*

2.9 PROPOSICIÓ *Un cos K és vietà si, i només si, és quadràtic i tancat per extracció d'arrels cúbiques i trisecció d'angles.* □

2.10 PROPOSICIÓ *L'extensió pitagòrica (respectivament euclidiana, vietana) d'un cos pitagòric (resp. euclidià, vietà) és també pitagòrica (resp. euclidiana, vietana).* □

2.11 PROPOSICIÓ *La intersecció de cossos vietans, euclidians, pitagòrics és, respectivament, un cos vietà, euclidià, pitagòric.*

Tot cos vietà és euclidià, i tot cos euclidià és pitagòric. □

2.12 DEFINICIÓ *El més petit cos pitagòric, euclidià i vietà —és a dir, la intersecció de tots els cossos pitagòrics, euclidians, vietans—, el designarem, respectivament, $\mathbb{P}, \mathbb{E}$ i $\mathbb{V}$.*

Òbviament, $\mathbb{P} \subseteq \mathbb{E} \subseteq \mathbb{V}$.

2.13 PROPOSICIÓ *Siguin P, Q, i ℓ, respectivament, dos punts i una recta de K.*

La recta $\overleftrightarrow{PQ}$, que passa per P i Q, és una recta de K.

La circumferència $Q(\overline{QP})$, que passa per P i té com a centre el punt Q, és una circumferència de K.

La paràbola $\mathcal{P}(Q, \ell)$, que té com a focus el punt Q i com a directriu la recta ℓ, és una paràbola de K.

DEMOSTRACIÓ És un exercici elemental de càlcul. □

2.14 PROPOSICIÓ *Siguin ℓ_1, ℓ_2 dues rectes concurrents de K. Aleshores les coordenades del punt d'intersecció pertanyen a K.*

28 Observem que, si és tancat per arrels de quàrtiques, és tancat per extracció d'arrels quadrades, atès que, si $a \in K$, aleshores $a^2 \in K$ i $\sqrt[4]{a^2} = \sqrt{a}$.

Siguin ℓ i $\mathcal{O}$, respectivament, una recta i una circumferència de K que es tallin. Aleshores les coordenades dels punts de tall pertanyen a una extensió euclidiana de K.

Siguin $\mathcal{O}_1$ i $\mathcal{O}_2$ dues circumferències de K que es tallin. Aleshores les coordenades dels punts de tall pertanyen a una extensió euclidiana de K.

Siguin ℓ i $\mathcal{P}$, respectivament, una recta i una paràbola de K que es tallin. Aleshores les coordenades dels punts de tall pertanyen a una extensió euclidiana de K.

Siguin $\mathcal{O}$ i $\mathcal{P}$, respectivament, una circumferència i una paràbola de K que es tallin. Aleshores les coordenades dels punts de tall pertanyen a una extensió vietana de K.

DEMOSTRACIÓ Són proposicions immediates. La primera ve del fet que, per resoldre un sistema d'equacions lineals, només cal fer servir les operacions del cos. La segona és conseqüència del fet que, en resoldre el sistema, s'obté una equació de segon grau. La tercera és conseqüència de l'observació següent: els punts de tall de dues circumferències que es tallen són els mateixos que els punts de tall d'una de les circumferències i de la recta que s'obté restant les equacions de les dues circumferències. La següent es deu al fet que, en resoldre el sistema, s'obté una equació de segon grau. La darrera és conseqüència del fet que l'equació resultant és una quàrtica. De fet, és suficient que K sigui quadràtic i tancat per arrels reals d'equacions cúbiques amb coeficients en K.□

2.15 COROLLARI *Un cos euclidià K conté les coordenades dels punts de tall de dues rectes, d'una recta i una circumferència, d'una recta i una paràbola, i de dues circumferències, totes de K i secants.*

Un cos vietà K conté les coordenades dels punts de tall d'una circumferència i d'una paràbola, ambdues de K i secants. □

2.16 PROPOSICIÓ *Siguin $\ell_1 := a_1X + b_1Y + c_1 = 0$ i $\ell_2 := a_2X + b_2Y + c_2 = 0$ dues rectes concurrents. Les dues bisectrius $\ell := aX + bY + c = 0$ i $\ell' := a'X + b'Y + c' = 0$ dels angles que formen les rectes ℓ_1 i ℓ_2 són, respectivament:*

$$\begin{aligned}(\cos\theta_1 - \cos\theta_2)X + (\sin\theta_1 - \sin\theta_2)Y - (\gamma_1 - \gamma_2) &= 0,\\ (\cos\theta_1 + \cos\theta_2)X + (\sin\theta_1 + \sin\theta_2)Y - (\gamma_1 + \gamma_2) &= 0,\end{aligned}$$

on $\cos\theta_i = \frac{a_i}{\sqrt{a_i^2+b_i^2}}$, $\sin\theta_i = \frac{b_i}{\sqrt{a_i^2+b_i^2}}$, $\gamma_i = \frac{-c_i}{\sqrt{a_i^2+b_i^2}}$, $i = 1, 2$.

DEMOSTRACIÓ Transformem les equacions en la forma $Y = m_iX + n_i$, $i = 1, 2$.[29] Suposem que la bisectriu té l'equació $Y = mX + n$. Aleshores

$$\frac{m_2 - m}{1 + m_2m} = \frac{m - m_1}{1 + mm_1}.$$

29 Els casos en els quals una de les rectes o la bisectriu és paral·lela a la recta $X = 0$ no comporten cap dificultat. Considerem les rectes perpendiculars, i fet.

Per tant, el pendent m satisfà l'equació de segon grau:

$$(m_1 + m_2)m^2 + 2(1 - m_1m_2)m - (m_1 + m_2) = 0.$$

D'aquí resulta que

$$m = -\frac{1 - m_1m_2}{m_1 + m_2} \pm \frac{1}{m_1 + m_2}\sqrt{1 + m_1^2 + m_2^2 + m_1^2m_2^2}.$$

Si $\langle \alpha, \beta \rangle$, amb $\alpha = \frac{n_2 - n_1}{m_1 - m_2}$, $\beta = \frac{m_1n_2 - m_2n_1}{m_1 - m_2}$, és el vèrtex de l'angle que formen les rectes ℓ_1 i ℓ_2, aleshores $n = \beta - m\alpha$.

La resta és un simple càlcul trigonomètric.[30] □

2.17 COROLLARI *En les condicions del teorema anterior, si $a_i, b_i, c_i \in K$, $i = 1, 2$, els coeficients a, b, c de les bisectrius de l'angle que formen ambdues rectes pertanyen a una extensió pitagòrica de K.*

En conseqüència, si K és un cos pitagòric, les bisectrius són rectes de K. □

2.18 COROLLARI *Si $\ell := aX + bY + c = 0, \ell' := a'X + b'Y + c' = 0$ són, respectivament, les bisectrius de les rectes concurrents ℓ_1, ℓ_2, i ℓ_1', ℓ_2' de K, i K és un cos pitagòric, aleshores les coordenades del punt de tall de ℓ i ℓ', si existeix, pertanyen a K.* □

2.19 PROPOSICIÓ *Siguin $\ell := aX + bY + c = 0$ una recta d'un cos K, $P := \langle x_0, y_0 \rangle$ un punt de K de la recta ℓ, $Q_1 := \langle \alpha_1, \beta_1 \rangle, Q_2 := \langle \alpha_2, \beta_2 \rangle$ dos punts de K, i $d = d(Q_1, Q_2) = \sqrt{(\alpha_1 - \alpha_2)^2 + (\beta_1 - \beta_2)^2}$. Els punts $P_1 := \langle x_1, y_1 \rangle$ i $P_2 := \langle x_2, y_2 \rangle$ de la recta ℓ tals que $d = d(P, P_1) = d(P, P_2)$ pertanyen al cos K_2, on $K_2 = K_1\left(\sqrt{a^2 + b^2}\right)$ i $K_1 = K(d)$.*

En conseqüència, si K és un cos pitagòric, els punts P_1 i P_2 són, ambdós, punts de K.

DEMOSTRACIÓ D'una banda, $d^2 = (\alpha_1 - \alpha_2)^2 + (\beta_1 - \beta_2)^2$. Per tant, d pertany a l'extensió pitagòrica $K_1 = K(d)$. Sigui ara $P^* := \langle x, y \rangle \in \ell$ tal que $d(P, P^*) = d$. Aleshores, restant $ax + by + c = 0$ i $ax_0 + by_0 + c = 0$, s'obté $a(x - x_0) + b(y - y_0) = 0$. Per tant, $y - y_0 = -\frac{a}{b}(x - x_0)$. Però $(x - x_0)^2 + (y - y_0)^2 = d^2$. D'ací ve que $\left(1 + \frac{a^2}{b^2}\right)(x - x_0)^2 = d^2$. Finalment,

$$x_1 = x_0 + \frac{b}{\sqrt{a^2 + b^2}}\, d, \qquad y_1 = y_0 - \frac{a}{\sqrt{a^2 + b^2}}\, d;$$
$$x_2 = x_0 - \frac{b}{\sqrt{a^2 + b^2}}\, d, \qquad y_2 = y_0 + \frac{a}{\sqrt{a^2 + b^2}}\, d.$$

En resulta, doncs, que $x_i, y_i \in K_2, i = 1, 2$, on $K_2 = K_1(\sqrt{a^2 + b^2})$. K_2 és una extensió pitagòrica de K_1, i K_1 ho és de K.

La segona part és immediata. □

30 Recordem que $m_i = \tan\theta_i = -\frac{a_i}{b_i}, i = 1, 2$, i $m = \tan\theta = -\frac{a}{b}$.

Aquestes darreres proposicions suggereixen quelcom que cal remarcar. Les extensions pitagòriques $K(\sqrt{a^2+b^2})$ estan, d'alguna manera, lligades a la capacitat de fer bisectrius d'angles els costats dels quals són de K, i alhora amb la capacitat del compàs de transportar segments donats.[31]

Abans de centrar-nos en els plecs, vegem com els canvis d'eixos afecten les descripcions dels punts, les rectes, les circumferències i les paràboles d'un subcòs K dels nombres reals. Concretant,

2.20 PROPOSICIÓ *Sigui K un cos. Suposem que fem una* translació d'eixos *a un punt $O' \in K$. Aleshores, tot punt, recta, circumferència i paràbola de K es transforma, respectivament, en el nou sistema de coordenades, en un punt, una recta, una circumferència, una paràbola de K.*

DEMOSTRACIÓ Suposem que el punt $O' := \langle x_0, y_0 \rangle$, expressat en el sistema original. Aleshores el canvi de coordenades és donat, com és ben sabut, per $X' = X - x_0, Y' = Y - y_0$. La resta és immediata. □

2.21 PROPOSICIÓ *Sigui K un cos pitagòric. Suposem que fem un* gir d'eixos *de manera que els nous eixos siguin rectes de K. Aleshores, tot punt, recta, circumferència i paràbola de K es transforma, respectivament, en el nou sistema de coordenades, en un punt, una recta, una circumferència, una paràbola de K.*

DEMOSTRACIÓ Suposem que l'eix d'abscisses nou $\overleftrightarrow{U'U}$, expressat en el sistema original, té l'equació $aX + bY = 0$. Aleshores, l'eix d'ordenades nou $\overleftrightarrow{V'V}$, expressat en el sistema de coordenades original, té l'equació $bX - aY = 0$, i el canvi de coordenades és donat, com és ben sabut, per

$$\begin{aligned} x &= u\cos\alpha - v\sin\alpha, \\ y &= u\sin\alpha + v\cos\alpha, \end{aligned}$$

on $\tan\alpha = -\frac{a}{b}$. Per tant, $\cos\alpha = \frac{b}{\sqrt{a^2+b^2}}$, $\sin\alpha = \frac{a}{\sqrt{a^2+b^2}}$. Ara, atès que $a, b \in K$ i que K és un cos pitagòric, resulta que $\sin\alpha, \cos\alpha \in K$. La resta és un càlcul senzill. □

3 El regle i el compàs

És ben conegut que, amb l'ús exclusiu del regle i el compàs, els únics nombres reals construïbles són els del cos euclidià $\mathbb{E}$. Això no obstant, per una qüestió d'elegància i de coherència interna del treball, en farem una presentació ràpida i resumida.[32]

31 És el caràcter mètric del compàs.

32 El lector interessat en una presentació més acurada i detalllada pot consultar [8, 9–22], [2, 13–30] o [12].

3.1 DEFINICIÓ *En el pla* $\mathbb{R}^2$ *un punt* Q *és un* punt construïble amb regle i compàs *a partir de la base* $\mathcal{B} = \{\langle 0,0\rangle, \langle 1,0\rangle\}$,[33] *o simplement un* punt construïble amb regle i compàs, *si, i només si, existeix una successió finita de punts*

$$Q_1, Q_2, \ldots, Q_{n-1}, Q_n,$$

que compleixen:

i) El punt Q_n *és el punt* Q.

ii) Per a cada índex i, $1 \leq i \leq n$, *tenim una de les situacions següents:*

a) Q_i *és un punt de la base* $\mathcal{B}$,

b) Q_i *és la intersecció de dues* $\mathcal{B}_{i-1}$*-rectes,*

c) Q_i *és la intersecció de dues* $\mathcal{B}_{i-1}$*-circumferències,*

d) Q_i *és la intersecció d'una* $\mathcal{B}_{i-1}$*-recta i d'una* $\mathcal{B}_{i-1}$*-circumferència,*

on una $\mathcal{B}_{i-1}$-recta *és una recta del pla* $\mathbb{R}^2$ *que passa per dos punts del conjunt* $\mathcal{B}_{i-1}$*, i una* $\mathcal{B}_{i-1}$-circumferència *és una circumferència del pla* $\mathbb{R}^2$ *que passa per un punt del conjunt* $\mathcal{B}_{i-1}$ *i té com a centre un altre punt del conjunt* $\mathcal{B}_{i-1}$*, sent* $\mathcal{B}_{i-1} = \{Q_1, \ldots, Q_{i-1}\}$.

3.2 DEFINICIÓ *Una recta* ℓ *és una* recta construïble amb regle i compàs *si, i només si, passa per dos punts diferents del pla* $\mathbb{R}^2$*, construïbles amb regle i compàs.*

Una circumferència $\mathcal{O}$ *és una* circumferència construïble amb regle i compàs *si, i només si, té com a centre un punt del pla* $\mathbb{R}^2$ *i passa per un altre punt del pla* $\mathbb{R}^2$*, ambdós construïbles amb regle i compàs.*

Un nombre real $a \in \mathbb{R}$ *és* construïble amb regle i compàs *si, i només si, el punt* $P_a := \langle a, 0\rangle$ *és un punt construïble amb regle i compàs.*[34]

De la definició anterior resulta de manera evident que qualsevol recta i circumferència construïble amb regle i compàs passa, almenys, per dos punts diferents, ambdós construïbles amb regle i compàs.

D'ara endavant, el quadrat unitat $\mathcal{Q} = \{O, I, J, K\}$, on $O := \langle 0,0\rangle$, $I := \langle 1,0\rangle$, $J := \langle 0,1\rangle$ i $K := \langle 1,1\rangle$, el designarem $\mathcal{Q}$. Els punts de l'eix $\ell_X := \overleftrightarrow{OI}$ —és a dir, els punts de la forma $\langle a, 0\rangle$—, els indicarem P_a, i els punts de l'eix $\ell_Y := \overleftrightarrow{OJ}$ —és a dir, els punts de la forma $\langle 0, b\rangle$—, els indicarem Q_b.

L'objectiu, com dèiem, és veure que $\mathbb{E}$ és el cos dels nombres reals construïbles amb l'ús exclusiu del regle i el compàs.

---

33 La base $\mathcal{B}$ pot tenir uns altres punts, però això no afegeix res nou a l'anàlisi que estem fent i, per aquesta raó, ens limitarem a la base esmentada.

34 Voldria fer notar, malgrat que tothom ho vegi clar, que *no tots* els punts d'una recta (o d'una circumferència) construïble amb regle i compàs són construïbles amb regle i compàs, ni de bon tros. Pensem, per exemple, en la recta $Y = X$. Conté el punt $\langle \pi, \pi\rangle$, que no és construïble amb regle i compàs (a partir de la base $\mathcal{B}$).

3.3 LEMA *El punt d'intersecció de dues rectes concurrents construïbles amb regle i compàs és construïble amb regle i compàs.*

Els punts d'intersecció d'una recta i d'una circumferència concurrents construïbles amb regle i compàs són construïbles amb regle i compàs.

Els punts d'intersecció de dues circumferències concurrents construïbles amb regle i compàs són construïbles amb regle i compàs.

DEMOSTRACIÓ Suposem que Q és el punt d'intersecció de dues rectes —o de dues circumferències, o d'una recta i d'una circumferència— construïbles amb regle i compàs. Aleshores existeixen quatre punts P_1, P_2, R_1 i R_2, construïbles amb regle i compàs, i $\overleftrightarrow{P_1P_2}, \overleftrightarrow{R_1R_2}$ són les dues rectes, construïbles amb regle i compàs, que es tallen en el punt Q —o bé $P_1(\overline{P_1P_2}), R_1(\overline{R_1R_2})$ les dues circumferències construïbles amb regle i compàs que es tallen en el punt Q; o bé $\overleftrightarrow{P_1P_2}$ la recta i $R_1(\overline{R_1R_2})$ la circumferència, construïbles amb regle i compàs, que es tallen en el punt Q. En tots els casos, disposem de quatre successions finites de punts,

$$P_{11}, \dots, P_{1n_1}; \quad P_{21}, \dots, P_{2n_2}; \quad R_{11}, \dots, R_{1n_1'}; \quad R_{21}, \dots, R_{2n_2'}$$

que satisfan les condicions de la definició 3.2, amb $P_{1n_1} = P_1$, $P_{2n_2} = P_2$, $R_{1n_1'} = R_1$, i $R_{2n_2'} = R_2$. Ara considerem la successió conjunta

$$P_{11}, \dots, P_{1n_1}, P_{21}, \dots, P_{2n_2}, R_{11}, \dots, R_{1n_1'}, R_{21}, \dots, R_{2n_2'}, Q.$$

Òbviament compleix totes les condicions de la definició 3.2, i això acaba la demostració. □

3.4 PROPOSICIÓ *Si Q i ℓ són, respectivament, un punt i una recta construïbles amb regle i compàs, la perpendicular a ℓ que passa per Q també ho és, de construïble amb regle i compàs.*

DEMOSTRACIÓ Tal com indica la figura 1, cal distingir dos casos: i) $Q \in \ell$ i ii) $Q \notin \ell$.

i) Si $Q \in \ell$, amb centre en Q, tirem la circumferència que passa per P_1, on P_1 és un altre dels punts construïbles amb regle i compàs de ℓ. Tallarà la recta ℓ en els punts, diametralment oposats, P_1 i P_2. Ara, amb centre en cadascun d'aquests i radi $\overline{P_1P_2}$, fem dos arcs de circumferència que es tallaran en el punt P. La recta $\overleftrightarrow{PQ}$ és la perpendicular buscada.

ii) Si $Q \notin \ell$, amb centre en el punt Q i un radi fet amb un segment que tingui un extrem en Q i l'altre en un punt de la recta ℓ construïble amb regle i compàs, tirem un arc de circumferència. Tallarà ℓ en dos punts Q_1 i Q_2. Ara, amb centre en Q_i, $i = 1, 2$, i radi $\overline{Q_1Q_2}$, determinem el punt P. La recta $\overleftrightarrow{PQ}$ és la perpendicular buscada. □

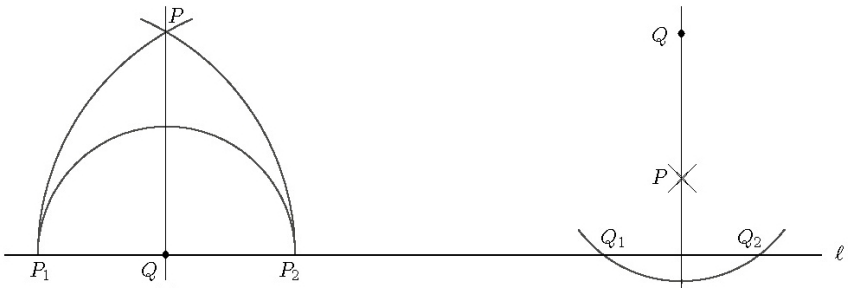


FIGURA 1

3.5 COROL·LARI *Siguin Q i ℓ, respectivament, un punt i una recta construïbles amb regle i compàs, amb $Q \notin \ell$. És possible construir, amb regle i compàs, la paral·lela a ℓ que passa per Q.*

DEMOSTRACIÓ Cal fer la perpendicular ℓ' a ℓ que passa per Q i després la perpendicular ℓ'' a ℓ' que passa per Q. Òbviament $Q \in \ell''$ i $\ell'' \parallel \ell$. □

3.6 COROL·LARI *Un punt $P := \langle a, b\rangle$ és construïble amb regle i compàs si, i només si, ho són els nombres reals a i b. És a dir, si, i només si, ho són els punts P_a, P_b.*

Per tant, el punt $K := \langle 1, 1\rangle$ és construïble amb regle i compàs i, de retruc, el quadrilàter unitat $\mathcal{Q}$ també.

DEMOSTRACIÓ És una conseqüència senzilla i immediata de la proposició anterior. Vegeu la figura 2.

Podem tirar l'eix ℓ_Y, determinar els punts J i K i construir les diagonals $\overleftrightarrow{OK}$ i $\overleftrightarrow{IJ}$. El quadrat $\mathcal{Q}$ i les seves dues diagonals són, doncs, construïbles amb regle i compàs.

També podem tirar les perpendiculars del punt P als eixos ℓ_X i ℓ_Y (i recíprocament dels punts P_a i P_b als eixos que, en tallar-se, determinen el punt P) i la paral·lela a la recta $\overleftrightarrow{IJ}$ que passa pel punt Q_b. □

3.7 PROPOSICIÓ *Els punts construïbles amb regle i compàs formen un cos euclidià.*

DEMOSTRACIÓ Les operacions aritmètiques elementals de sumar, restar, multiplicar i dividir nombres reals construïbles amb regle i compàs són, al seu torn, construïbles amb regle i compàs.[35]

L'extracció d'arrels quadrades de nombres reals positius, construïbles amb regle i compàs, també és construïble amb regle i compàs. És un exercici senzill de geometria.

35 De fet, solament cal el regle. Vegeu la secció 4.

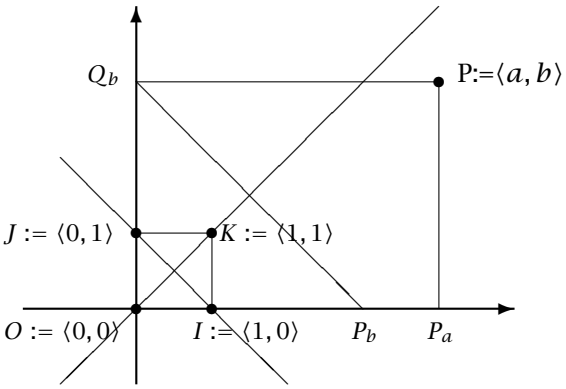


FIGURA 2

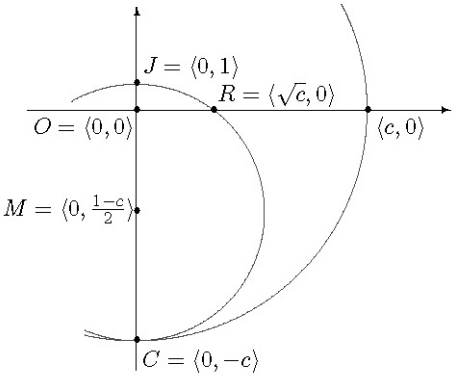


FIGURA 3

Tanmateix, la figura 3 mostra l'extracció de l'arrel quadrada $\sqrt{c}$ d'un nombre $c > 0$.[36] □

Anomenem $\mathbb{E}^*$ el cos euclidià dels nombres reals construïbles amb regle i compàs. Aleshores,

3.8 COROLLARI *El cos euclidià $\mathbb{E}$ és inclòs en el cos euclidià dels nombres reals construïbles amb regle i compàs $\mathbb{E}^*$.*

36 Vegeu [4, 14]. Per a l'extracció d'arrels quadrades, el compàs és essencial.
La complexitat de la nostra figura —hauria estat suficient, com fa Descartes, determinar la mitjana proporcional de c i 1— ve del fet que hem volgut representar la dada inicial c i el resultat final $\sqrt{c}$ a l'eix de les ics. És a dir, partim del punt $P_c := \langle c, 0\rangle$, i determinem el punt $P_{\sqrt{c}} := \langle \sqrt{c}, 0\rangle$.

DEMOSTRACIÓ D'acord amb la definició 2.12, el cos euclidià $\mathbb{E}$ —el més petit dels cossos euclidians de $\mathbb{R}$— és donat per

$$\mathbb{E} = \bigcap_{K \in \mathcal{E}} K,$$

on $\mathcal{E}$ és la classe dels subcossos euclidians de $\mathbb{R}$ i, per tant, $\mathbb{E}^* \in \mathcal{E}$. □

Hem de veure que tot punt construïble amb regle i compàs pertany al cos euclidià $\mathbb{E}$.

3.9 DEFINICIÓ *Una* extensió euclidiana (quadràtica) iterada

$$K_n = K\left(\sqrt{\Delta_1}, \sqrt{\Delta_2}, \ldots, \sqrt{\Delta_{n-1}}\right)$$

d'un cos K *és el terme final de la cadena d'extensions euclidianes [quadràtiques]*

$$K_0 = K \subseteq K_1 \subseteq K_2 \subseteq \cdots \subseteq K_{n-1} \subseteq K_n,$$

on cada $K_i = K_{i-1}(\sqrt{\Delta_i}), \Delta_i \in K_{i-1}, \Delta_i > 0, i = 1, \ldots, n.$

3.10 PROPOSICIÓ *Les coordenades d'un punt construïble amb regle i compàs pertanyen a una extensió euclidiana iterada de* $\mathbb{Q}$.

DEMOSTRACIÓ Com hem vist en els prerequisits, cada cop que fem l'operació de tallar dues rectes, una recta i una circumferència, o dues circumferències, ens col·loquem en un cos que, com a màxim, és una extensió euclidiana de l'anterior. Per tant, tot nombre real construït amb regle i compàs, atès que només necessita un nombre finit d'operacions geomètriques, es troba en una extensió euclidiana iterada de $\mathbb{Q}$. □

3.11 COROL·LARI *Tot nombre real* $\alpha \in \mathbb{E}^*$ *pertany a una extensió euclidiana iterada del cos* $\mathbb{Q}$ *dels nombres racionals.*

DEMOSTRACIÓ És immediata. □

3.12 TEOREMA *El cos* $\mathbb{E}$ *coincideix amb el cos* $\mathbb{E}^*$ *dels nombres construïbles amb regle i compàs.*

DEMOSTRACIÓ Només hem de veure que el cos $\mathbb{E}$ és igual a la reunió de totes les extensions euclidianes iterades de $\mathbb{Q}$, la qual cosa és trivial perquè $\mathbb{Q} \subseteq \mathbb{E}$ i $\mathbb{E}$ és tancat per arrels quadrades. □

3.13 COROL·LARI *El cos* $\mathbb{E}$ *és el més petit subcòs del cos* $\mathbb{R}$ *dels nombres reals que és tancat per arrels reals d'equacions de segon grau amb coeficients en* $\mathbb{E}$.

DEMOSTRACIÓ És trivial. □

3.14 PROPOSICIÓ *Tota extensió euclidiana de K, $K(\sqrt{\Delta})$, és un espai vectorial sobre K de dimensió 2.*

Tota extensió euclidiana iterada de K, K', és un K-espai vectorial sobre K la dimensió del qual és una potència de 2.

DEMOSTRACIÓ N'hi ha prou veient que:

a) $\left\{1, \sqrt{\Delta}\right\}$ és una base de $K(\sqrt{\Delta})$ sobre K.

b) Per inducció sobre el nombre n de passos en la cadena d'extensions quadràtiques que calen per passar de K a K'. Per a $n = 0$, la dimensió és $1 = 2^0$.

Si $\{\beta_1, \ldots, \beta_{n_i}\}$, amb $n_i = 2^{m_i}$ és una base de K_i sobre K, aleshores, d'acord amb la definició 3.9, $\{\beta_1, \ldots, \beta_{n_i}, \beta_1\sqrt{\Delta_i}, \ldots, \beta_{n_i}\sqrt{\Delta_i}\}$ és trivialment una base de K_{i+1} sobre K. Per tant, $n_{i+1} = 2 \times 2^{m_i} = 2^{m_i+1}$.

Això acaba la demostració.[37] □

3.15 TEOREMA (TEOREMA DE WANTZEL) *Tot nombre α, construïble amb regle i compàs, és arrel d'un polinomi (irreductible) amb coeficients en $\mathbb{Q}$, el grau del qual és una potència de 2.*

DEMOSTRACIÓ Suposem que $\alpha \in K$, on K és una extensión iterada quadràtica de $\mathbb{Q}$. Aleshores $\mathbb{Q} \subseteq \mathcal{K}(\alpha) \subseteq K$ (vegeu el teorema C.6 de l'apèndix C). Per tant,

$$[K : \mathbb{Q}] = [K : \mathcal{K}(\alpha)] \times [\mathcal{K}(\alpha) : \mathbb{Q}] = 2^m.$$

D'on en resulta que $[\mathcal{K}(\alpha\colon \mathbb{Q}] = 2^r$, amb $r \leq m$, és una potència de 2. □

Tanmateix, hi ha arrels reals d'equacions irreductibles sobre $\mathbb{Q}$ de grau 2^k, per a un cert $k \in \mathbb{N}$, que no són construïbles amb regle i compàs, com mostra l'exemple següent:[38] considerem el polinomi $P(X) = X^4 - X - 1$.

i) Suposem que, segons el mètode de Descartes de resolució de quàrtiques,[39]

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

Aleshores tenim

$$\left\{\begin{array}{rcl} b + b' - a^2 &=& 0 \\ ab' - ab &=& -1 \\ bb' &=& -1 \end{array}\right. \quad \Longrightarrow \quad \left\{\begin{array}{rcl} b + b &=& a^2 \\ a(b' - b) &=& -1 \\ bb' &=& -1\,. \end{array}\right.$$

37 Vegeu també l'apèndix C.
38 Aquest exemple l'he manllevat de [2, 39–42].
39 [4, 118–119].

D'aquí ve que b i b' siguin les arrels de l'equació $Y^2 - a^2Y - 1 = 0$, i podem suposar que $a > 0$. Per tant, $b' < b$. D'on resulta que

$$\begin{cases} b &= \dfrac{a^2 + \sqrt{a^4+4}}{2} \\ b' &= \dfrac{a^2 - \sqrt{a^4+4}}{2} \end{cases} \qquad \text{i} \qquad b' - b = -\sqrt{a^4+4}\,.$$

És a dir, $a\sqrt{a^4+4} = 1$. Ara bé, el polinomi $X^2 + aX + b$ té el discriminant

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

Per tant, les arrels de l'equació $X^2 + aX + b = 0$ són complexes conjugades. En canvi, el polinomi $X^2 - aX + b'$ té el discriminant

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

Per tant, l'equació $X^2 - aX + b' = 0$ té dues arrels reals c_1 i c_2.
Atès que $a^2(a^4+4) = 1$, resulta que $a^2 > 0$ és una arrel real del polinomi $Z^3 + 4Z - 1$, que és irreductible sobre $\mathbb{Q}[Z]$. Aleshores, pel teorema de Wantzel, a^2 no és construïble amb regle i compàs, De retruc, a tampoc. Ara bé, $c_1 + c_2 = a$. Una almenys de les arrels reals c_1 i c_2 no és construïble amb regle i compàs. Així el polinomi

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

té almenys una arrel real que no és construïble amb regle i compàs.

ii) $P(X)$ és irreductible sobre $\mathbb{Q}[X]$. Òbviament, per i), $a \notin \mathbb{Q}$. Per tant, la descomposició

$$P(X) = (X^2 + aX + b)(X^2 - aX + b')$$

no és una descomposició sobre $\mathbb{Q}[X]$, però el polinomi $X^2 + aX + b$ no té arrels reals i, per tant, no és possible fer cap altra descomposició a $\mathbb{R}[X]$. En resulta, doncs, la irreductibilitat de $P(X)$ en $\mathbb{Q}[X]$.[40] □

Hi ha una funció parcial del compàs que consisteix a portar segments.

3.16 DEFINICIÓ *L'operació* portar segments *és la següent. Donada una recta ℓ, un punt $P \in \ell$ i dos punts Q_1, Q_2,* podem determinar *dos punts P_1, P_2 de ℓ els segments $\overline{P_1P}$ i $\overline{PP_2}$ dels quals tinguin la mateixa longitud que el segment $\overline{Q_1Q_2}$.*[41]

40 Hom pot preguntar-se: no és possible que $X^4 - X - 1 = (X - a)(X^3 + bX^2 + cX + d)$? És un exercici demostrar que, per determinar a, cal resoldre precisament l'equació inicial $a^4 - a - 1 = 0$.
41 Aquesta operació la trobem ja a [5, proposició 2]. Vegeu [19, I, 704].

Com hem vist a la proposició 2.19, aquesta operació és més feble que l'operació usual del compàs —que consisteix a generar punts tot tallant rectes i circumferències amb circumferències. De fet, per tancar un cos de nombres reals amb l'operació de portar distàncies només calen les extensions pitagòriques.[42]

4 Els plecs simples

Ara preparem el terreny per introduir els *plecs simples* que, més endavant, donaran lloc als *plecs genèrics*:

4.1 DEFINICIÓ *Donada una recta ℓ, la* reflexió ρ_ℓ *del pla, relativa a la recta ℓ (figura 4), és l'aplicació de $\mathbb{R}^2$ en $\mathbb{R}^2$ que transforma cada punt Q de $\mathbb{R}^2$ d'acord amb l'expressió*

$$\rho_\ell(Q) = Q^\ell = \begin{cases} Q, & \text{quan } Q \in \ell, \\ Q', & \text{quan } Q \notin \ell \text{ i } \ell \text{ és la mediatriu del segment } \overline{QQ'}. \end{cases}$$

La imatge del punt Q produïda per la reflexió, relativa a la recta ℓ, la designarem $\rho_\ell(Q)$, o Q^ℓ. Si ℓ' és una altra recta, aleshores

$$\rho_\ell\langle\ell'\rangle = \ell'^\ell = \{\rho_\ell(Q) : Q \in \ell'\}.$$

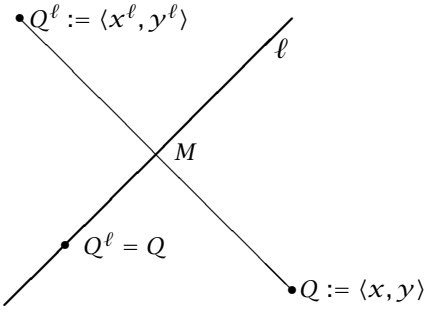


FIGURA 4

4.2 LEMA *$Q^\ell = P$ si, i només si, $P^\ell = Q$.*

DEMOSTRACIÓ És una conseqüència immediata de la definició. □

4.3 PROPOSICIÓ *En el pla cartesià, la imatge del punt $Q := \langle x, y \rangle$ per la reflexió ρ_ℓ, relativa a la recta ℓ d'equació $aX + bY + c = 0$, és el punt $Q^\ell := \langle x^\ell, y^\ell \rangle$, on*

$$x^\ell = x - \frac{2a(ax + by + c)}{a^2 + b^2},$$

42 Podríem refer tota aquesta secció i veure que, amb aquesta operació, el cos de nombres reals que s'obté és $\mathbb{P}$. El lector interessat pot consultar, per exemple, [2, 156–163] o bé [12, 83–96] .

$$y^\ell \quad = \quad y - \frac{2b(ax+by+c)}{a^2+b^2}.$$

DEMOSTRACIÓ Distingim els dos casos possibles: i) $Q \in \ell$, ii) $Q \notin \ell$.

i) Si $Q \in \ell$, aleshores $ax+by+c=0$. Per tant, $x^\ell = x, y^\ell = y$, i $Q^\ell = Q$.

ii) Si $Q \notin \ell$, aleshores ℓ és la mediatriu del segment $\overline{QQ^\ell}$.

a) El punt mitjà M (figura 4) del segment $\overline{QQ^\ell}$ té coordenades $\langle \frac{x+x^\ell}{2}, \frac{y+y^\ell}{2} \rangle$.

b) La recta $\overleftrightarrow{QQ^\ell}$ té pendent $m = \frac{y^\ell - y}{x^\ell - x}$.

c) El pendent de la recta ℓ és $m_\ell = -\frac{x^\ell - x}{y^\ell - y}$. Per tant, $\frac{a}{b} = \frac{x^\ell - x}{y^\ell - y}$.

d) El punt M pertany a ℓ. Per tant, $a\frac{x+x^\ell}{2} + b\frac{y+y^\ell}{2} + c = 0$.

e) Finalment, de *c)* i *d)* tenim

$$\begin{aligned} bx^\ell - ay^\ell &= bx - ay, \\ ax^\ell + by^\ell &= -2c - ax - by. \end{aligned}$$

Resolent aquest sistema, obtenim les expressions que cercàvem:

$$\begin{aligned} x^\ell &= x - \frac{2a(ax+by+c)}{a^2+b^2}, \\ y^\ell &= y - \frac{2b(ax+by+c)}{a^2+b^2}. \end{aligned}$$

Això acaba la demostració. □

4.4 COROL·LARI *Si ℓ és una recta de K i $x, y \in K$, aleshores $x^\ell, y^\ell \in K$.* □

Ara ja podem introduir els *plecs simples*.

4.5 DEFINICIÓ *Donats un punt Q i una recta ℓ, un* plec simple $\mathfrak{p}(Q,\ell)$ *és una recta ℓ' que genera una reflexió $\rho_{\ell'}$ que transporta el punt Q damunt de la recta ℓ.*

Si els coeficients de l'equació que defineix $\mathfrak{p}(Q,\ell)$ són de K, on Q i ℓ són de K, aleshores $\mathfrak{p}(Q,\ell)$ és un plec de K.

En general, quan no hi hagi perill de confusió, per indicar un plec escriurem simplement $\mathfrak{p}$. A més, solament usarem la notació $\mathfrak{p}$ quan es tracti d'un plec rellevant. Altrament el considerarem una recta i l'indicarem simplement ℓ. Finalment, en les figures, els plecs rellevants els indicarem amb línies de puntets.

4.6 COROL·LARI *Si tallem dos plecs simples $\mathfrak{p}_1, \mathfrak{p}_2$ de K concurrents, les coordenades del punt de tall pertanyen a K.* □

Fem una anàlisi de la naturalesa dels plecs simples que porten un punt Q damunt d'una recta ℓ.

4.7 PROPOSICIÓ *Siguin Q un punt, ℓ una recta, i $\mathfrak{p} = \mathfrak{p}(Q, \ell)$ un plec simple que porti el punt Q damunt de la recta ℓ. Aleshores tenim les possibilitats següents:*

i) Si $Q \in \ell$, aleshores $Q^{\mathfrak{p}} = Q$ si, i només si, $Q \in \mathfrak{p}$.

ii) Si $Q \in \ell$, aleshores $Q^{\mathfrak{p}} \neq Q$ si, i només si, $\mathfrak{p}$ és la mediatriu del segment $\overline{QQ^{\mathfrak{p}}}$; si, i només si, $\mathfrak{p} \perp \ell$ però no conté Q.

iii) Si $Q \notin \ell$, aleshores $Q^{\mathfrak{p}} \in \ell$ si, i només si, $\mathfrak{p}$ és tangent a la paràbola de focus Q i directriu ℓ.

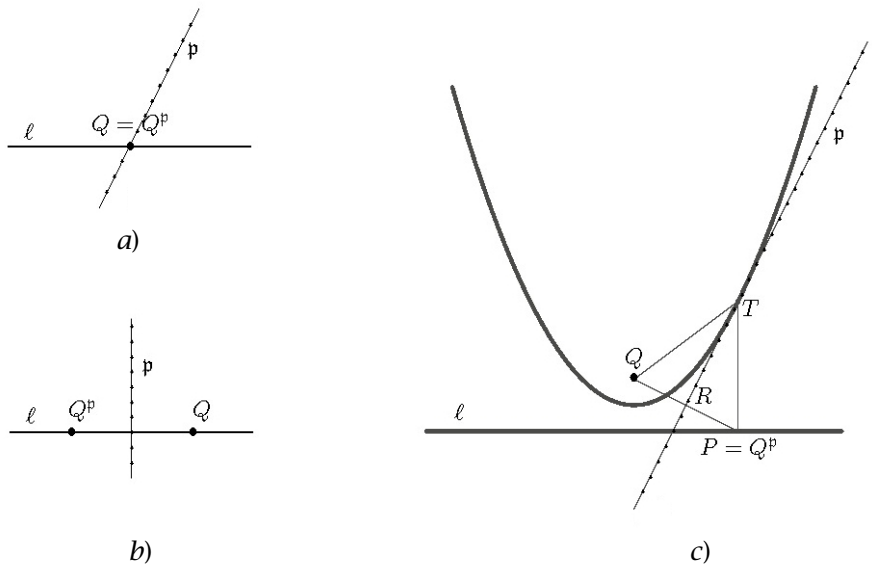


FIGURA 5

DEMOSTRACIÓ i) És evident que qualsevol recta que passi per Q és un plec. Recíprocament, tot plec ha de passar per Q (figura 5a).

ii) Si $Q \in \ell$, una recta ℓ' és un plec $\mathfrak{p}$ que porta Q damunt de la recta ℓ si, i només si, és la mediatriu del segment $\overline{QQ^{\ell'}}$. Per tant, tota perpendicular ℓ' a la recta ℓ que no passi per Q és un plec $\mathfrak{p}$, i tot plec $\mathfrak{p}$ és una recta ℓ' perpendicular a ℓ que no passa per P (figura 5b).

iii) Hem de veure les dues implicacions:

$\Rightarrow$) Suposem que $\mathfrak{p}$ és una tangent a la paràbola de focus Q i directriu ℓ, i sigui T el punt de tangència (figura 5c). Fem la perpendicular a ℓ des de T.

Talla ℓ en P. Aleshores $\overline{TQ} = \overline{TP}$ i, atès que $\mathfrak{p}$ és tangent a la paràbola de focus Q i directriu ℓ, és la bisectriu de l'angle $\angle QTP$. Unim P i Q. La recta $\overleftrightarrow{PQ}$ talla la tangent $\mathfrak{p}$ en el punt R. És clar que els triangles $\triangle PTR, \triangle QTR$ són iguals, perquè tenen dos costats, i l'angle que formen, iguals. Per tant, $\overline{PR} = \overline{RQ}$, i $\angle PRT = \angle QRT = \frac{\pi}{2}$. En conseqüència, la recta $\mathfrak{p}$ és la mediatriu del segment $\overline{PQ}$ i, de retruc, $P = Q^{\mathfrak{p}}$.

$\Leftarrow$) Suposem ara que $\mathfrak{p}$ és un plec que porta el punt Q damunt la recta ℓ (figura 5c). Aleshores $\mathfrak{p}$ és la mediatriu del segment $\overline{QQ^{\mathfrak{p}}}$. La perpendicular des de $Q^{\mathfrak{p}}$ a ℓ talla $\mathfrak{p}$ en el punt T. Aleshores $\overline{QT} = \overline{TQ^{\mathfrak{p}}}$ perquè els triangles rectangles $\triangle QRT, \triangle Q^{\mathfrak{p}}RT$ són iguals, atès que tenen els dos catets iguals. Això fa que T sigui un punt de la paràbola de focus Q i directriu ℓ.

Veure que és tangent a la paràbola és una conseqüència immediata del fet que $\mathfrak{p}$ passa per un punt T de la paràbola i determina amb les rectes $\overleftrightarrow{QT}, \overleftrightarrow{TQ^{\mathfrak{p}}}$ angles iguals. □

A la demostració hem usat el lema següent, ben conegut de tothom:

4.8 LEMA *Una recta que passi per un punt T de la paràbola i divideixi l'angle format pel radi vector $\overleftrightarrow{QT}$ i per la recta $\overleftrightarrow{Q^{\mathfrak{p}}T}$ per la meitat caracteritza la tangent a la paràbola.* □

Tanmateix, si el lector vol una demostració *ad hoc*, pot suposar que la recta $\mathfrak{p}$ talla la paràbola en un punt $R \neq T$ (figura 6). Aleshores $\overline{RP'} = \overline{RQ}$, on P' és el punt en què la perpendicular des de R a la recta ℓ talla ℓ, perquè R pertany a la paràbola. Ara bé, $\mathfrak{p}$ és la mediatriu del segment $\overline{QQ^{\mathfrak{p}}}$. Per tant, $\overline{RQ} = \overline{RQ^{\mathfrak{p}}}$. Resulta, doncs, que $\overline{RQ^{\mathfrak{p}}} = \overline{RP'}$ i el triangle $\triangle P'RQ^{\mathfrak{p}}$ fóra un triangle isòsceles amb un angle recte a la base. Impossible!

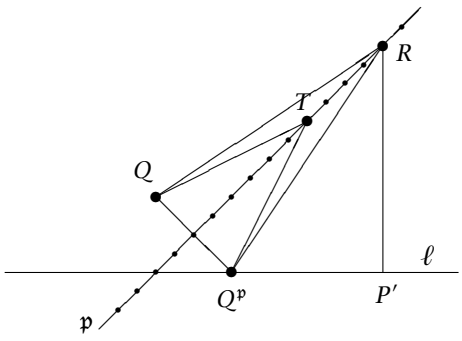


FIGURA 6

5 El regle sol

No farem pas un estudi exhaustiu del que hom pot aconseguir amb regle sol. Tanmateix, podem dir que, amb regle sol, l'única cosa que s'aconsegueix és el cos $\mathbb{Q}$.[43]

Nosaltres només demostrarem que, amb regle sol, si disposem d'un quadrat, és possible fer una paral·lela a una recta donada ℓ des d'un punt $P \notin \ell$. Això permet establir, usant el teorema de Tales, l'estructura de cos dels nombres construïbles amb regle sol. De retruc, sempre que disposem d'una operació que simuli el regle —la possibilitat de fer una recta per dos punts donats—, els nombres construïbles es podran sumar, restar, multiplicar i dividir i, per tant, tindrem un cos.

5.1 DEFINICIÓ *En el pla $\mathbb{R}^2$ un punt Q és un* punt construïble amb regle sol *a partir del quadrat unitat $\mathcal{Q}$ si, i només si, existeix una successió finita de punts*

$$Q_1, Q_2, \ldots, Q_{n-1}, Q_n,$$

que compleixen:

i) El punt Q_n és el punt Q.

ii) Per a cada índex $i, 1 \leq i \leq n$, tenim una de les situacions següents:

a) Q_i és un punt del conjunt $\mathcal{Q} * \{\langle 1,0\rangle, \langle 0,1\rangle, \langle 2,0\rangle, \langle 0,2\rangle\}$.

b) Q_i és la intersecció de dues $\mathcal{B}_{i-1}$-rectes, amb $i > 1$,

on una $\mathcal{B}_{i-1}$-recta és una recta del pla $\mathbb{R}^2$ que passa per dos punts del conjunt $\mathcal{B}_{i-1}$, sent $\mathcal{B}_{i-1} = \{Q_1, \ldots, Q_{i-1}\}$.

5.2 DEFINICIÓ *Una recta ℓ és una* recta construïble amb regle sol *si, i només si, passa per dos punts del pla $\mathbb{R}^2$ construïbles amb regle sol.*

Un nombre real $a \in \mathbb{R}$ és construïble amb regle sol *si, i només si, el punt $P_a := \langle a, 0\rangle$ és un punt construïble amb regle sol.*

5.3 LEMA *Si disposem del quadrat unitat $\mathcal{Q}$, donades dues rectes paral·leles ℓ' i ℓ'' i un punt Q, és possible fer la recta ℓ, que passa per Q, i és paral·lela a les dues rectes donades.*

DEMOSTRACIÓ (figura 7)

1. Tirem una recta ℓ_1 que passi per Q i per un dels vèrtexs O, I, J, K del quadrat unitat i que talli les rectes ℓ' i ℓ''. Obtindrem dos punts: P_1' i P_1''.

2. Fem una recta com l'anterior, però diferent, ℓ_2. Tallarà les rectes ℓ' i ℓ'' en dos punts P_2' i P_2''.

3. Considerem ara les rectes ℓ_1', ℓ_2' que passen, respectivament, pels punts P_1', P_2'' i P_2', P_1''. Es tallen en el punt P.[44]

43 El lector interessat pot consultar [2, 119–139].

44 El cas particular de paral·lelisme es pot arranjar perquè disposem d'un quadrat i del punt mitjà del quadrat.

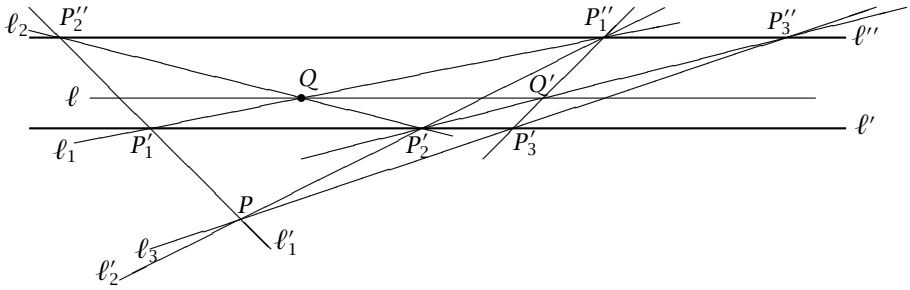


FIGURA 7

4. Ara unim el punt P amb un dels vèrtex del quadrat unitat $\mathcal{Q}$ de manera que s'obtingui una recta que talli les paral·leles ℓ', ℓ''. Obtindrem els punts P_3', P_3''.

5. Les rectes $\overleftrightarrow{P_1''P_3'}$ i $\overleftrightarrow{P_2'P_3''}$ es tallen en un punt Q'.

6. La recta ℓ que passa per Q i Q' és la paral·lela buscada. □

5.4 LEMA *Si disposem del quadrat unitat $\mathcal{Q}$, donada una recta ℓ i un punt $Q \notin \ell$, podem fer la recta paral·lela a ℓ que passa per Q.*

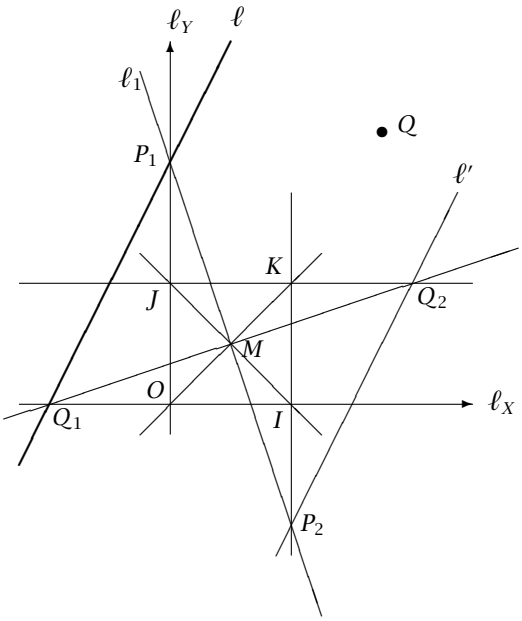


FIGURA 8

DEMOSTRACIÓ (figura 8). Podem suposar que ℓ no és paral·lela a cap dels eixos de coordenades $\ell_X := \overleftrightarrow{OI}$, $\ell_Y := \overleftrightarrow{OJ}$.[45]

Aleshores, seguim els passos següents:
1. Sigui $P_1 \in \ell \cap \ell_Y$ i $Q_1 \in \ell \cap \ell_X$.
2. Considerem el punt mitjà $M = \langle \frac{1}{2}, \frac{1}{2} \rangle$ del quadrat unitat.[46]
3. Considerem les rectes $\ell_1 := \overleftrightarrow{P_1M}$ i $\ell_2 := \overleftrightarrow{Q_1M}$.
4. La recta ℓ_1 talla, respectivament, les rectes $X = 1$ i $Y = 1$ en els punts P_2 i Q_2.
5. La recta $\ell' := \overleftrightarrow{P_2Q_2}$ és paral·lela a la recta donada ℓ perquè l'homotècia de centre M transforma I en J, $X = 0$ en $X = 1$, $Y = 0$ en $Y = 1$, P_1 en P_2, i Q_1 en Q_2. Per tant, la recta ℓ es transforma en la recta ℓ'. De tot això resulta que ℓ i ℓ' són paral·leles.
6. Apliquem ara el lema 5.3 a les paral·leles ℓ, ℓ' i al punt Q. Això acaba la demostració. □

Ara només cal veure que, si sabem fer rectes paral·leles a rectes donades que passin per punts donats, podem sumar, restar, multiplicar i dividir quantitats reals. Òbviament, la paral·lela pel punt P_a a la recta $\overleftrightarrow{IJ}$ talla l'eix ℓ_Y en el punt Q_a. La paral·lela per Q_a a la recta $\overleftrightarrow{OK}$ talla l'eix ℓ_X en el punt P_{-a} (figura 9a).

També és clar que, donats els punts P_a i P_b, podem trobar el punt $P := \langle a, b \rangle$, i recíprocament.

Les figures 9b) i 9c) mostren la manera d'efectuar les operacions de sumar, restar, multiplicar i dividir.

5.5 COROL·LARI *Si disposem del quadrat unitat $\mathcal{Q}$, els nombres construïbles amb regle sol formen un cos.* □

5.6 PROPOSICIÓ *Si disposem del quadrat unitat $\mathcal{Q}$, dos punts P_1, P_2 de K determinen una recta ℓ de K.*

Cada recta ℓ de K conté, almenys, dos punts P_1, P_2 de K.

DEMOSTRACIÓ A la proposició 2.13 vèiem una implicació.

Ara hem de veure que, si ℓ és una recta de K i disposem del quadrat unitat $\mathcal{Q}$, aleshores ℓ necessàriament talla dues rectes paral·leles: $Y = 0, Y = 1$, o bé $X = 0, X = 1$. Per tant, té dos punts de K, segons la proposició 2.14. □

És obvi que tots aquests resultats els podem aplicar quan disposem de regle i compàs.

6 La papiroflèxia genèrica

Ara introduïm què entendrem per fer una construcció amb papiroflèxia genèrica, i en les seccions següents especificarem aquesta generalitat per tal

45 Si ho fos, aplicaríem el lema 5.3.

46 Si $M \in \ell$, considerem, per exemple, el punt $\langle 1, \frac{1}{2} \rangle$ i les rectes $Y = 0, Y = 1, X = 0, X = 2$.

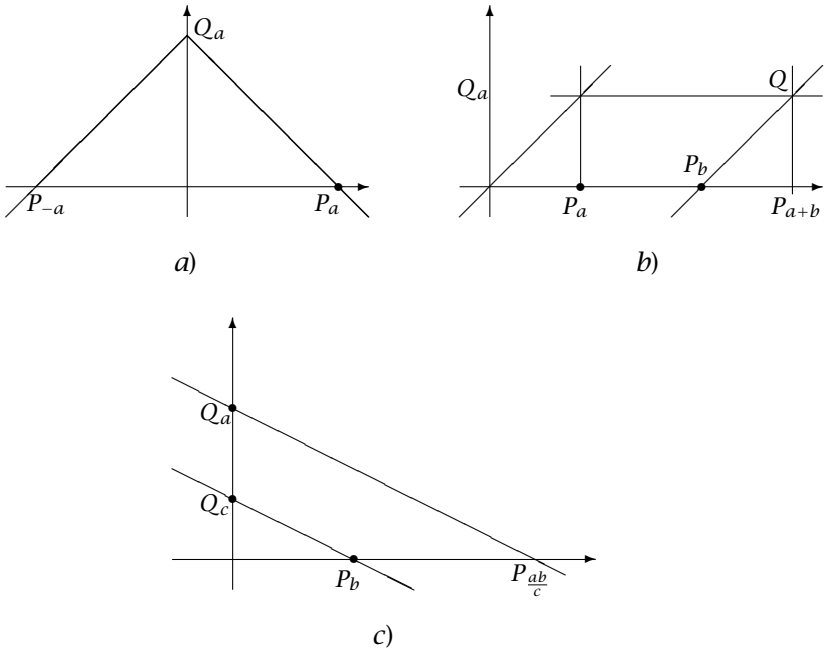


FIGURA 9

d'aconseguir les papiroflèxies pitagòrica, euclidiana i parabòlica.

Abans d'establir la papiroflèxia genèrica, necessitem definir amb rigor les dues operacions permeses en la construcció papiroflèxica.

6.1 DEFINICIÓ *Les operacions bàsiques de la papiroflèxia genèrica són:*

$\mathbf{O}_1$) *Donats dos punts diferents del pla P i Q, l'*operació de plegament lineal *genera, com a plec resultant $\mathfrak{p}$, la recta $\mathfrak{p} := \overleftrightarrow{PQ}$ que passa pels punts P i Q.*

Formalment, si P i Q són dos punts del pla $P \neq Q$, aleshores $\mathbf{O}_1(P,Q) = \mathfrak{p} := \overleftrightarrow{PQ}$.

Els plecs generats per l'operació de plegament lineal $\boldsymbol{O}_1$ s'anomenen plecs bàsics lineals.

$\mathbf{O}_2$) *Donats dos punts del pla P i Q, i dues rectes ℓ i ℓ', l'*operació de plegament genèric *genera, com a plec resultant, qualsevol recta $\mathfrak{p} := \mathfrak{p}(P,Q;\ell,\ell')$ tal que $P^{\mathfrak{p}} \in \ell$ i $Q^{\mathfrak{p}} \in \ell'$, sempre que només n'hi hagi un nombre finit.*[47]

47 Quan vulguem, posar de manifest les rectes ℓ i ℓ', i el punts P i Q, ho especificarem en la forma $\mathfrak{p}(P,Q:\ell,\ell')$, però, en general, ho ometrem.

És clar que quan $\mathfrak{p}$ s'obté aplicant l'operació $\mathbf{O}_2$, el plec $\mathfrak{p}$ és un plec simple, però, d'alguna manera, doblement simple.

Cada un dels plecs generats per l'operació de plegament genèric $\boldsymbol{O}_2$ s'anomena plec bàsic genèric.

Formalment, si P i Q són dos punts del pla, i ℓ i ℓ', dues rectes, aleshores $\mathbf{O}_2(P,Q,\ell,\ell') = \mathfrak{p} := \mathfrak{p}(P,Q;\ell,\ell')$ sempre que $P^{\mathfrak{p}} \in \ell$ i $Q^{\mathfrak{p}} \in \ell'$, i n'hi hagi solament un nombre finit.[48]

De fet, encara que hem distingit formalment entre l'acció —fer un plegament— i el resultat —aconseguir un plec—, en moltes ocasions usarem ambdós termes de manera indistinta perquè no comporten cap mena de confusió.

És clar que el plegament lineal —l'operació $\mathbf{O}_1$— fa el paper de regle.

En especificar l'operació plegament genèric, obtenim els plecs específics de cada tipus. I veurem que, quan l'operació plegament genèric —l'operació $\mathbf{O}_2$— és prou potent, permet deduir l'operació plegament lineal $\mathbf{O}_1$ com a operació subsidiària. Això succeix en els casos euclidià i parabòlic.

També veurem que, en tots els casos, disposem del quadrilàter unitat $\mathcal{Q}$ i dels punts $\langle 2,0\rangle, \langle 0,2\rangle$, i, en conseqüència, dels resultats establerts amb anterioritat. Per tant, en qualsevol papiroflèxia, disposem dels resultats de la secció 5.

6.2 DEFINICIÓ *En el pla $\mathbb{R}^2$ una recta $\mathfrak{p}$ és un* plec genèric, *a partir de la base de rectes $\mathcal{B} = \{Y = 0, X = 0, X + Y = 1\}$, si, i només si, existeix una successió finita de línies rectes*

$$\ell_1, \ell_2, \ldots, \ell_{i-1}, \ell_i, \ell_{i+1}, \ldots, \ell_n,$$

que compleixen:

i) La recta ℓ_n és el plec $\mathfrak{p}$.

ii) Per a cada índex $i, 1 \leq i \leq n$, tenim una de les situacions següents:

a) La recta ℓ_i és una recta de la base $\mathcal{B}$,

b) La recta ℓ_i s'obté aplicant l'operació de plegament lineal a dos punts diferents P i Q de $\mathcal{B}_{i-1}$,

c) La recta ℓ_i s'obté aplicant l'operació de plegament genèric a dos punts P, Q de $\mathcal{B}_{i-1}$, i a dues rectes ℓ i ℓ' de $\mathcal{B}_{i-1}$,

on $\mathcal{B}_{i-1}$ designa el conjunt que conté les rectes $\ell_1, \ell_2, \ldots, \ell_{i-1}$ i tots els punts d'intersecció d'aquestes rectes.

6.3 DEFINICIÓ *Un* punt genèric *és el que s'obté tallant dos plecs genèrics no paral·lels.*

Un nombre real a és genèric *si, i només si, el punt P_a és un punt genèric.*

6.4 PROPOSICIÓ *Es compleixen:*

a) Si P i Q són dos punts genèrics del pla, diferents, i $\mathfrak{p}$ és el plec obtingut aplicant-los l'operació $\boldsymbol{O}_1$, aleshores $\mathfrak{p}$ és un plec genèric.

48 La condició «que només n'hi hagi un nombre finit» és bàsica com podem veure a la nota 49.

b) Si P i Q són dos punts genèrics del pla, i $\mathfrak{p}_1$ i $\mathfrak{p}_2$ són dos plecs genèrics, i $\mathfrak{p}$ és un plec obtingut aplicant-los l'operació $\mathbf{O}_2$, aleshores $\mathfrak{p}$ també és un plec genèric.

DEMOSTRACIÓ *a*) Considerem la successió

$$\ell^1_1,\dots,\ell^1_{n_1},\ell^2_1,\dots,\ell^2_{n_2},\ell^3_1,\dots,\ell^3_{n_3},\ell^4_1,\dots,\ell^4_{n_4},\mathfrak{p} \qquad (*)$$

en la qual cada un dels blocs $\ell^i_1,\dots,\ell^i_{n_i}$, $i=1,2,3,4$, satisfà les condicions de la definició 6.2 i, a més, $P\in\ell^1_{n_1}\cap\ell^2_{n_2}$, i $Q\in\ell^3_{n_3}\cap\ell^4_{n_4}$. Aleshores la successió (*) satisfà la definició 6.2.

b) Anàlogament, considerem la successió

$$\ell^1_1,\dots,\ell^1_{n_1},\ell^2_1,\dots,\ell^2_{n_2},\ell^3_1,\dots,\ell^3_{n_3},\ell^4_1,\dots,\ell^4_{n_4},\ell^5_1,\dots,\ell^5_{n_5},\ell^6_1,\dots,\ell^6_{n_6},\mathfrak{p} \qquad (**)$$

en la qual cada un dels blocs $\ell^i_1,\dots,\ell^i_{n_i}$, $i=1,2,3,4,5,6$, satisfà les condicions de la definició 6.2 i, a més, $P\in\ell^1_{n_1}\cap\ell^2_{n_2}$, $Q\in\ell^3_{n_3}\cap\ell^4_{n_4}$, $\mathfrak{p}_1:=\ell^5_{n_5}$, i $\mathfrak{p}_2:=\ell^6_{n_6}$. Aleshores (**) satisfà la definició 6.2. □

En les tres seccions següents especificarem el plegament genèric —és a dir, l'operació $\mathbf{O}_2$— perquè serveixi, de manera evolutiva, d'eina alternativa a les construccions geomètriques clàssiques esmentades a la introducció. Cada una de les seccions 7, 8 i 9, queda determinada, de fet, per l'especificació de l'operació simple genèrica $\mathbf{O}_2$. En una primera lectura, les especificacions poden semblar sofisticades o injustificades, però el desenvolupament ulterior les justificarà plenament.

7 La papiroflèxia pitagòrica

El plegament pitagòric s'obté quan el plegament genèric $\mathbf{O}_2$ es concreta de la manera següent:

7.1 DEFINICIÓ *El plec genèric de la definició 6.2 s'anomena* plec pitagòric *quan, en l'operació plegament genèric $\boldsymbol{O}_2$, $\ell=\ell'$, $P\in\ell$, $P^{\mathfrak{p}}=P$ i $Q^{\mathfrak{p}}\in\ell$.*

7.2 DEFINICIÓ *Aquests plecs proporcionen la* papiroflèxia pitagòrica.

Els plecs que s'obtenen els anomenarem plecs pitagòrics, *o també* rectes pitagòriques.

Un punt pitagòric *és el que s'obté tallant dos plecs pitagòrics.*

Un nombre real a l'anomenarem nombre real pitagòric *si el punt P_a s'obté tallant plecs pitagòrics.*

A la figura 10 observem que, si disposem d'una recta ℓ, i de dos punts P i Q tals que $P\in\ell$, de fet el que busquem és un plec $\mathfrak{p}$ que passi per P i, alhora, transformi el punt Q en un punt $Q^{\mathfrak{p}}$ tal que $Q^{\mathfrak{p}}\in\ell$. O, millor encara, si considerem la recta $\overleftrightarrow{PQ}$, resulta que el plec $\mathfrak{p}$ és pitagòric si, i només si, és la *bisectriu* de l'angle que formen les rectes ℓ i $\overleftrightarrow{PQ}$, amb vèrtex en el punt comú P.

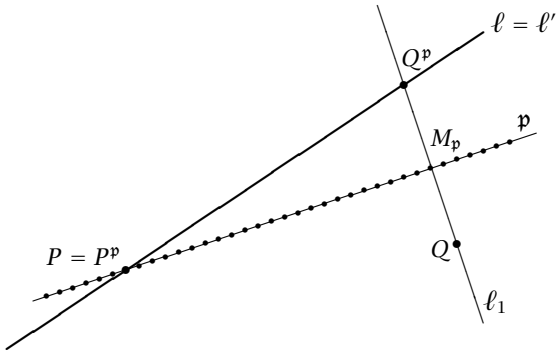


FIGURA 10

Un cas particular i curiós d'aquest tipus de plegament l'obtenim quan el punt $Q \neq P$ també pertany a la recta ℓ.[49] Aleshores resulta que el plec $\mathfrak{p}$ és la recta perpendicular a ℓ que passa per P (figura 11).

Atès que disposem de les rectes ℓ_X, ℓ_Y i dels punts $\langle 0,0\rangle$, $\langle 1,0\rangle$, $\langle 0,1\rangle$, d'aquest resultat es dedueix que podem construir el quadrilàter unitat $\mathcal{Q}$, i també els punts $\langle 2,0\rangle$, $\langle 0,2\rangle$.

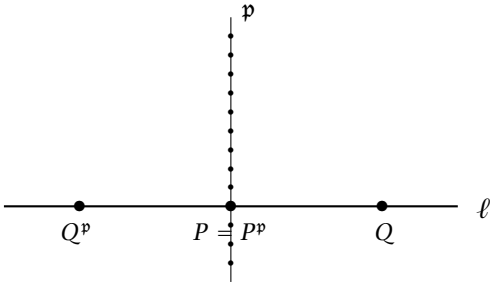


FIGURA 11

7.3 PROPOSICIÓ *Dos punts pitagòrics determinen una recta pitagòrica.*
Tota recta pitagòrica conté, almenys, dos punts pitagòrics.
Dos plecs pitagòrics, no paral·lels, determinen un punt pitagòric.

DEMOSTRACIÓ El punt primer és conseqüència de l'existència de l'operació de plegament $\mathbf{O}_1$.

El punt segon és degut al fet que disposem del quadrilàter unitat $\mathcal{Q}$ i tot plec ha de tallar, almenys, dos dels costats del quadrilàter.

En virtut de la definició 7.2 tenim el punt tercer. □

49 Si $Q = P$ i $P \in \ell$, aleshores *totes* les rectes $\mathfrak{p}$ del pla que passen per P compleixen: $P^{\mathfrak{p}} \in \ell$ i $Q^{\mathfrak{p}} \in \ell'$. N'hi ha, doncs, *infinites* i el cas queda exclòs d'acord amb l'acotació que hem imposat a l'operació bàsica $\mathbf{O}_2$ en la definició 6.1.

7.4 PROPOSICIÓ *Donats una recta ℓ i un punt P, exterior a ℓ, i ambdós pitagòrics, la recta ℓ', paral·lela a ℓ que passa per P, és un plec pitagòric.*

DEMOSTRACIÓ Atès que disposem de regle —el plegament lineal $\mathbf{O}_1$— i del quadrilàter unitat $\mathcal{Q}$, apliquem el lema 5.4. □

7.5 COROL·LARI *Els nombres reals construïbles amb papiroflèxia pitagòrica formen un subcòs K del cos $\mathbb{R}$ dels nombres reals.* □

7.6 COROL·LARI *Donats una recta ℓ i un punt P, exterior a ℓ, i ambdós pitagòrics, la perpendicular ℓ' a ℓ, que passa per P, és un plec pitagòric.*

DEMOSTRACIÓ D'antuvi fem la paral·lela ℓ' a ℓ que passa per P. Aquesta recta conté, almenys, un punt pitagòric Q, diferent de P. Podem repetir la construcció de la figura 11, que dóna l'esmentada recta perpendicular. □

7.7 COROL·LARI *Un punt $P := \langle a, b\rangle$ del pla cartesià és pitagòric si, i només si, cada un dels nombres reals a i b és un nombre pitagòric.* □

Una qüestió d'interès és la següent. Hem establert els plegaments pitagòrics com les rectes del pla que porten un punt Q damunt d'una recta ℓ i alhora passen per un punt donat P. Ara podem preguntar-nos si, en el cas que Q sigui un punt pitagòric, el punt transformat $Q^{\mathfrak{p}}$ també ho és. La resposta és afirmativa, perquè podem fer perpendiculars.

7.8 PROPOSICIÓ *Si P i Q són dos punts pitagòrics, ℓ és una recta pitagòrica, $P \in \ell$, i $\mathfrak{p} := \mathfrak{p}(P, Q; \ell, \ell)$ és un plegament pitagòric, aleshores $Q^{\mathfrak{p}}$ i $M_{\mathfrak{p}}$, on $M_{\mathfrak{p}}$ és el punt mitjà del segment $\overline{QQ^{\mathfrak{p}}}$, són punts pitagòrics.*

DEMOSTRACIÓ És un exercici elemental. Des del punt Q fem una perpendicular ℓ_1 a $\mathfrak{p}$. La perpendicular ℓ_1 talla el plec $\mathfrak{p}$ en el punt $M_{\mathfrak{p}}$ i la recta pitagòrica ℓ en el punt $Q^{\mathfrak{p}}$ (figura 10). Per tant, ambdós són punts pitagòrics. □

Ara volem establir quina és l'àlgebra de la papiroflèxia pitagòrica. És a dir, volem caracteritzar el subcòs K de $\mathbb{R}$ format pels nombres reals pitagòrics. I, tal com avançàvem després de la proposició 2.15, com que fem bisectrius d'angles formats per rectes concurrents donades, sembla raonable esperar que obtindrem el cos $\mathbb{P}$.

Per veure-ho, seguirem el mateix camí que hem seguit en la secció 3 i ens basarem en resultats de les seccions 2 i 4.

7.9 PROPOSICIÓ *Si a i b són dos nombres reals pitagòrics, aleshores $\sqrt{a^2 + b^2}$ també ho és.*

DEMOSTRACIÓ (figura 12). Suposem que a, b són no nuls. Considerem els punts P_a i Q_b. Fem la paral·lela ℓ_1 a ℓ_X que passa per Q_b i la paral·lela ℓ_2 a ℓ_Y que passa per P_a. Es tallen en el punt $P := \langle a, b\rangle$. Ara fem un plegament pitagòric $\mathfrak{p}$, aplicat als punts O, P, i a la recta ℓ_X. Obtenim el punt $P^{\mathfrak{p}}$ que, òbviament, és el punt $P_{\sqrt{a^2+b^2}}$, perquè $\overline{OP} = \sqrt{a^2 + b^2}$ i els triangles rectangles $\triangle OPM, \triangle OMP^{\mathfrak{p}}$ són iguals. □

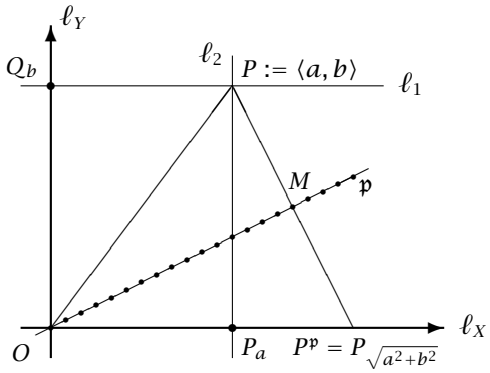


FIGURA 12

Podíem haver donat una demostració alternativa més algebraica.[50]

7.10 COROL·LARI *Si K_Π designa el cos dels nombres reals pitagòrics, aleshores $\mathbb{P} \subseteq K_\Pi$.* □

7.11 DEFINICIÓ *Una* extensió pitagòrica iterada

$$K_n = K\left(\sqrt{\Pi_1}, \sqrt{\Pi_2}, \ldots, \sqrt{\Pi_{n-1}}\right)$$

d'un cos K és el terme final de la cadena d'extensions pitagòriques

$$K_0 = K \subseteq K_1 \subseteq K_2 \subseteq \cdots \subseteq K_{n-1} \subseteq K_n,$$

on cada $K_i = K_{i-1}(\sqrt{\Pi_i}), \Pi_i = a_{i-1}^2 + b_{i-1}^2$, amb $a_{i-1}, b_{i-1} \in K_{i-1}, i = 1, \ldots, n$.

7.12 PROPOSICIÓ *Donat un cos K, dos punts P, Q i una recta ℓ, tots tres de K, aleshores*

a) el plec que s'obté amb l'operació $\boldsymbol{O}_1$ és una recta de K;
b) el plec que s'obté amb l'operació de plegament pitagòric és una recta d'una certa extensió pitagòrica de K.

DEMOSTRACIÓ És una conseqüència immediata de les proposicions 2.9 i 2.13.□

7.13 COROL·LARI *Tot nombre real pitagòric és en una extensió pitagòrica iterada de $\mathbb{Q}$.*

DEMOSTRACIÓ És una conseqüència immediata de la proposició 2.14. □

50 Considerem la paràbola de focus $\langle a, b\rangle$ i directriu $Y = 0$. La seva equació és $x^2 - 2ax + a^2 + b^2 = 2by$. Considerem la tangent que passa pel punt $\langle 0, 0\rangle$. Té l'equació $y = \frac{\sqrt{a^2+b^2}-a}{b}x$. Tallem aquesta recta amb la recta $X = 1$ i obtenim el punt pitagòric $\left\langle 1, \frac{\sqrt{a^2+b^2}-a}{b}\right\rangle$. Per tant, $\sqrt{a^2+b^2} \in \mathbb{P}$.

7.14 PROPOSICIÓ *El cos $\mathbb{P}$ és la reunió de totes les extensions pitagòriques iterades de $\mathbb{Q}$.*

DEMOSTRACIÓ Òbviament, d'una banda $\mathbb{Q} \subseteq \mathbb{P}$ i, d'una altra, $\mathbb{P}$ és tancat per $\sqrt{a^2+b^2}$, quan $a, b \in \mathbb{P}$. □

7.15 TEOREMA *El cos K_Π dels nombres reals pitagòrics és $\mathbb{P}$.*

DEMOSTRACIÓ Un corol·lari immediat dels resultats anteriors. □

7.16 COROL·LARI *El cos $\mathbb{P}$ és el més petit subcòs de $\mathbb{R}$ que, per a tota equació de segon grau $aX^2+bX+c=0$, amb $a,b,c \in \mathbb{P}$, i discriminant Δ de la forma $\Delta = \xi_1^2+\xi_2^2$, amb $\xi_1, \xi_2 \in \mathbb{P}$, conté les seves arrels reals.* □

Sabem que $\mathbb{P} \subseteq \mathbb{E}$, perquè $\mathbb{E}$ és tancat per arrels quadrades. És la justificació algèbrica. O bé perquè, amb regle i compàs, podem fer les operacions de plegament lineal i de plegament pitagòric.[51] Seria la justificació geomètrica.

La qüestió és saber si coincideixen o no.

7.17 PROPOSICIÓ $\mathbb{P} \subsetneq \mathbb{E}$.

Per veure-ho, usarem el lema següent:

7.18 LEMA *Si $\alpha \in \mathbb{P}$ i $P(X) \in \mathbb{Q}[X]$ és un polinomi minimal de α, aleshores totes les arrels de $P(X)$ pertanyen a $\mathbb{P}$.*

DEMOSTRACIÓ Sigui β una altra arrel de $P(X)$, $\beta \neq \alpha$. Considerem l'isomorfisme

$$\sigma : \mathbb{Q}(\alpha) \to \mathbb{Q}(\beta)$$

que deixa fix $\mathbb{Q}$ i transforma α en β.

Considerem l'extensió $\sigma : \mathbb{Q}(\alpha) \hookrightarrow \mathbb{C}$ i la perllongació $\overline{\sigma} : \mathbb{P} \hookrightarrow \mathbb{C}$. Sigui ara

$$\overline{\sigma}^{-1}\langle \mathbb{P} \rangle = \{\xi \in \mathbb{P} : \overline{\sigma}(\xi) \in \mathbb{P}\} \subseteq \mathbb{P}.$$

Afirmem que $\overline{\sigma}^{-1}\langle \mathbb{P} \rangle$ és un cos pitagòric. Que és un cos és trivial. Vegem, doncs, que és pitagòric.

Suposem que $\xi_1, \xi_2 \in \overline{\sigma}^{-1}\langle \mathbb{P} \rangle$. Aleshores, sigui $\xi = \sqrt{\xi_1^2+\xi_2^2}$. És clar que

$$\overline{\sigma}(\xi^2) = \overline{\sigma}(\xi_1^2) + \overline{\sigma}(\xi_2^2) \in \mathbb{P}.$$

Per tant,

$$\overline{\sigma}(\xi) = \pm\sqrt{\overline{\sigma}(\xi_1^2) + \overline{\sigma}(\xi_2^2)} \in \mathbb{P}$$

i, de retruc, $\xi \in \overline{\sigma}^{-1}\langle \mathbb{P} \rangle$.

51 Recordem que, amb regle i compàs, és possible fer la bisectriu d'un angle donat. Vegeu [5, proposició 9], [19, 711].

Ara bé, $\overline{\sigma}^{-1}\langle\mathbb{P}\rangle \subseteq \mathbb{P}$, $\overline{\sigma}^{-1}\langle\mathbb{P}\rangle$ és un subcòs de $\mathbb{R}$ i $\mathbb{P}$ és el més petit de tots els subcossos pitagòrics de $\mathbb{R}$. Per tant, $\overline{\sigma}^{-1}\langle\mathbb{P}\rangle = \mathbb{P}$. Això, conjuntament amb el fet que $\alpha \in \mathbb{P}$ i $\sigma(\alpha) = \overline{\sigma}(\alpha) = \beta$, permet concloure que $\beta \in \mathbb{P}$.[52] □

DEMOSTRACIÓ DE LA PROPOSICIÓ 7.17 Òbviament, el nombre $\sqrt[4]{2} \in \mathbb{E}$. Considerem el seu polinomi minimal sobre $\mathbb{Q}$, $X^4 - 2 = 0$. Les seves arrels són $\pm\sqrt[4]{2}$, $\pm i\sqrt[4]{2}$. Per tant, no totes les arrels pertanyen a $\mathbb{P}$. Aplicant el lema 7.18, $\sqrt[4]{2} \notin \mathbb{P}$. □

* * *

Ara, com a cloenda d'aquesta secció, veurem que la papiroflèxia pitagòrica és equivalent a disposar del regle i de l'operació del compàs que consisteix a portar segments rectilinis.[53]

7.19 LEMA *Amb papiroflèxia pitagòrica, donats els punts Q_1, Q_2, la recta ℓ, i el punt $P \in \ell$, si podem fer un punt $P_1 \in \ell$ que $\overline{P_1P} = \overline{Q_1Q_2}$, també podem fer un punt $P_2 \in \ell$ que $\overline{PP_2} = \overline{Q_1Q_2}$.*

DEMOSTRACIÓ Cal refer la figura 11 i el raonament de la figura 9a, aplicat al punt P, la recta ℓ, i el segment $\overline{P_1P_2}$. □

7.20 TEOREMA *Disposar del regle i de l'operació de portar segments és equivalent a la papiroflèxia pitagòrica.*

DEMOSTRACIÓ A) Amb la notació del lema 7.19, els plegaments pitagòrics permeten portar segments.

A1) Suposem que un almenys dels punts Q_1, Q_2 no pertany a ℓ (figura 13a). Per exemple, Q_2.

1. Fem la paral·lela ℓ_1 a ℓ per Q_1.
2. Fem el plec $\mathfrak{p}(Q_2, \ell_1)$, que passa per Q_1.
3. Considerem el punt $Q_2^{\mathfrak{p}} \in \ell_1$. Òbviament, $\overline{Q_1Q_2} = \overline{Q_1Q_2^{\mathfrak{p}}}$.
4. Fem la paral·lela ℓ' per $Q_2^{\mathfrak{p}}$ a la recta $\overleftrightarrow{PQ_1}$. Talla ℓ en P_1 i $\overline{PP_1} = \overline{Q_1Q_2}$.

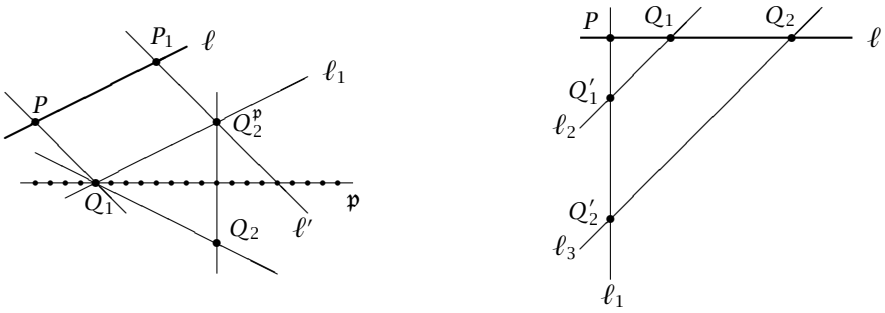
A2) Si Q_1 i Q_2 pertanyen a ℓ, procedim de la manera següent (figura 13b):

1. Fem la perpendicular ℓ_1 a ℓ per P.
2. Fem una paral·lela ℓ_2 a OK [o a OI] per Q_1. Tindrem un punt $Q_1' \in \ell_1$.
3. Fem una paral·lela ℓ_3 a OK [o a OI] per Q_2. Tindrem un punt $Q_2' \in \ell_1$. Ara som en el cas (A1).

B) El regle i l'operació de portar segments permet fer plegaments pitagòrics.

52 El lector interessat a veure una demostració que no utilitzi el llenguatge dels isomorfismes pot consultar [12, 90–92]. Tot rau a veure que, si $\sqrt{\xi^2 + \sqrt{\xi_1^2 + \xi_2^2}} \in \mathbb{P}$, aleshores $\sqrt{\xi^2 - \sqrt{\xi_1^2 + \xi_2^2}} \in \mathbb{P}$. Ara bé, $\sqrt{1 + \sqrt{5}} \in \mathbb{P}$ i $\sqrt{1 - \sqrt{5}} \notin \mathbb{P}$.

53 Vegeu [2, 156–168] i, en particular, 163–168.



a) *b*)

FIGURA 13

B1) Donats $Y = 0, X = 0, X+Y = 1$,[54] podem fer un quadrat $IJI'J'$ (figura 14a).

B2) Podem fer paral·leles perquè disposem de l'operació regle, d'un quadrat i de les seves diagonals.

B3) Ara suposem que tenim una recta ℓ i dos punts P, Q, amb $P \in \ell$ i $Q \notin \ell$.

1. Fem la paral·lela ℓ' a ℓ que passa per Q. Ara determinem el punt Q' de ℓ' que $\overline{QQ'} = \overline{PQ}$.

2. Fem la recta $\overleftrightarrow{PQ'}$. És la bisectriu buscada i, de retruc, el plec que porta el punt Q damunt de la recta ℓ (figura 14b).

B4) Ara suposem que tenim una recta ℓ i dos punts P, Q, amb $P \in \ell$ i $Q \in \ell$. Aleshores, com hem vist a la figura 11, el plec —o, si ho preferiu, la bisectriu— és la perpendicular a la recta ℓ que passa pel punt P. Hem de veure, doncs, que amb el regle i l'operació de portar segments podem fer perpendiculars a rectes donades en un punt d'aquestes.

Per P fem passar rectes paral·leles a les rectes $\overleftrightarrow{II'}, \overleftrightarrow{JJ'}$. Portem el segment $\overline{OI}$, a partir de P, damunt d'aquestes dues rectes i cap a ambdós costats. Unim els punts I^*, I'^*, J^*, J'^* que s'obtenen. S'aconsegueix el quadrat unitat de la figura 14a traslladat al punt P (figura 14c).

La recta ℓ talla un dels costats unitat en un punt R. Considerem el segment $\overline{I^*R}$ i portem-lo damunt la recta $\overleftrightarrow{J^*I'^*}$, tal com s'indica a la figura 14c. S'obté el punt R'. La recta $\overleftrightarrow{R'P}$ és perpendicular a la recta ℓ pel punt P. És el plec buscat. Passa per P i transporta el punt Q damunt la recta ℓ. □

54 Sempre cal una base inicial.

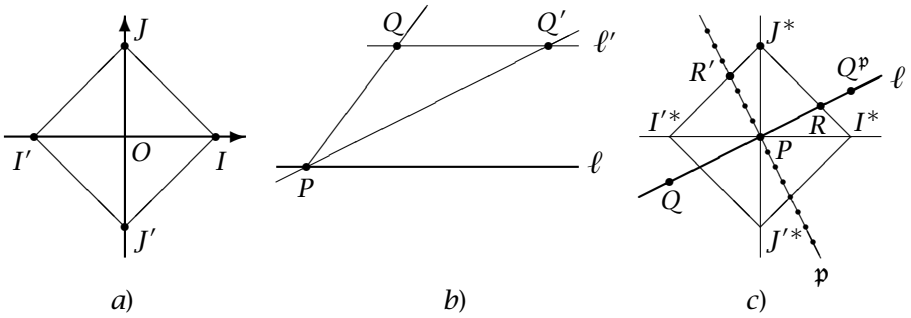


FIGURA 14

8 La papiroflèxia plana

El text de geometria amb papiroflèxia més antic és el ja clàssic *Geometric exercices in paper folding*. T. Sundara Row —l'autor— hi ofereix d'una manera una mica *informal* la geometria de l'*Elements*, i també uns altres resultats. La diferència amb el text de l'alexandrí és que Row fa la geometria de l'*Elements* usant la tècnica de la papiroflèxia.

Un cop ha mostrat la manera de construir el quadrat, el triangle equilàter, el pentàgon, l'hexàgon, l'octògon, el decàgon, el dodecàgon i el pentadecàgon, a més de les construccions aproximades de l'heptàgon i l'enneàgon, fa un bon grapat de construccions curioses usant sempre la tècnica de la papiroflèxia.[55]

Malgrat que l'autor no precisa ben bé què és un plec i com s'aconsegueix un punt papiroflèxic, la lectura atenta de les seves construccions permet copsar el significat que els dóna.

Per tal de fer entenedora la seva metodologia, repassarem la construcció del *segment auri*,[56] del pentàgon, i la construcció d'un segment de longitud $\sqrt[4]{2}$. Així quedarà ben palesa la seva tècnica i alhora quedarà clar que la seva papiroflèxia és més potent que no pas la papiroflèxia pitagòrica.

L'objectiu final d'aquesta secció és veure que la papiroflèxia de Sundara Row és equivalent a la geometria plana. Ho establirem algèbricament i geomètricament.

8.1 PROBLEMA *Donat un segment AB, determinar-ne el punt X tal que el rectangle de costats AB i XB sigui igual al quadrat de costat AX.*[57]

RESOLUCIÓ (figura 15).

1. Fem el quadrat $ABCD$ de costat AB.

55 Vegeu [16].

56 És el nombre real α que fa que $\frac{1}{\alpha} = \frac{\alpha}{1-\alpha}$; és a dir, tal que $\alpha^2 + \alpha - 1 = 0$. Per tant, $\alpha = \frac{1}{2}\sqrt{5} - \frac{1}{2} \in \mathbb{P}$, atès que $\sqrt{5} = \sqrt{2^2 + 1^2}$.

57 Formalment, $AB \times XB = AX^2$. Vegeu [16, 18, §51]. Compareu-ho amb [19, teorema 11].

2. Determinem el punt mitjà E del costat BC.
3. Fem el plec lineal $\mathfrak{p}_1$ que passa per A i E.
4. Ara fem el plec pitagòric $\mathfrak{p}$ que passa per E i porta el punt B damunt la recta ℓ_1.[58]
5. El plec $\mathfrak{p}$ talla la recta ℓ en el punt F. Marquem el punt $B^{\mathfrak{p}}$.
6. Ara fem AX igual a $AB^{\mathfrak{p}}$.
7. El punt X és el punt buscat. □

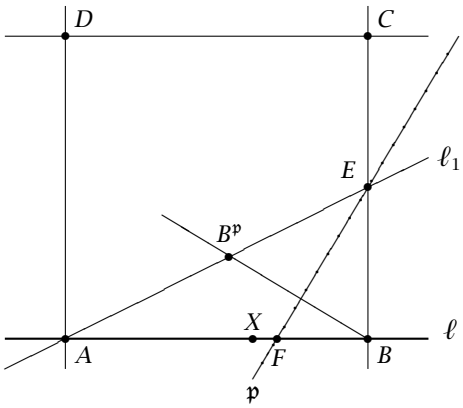


FIGURA 15

És fàcil constatar que, efectivament, AX és el *segment auri* corresponent al segment AB.[59] Òbviament, si $A = O, B = I$, aleshores $X = P_\alpha$ amb $\alpha \in \mathbb{P}$, perquè solament hem usat plegaments pitagòrics.[60]

Tot seguit fa la construcció del pentàgon regular. La construcció de Row és interessant perquè introdueix un plegament que no és pitagòric.

8.2 PROBLEMA *Donat un segment AB, determinar un triangle isòsceles $\triangle BAN$ tal que l'angle de la base valgui el doble que l'angle en el vèrtex.*[61]

RESOLUCIÓ 1. A la figura 16, damunt la recta $\ell := \overleftrightarrow{AB}$ determinem X tal com hem fet en el problema 8.1.
2. Fem el quadrat de costat AB.
3. Fem la perpendicular ℓ_1 a la recta ℓ que passa pel punt X. Talla la recta $\ell' := \overleftrightarrow{DC}$ en el punt H.

58 A la figura 15 el plec l'hem fet de punts molt petits perquè, en aquesta secció, els plecs rellevants són els plans i no pas els pitagòrics.
59 Vegeu [16, 19].
60 Si $\overline{AB} = 1$, aleshores $\overline{AX} = x$, on $x = d(A,E) - \frac{1}{2} = \frac{1}{2}\sqrt{5} - \frac{1}{2}$ és el segment auri.
61 Vegeu [16, 30–31, §71]. Compareu-ho amb [5, teorema 10 del llibre IV], a [19, 780–781].

4. Considerem el punt mitjà M del segment $\overline{XB}$.
5. Fem la perpendicular ℓ_2 a ℓ que passa pel punt M. Talla la recta ℓ' en el punt O.
6. Ara fem un plec $\mathfrak{p} := \mathfrak{p}(X, A; \ell, \ell_2)$ que passi pel punt X i porti el punt A damunt la recta ℓ_2. La perpendicular a aquest plec determina un punt N damunt el segment $\overline{OM}$.[62]
7. Òbviament $\overline{XN} = \overline{AX}$.
8. Unim els punts N i B amb una recta ℓ_3 i els punts X i N amb una recta ℓ_4.
9. El triangle $\triangle BAN$ és el triangle buscat. □

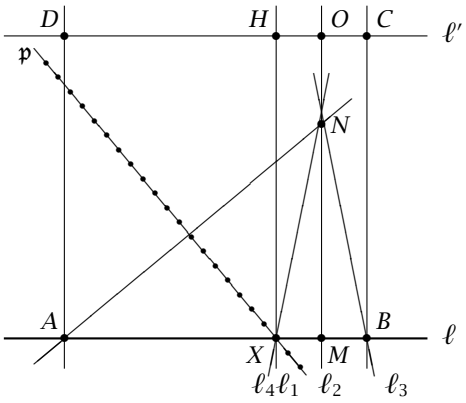


FIGURA 16

De retruc en resulta que $\angle NAB = \frac{1}{5}\pi$.[63] En aquesta construcció hem fet un plec que no s'obté amb els plegaments pitagòrics. És el plec que cal introduir com a plegament pla.

De moment l'intuïm copiant-lo de la demostració anterior, tal com s'exposa a la figura 17. De fet, el podríem anomenar *plec en el sentit de Row*, en honor a T. Sundara Row.

62 Recordem que el punt transportat per un plec és un punt papiroflèxic, segons hem vist a la proposició 7.8.

63 Vegem-ne la prova de [16, 21-23]. D'entrada $\overline{AX} = \overline{XN} = \overline{NB}$. A més, tenim la cadena següent d'implicacions:

$$\left.\begin{array}{rcl} \angle ABN & = & \angle NXB \\ \angle NAX & = & \angle XNA \end{array}\right\} \Rightarrow \angle NXB = \angle ABN = \angle NAX + \angle XNA = 2\angle NAX.$$

I també,

$$\overline{AN}^2 = \overline{MN}^2 + \overline{AM}^2 = \overline{BN}^2 - \overline{BM}^2 + \overline{AM}^2 = \overline{BN}^2 + (\overline{AM} - \overline{BM})(\overline{AM} + \overline{BM}) =$$
$$= \overline{BN}^2 + \overline{AB} \times \overline{AX} = \overline{NX}^2 + \overline{AB} \times \overline{AX} = \overline{AX}^2 + \overline{AB} \times \overline{AX} = \overline{AB} \times \overline{BX} + \overline{AB} \times \overline{AX} = \overline{AB}^2.$$

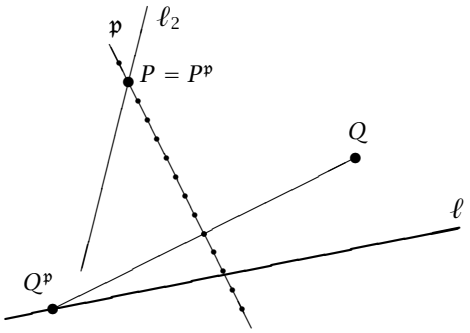


FIGURA 17

Ens proporciona la manera com hem d'especificar l'operació genèrica simple $\mathbf{O}_2$ que, a la definició 8.4, anomenarem *plegament pla*: a cada dos punts P i Q i a cada recta ℓ, li associa el plec $\mathfrak{p}$ que passa pel punt P i porta el punt Q damunt la recta ℓ. És a dir, $\mathbf{O}_2(P, Q, \ell) = \mathfrak{p}$ que $P^{\mathfrak{p}} = P$ i $Q^{\mathfrak{p}} \in \ell$.

Observem que ara no imposem pas la limitació del plegament pitagòric segons la qual el punt P ha de pertànyer a la recta ℓ. Òbviament, quan el punt $P \in \ell$, el plegament pla esdevé un plegament pitagòric. La papiroflèxia plana serà, doncs, tan potent almenys com la pitagòrica.

Ara hem d'introduir el plegament pla com una especificació del plegament genèric i després veure que el cos de punts plans és precisament el cos $\mathbb{E}$. Ho farem de dues maneres. L'una més algèbrica, i l'altra més geomètrica.

Abans, però, veurem una construcció de Row que suggereix aquest resultat.

8.3 PROBLEMA *Usant plegaments euclidians, en el sentit de Row, és possible construir un segment de longitud* $\sqrt[4]{2}$.[64]

RESOLUCIÓ 1. Sigui OI el segment unitat de l'eix ℓ_X.

2. Fem un punt T de la recta ℓ_X de manera que $\overline{OT}$ tingui quatre unitats de longitud.
3. Sigui M el punt mitjà del segment TQ, on Q és un punt de ℓ_X.
4. Sigui $\mathfrak{p}$ el plec que passa per M i porta el punt Q damunt de la recta ℓ_Y (figura 18).
5. Sigui $Q^{\mathfrak{p}}$ el punt transportat.
6. Fem la perpendicular a ℓ_X que passa per Q i la perpendicular a ℓ_Y que passa per $Q^{\mathfrak{p}}$. Es tallen en el punt P. Tot rau aleshores a calcular la longitud dels segments $\overline{QP} = \overline{OQ^{\mathfrak{p}}}$.

$$\overline{QP}^2 = (\overline{OQ^{\mathfrak{p}}})^2 = (\overline{MQ^{\mathfrak{p}}})^2 - \overline{OM}^2 = \overline{MQ}^2 - \overline{OM}^2 = \left(\frac{\alpha}{2} + 2\right)^2 - \left(\frac{\alpha}{2} - 2\right)^2 = 4\alpha,$$

on α és la distància del segment $\overline{OQ}$. És a dir, $Q = P_\alpha$.

64 Vegeu [16, 117–118, §236], dins la secció II, «La paràbola» del capítol III, dedicat a les «Les seccions còniques». Està vinculat, doncs, amb el teorema 4.7.

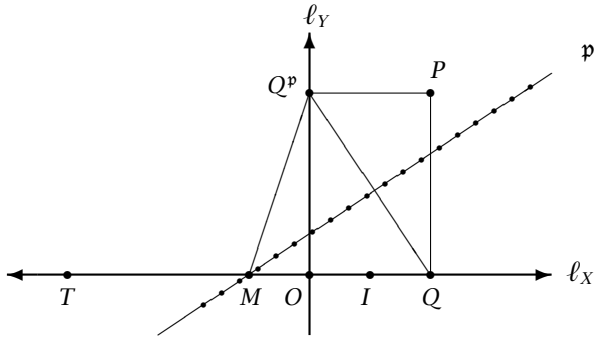


FIGURA 18

Això ens diu que el punt P pertany a la *paràbola* que, en el sistema de referència $Y = 0$, $X = 0$, $X + Y = 1$, té l'equació cartesiana $y^2 = 4x$.

Per tant, si el punt $Q := \langle \alpha, 0 \rangle$ és un punt ja construït, el punt $P = \langle \alpha, \beta \rangle$, amb $\beta^2 = 4\alpha$, queda construït amb la papiroflèxia de Row —la papiroflèxia plana.[65]

Suposem, doncs, que $\alpha = \sqrt{2}$. Aleshores $\beta = 2\sqrt[4]{2}$ i, de retruc, $\sqrt[4]{2}$ és construïble. Hem ampliat, doncs, la potència de la papiroflèxia.[66] □

Ara estem ja en situació d'establir, amb rigor, com especificar la papiroflèxia genèrica per tal d'obtenir la papiroflèxia plana.

El plegament pla s'obté quan el plegament genèric $\mathbf{O}_2$ es concreta de la manera següent:

8.4 DEFINICIÓ *El plegament genèric —l'operació $\boldsymbol{O}_2$— de la definició 6.1 esdevé un* plegament pla *o* euclidià *quan $P^{\mathfrak{p}} = P \in \ell'$ i $Q \in \mathfrak{p} \in \ell$ (figura 17).*

Aquest plegament, juntament amb el plegament lineal, proporciona la papiroflèxia plana *o* euclidiana.

Els plecs que s'obtenen aplicant qualsevol d'ambdós tipus de plegaments els anomenarem plecs plans *o* euclidians*, o també* rectes planes *o* euclidianes.

Un punt pla *o* euclidià *és el que s'obté tallant dues rectes planes.*

Un nombre real a l'anomenarem nombre real pla *o* euclidià *si el punt P_a s'obté tallant plecs plans.*

---

65 Si $\sqrt{2p}$ i α són construïbles, i $\beta^2 = 2p\alpha$, aleshores β és un nombre real construïble amb aquesta nova papiroflèxia.

66 D'aquest fet se n'adonà Robert C. Yates, el qual l'any 1949 establia, com a definició de papiroflèxia, la papiroflèxia plana. (Vegeu [24, secció IV, 54–65].) La papiroflèxia de Yates es basa en tres operacions:

Plegament lineal. Donats dos punts P, Q, hi ha un plec $\mathfrak{p}$ que passa per ells.

Plegament pla. Donada una recta ℓ i dos punts P, Q, podem fer els plecs $\mathfrak{p}$ que $P \in \mathfrak{p}$ i $Q^{\mathfrak{p}} \in \ell$, sempre que n'existeixi algun.

Plegament de superposició. Donats dos punts P, Q, podem fer el plec $\mathfrak{p}$ que porta el punt P damunt del punt Q.

Observem que, de fet, el punt $Q^{\mathfrak{p}}$ s'obté tallant la circumferència de centre P i radi $\overline{PQ}$ amb la recta ℓ.[67] Els plecs produïts pel plegament pla, quan existeixen, es poden fer amb regle i compàs. Això significa que el cos K_E dels nombres reals plans està inclòs dins del cos $\mathbb{E}$. Coincidiran sempre que puguem veure que K_E és tancat per arrels quadrades, quelcom que ja hem indicat abans.

En definitiva, doncs,

8.5 PROPOSICIÓ *Els cos dels nombres reals plans és* $\mathbb{E}$. □

No obstant això, n'oferirem una demostració geomètrica constructiva.

Abans, però, farem algunes observacions relatives a la papiroflèxia plana.

8.6 PROPOSICIÓ *Els plecs i els nombres pitagòrics són plans.*

DEMOSTRACIÓ Només cal imposar que el punt P sigui un punt de la recta ℓ.□

Com hem vist a la pàgina 109, en la papiroflèxia pitagòrica, fer la paral·lela i la perpendicular a una recta ℓ des d'un punt $P \notin \ell$ era llarg. Ara, en canvi, és força més curt i senzill.[68]

8.7 PROPOSICIÓ *Donada una recta ℓ i un punt P, podem fer la perpendicular a ℓ que passa per P.*

DEMOSTRACIÓ Si $P \in \ell$, usem la proposició anterior i la construcció de la figura 11.

Suposem, doncs, que $P \notin \ell$. Agafem un punt $Q \in \ell$, que existeix sempre perquè ℓ ha de tallar necessàriament una de les tres rectes bàsiques (figura 19). Aleshores existeix un plec $\mathfrak{p}$ que passa per P de manera que $Q^{\mathfrak{p}} \in \ell$. És la perpendicular buscada. □

8.8 COROL·LARI *Donada una recta ℓ i un punt $P \notin \ell$, podem fer la paral·lela a ℓ que passa per P.* □

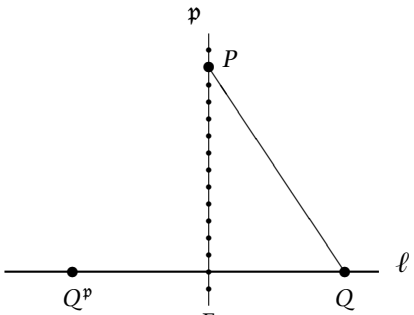


FIGURA 19

67 Òbviament aquest tall pot no existir, com ja advertia Yates. Aleshores el plec $\mathfrak{p}$ no existeix.
68 De fet, podem evitar-nos les proposicions 5.3 i 5.4.

Com hem repetit a bastament, per generar una papiroflèxia calen les dues operacions de plegament simple $\mathbf{O}_1$ i $\mathbf{O}_2$, però, en el cas en què l'operació $\mathbf{O}_2$ sigui la de la definició 8.4, el fet més important és que el plegament lineal és deduïble del plegament pla.

8.9 PROPOSICIÓ *Donats dos punts P i Q, diferents, usant el plegament pla podem fer la recta que passa per P i Q.*

DEMOSTRACIÓ Aquests punts els hem obtingut tallant plecs. Agafem doncs una recta ℓ_Q que passi per Q (figura 26). Ara considerem els plecs que passen per P i porten el punt Q damunt la recta ℓ. De fet, n'hi ha dos. La perpendicular $\mathfrak{p}'$ descrita en la proposició anterior i la recta $\mathfrak{p}$ que passa per P i per Q. □

8.10 PROPOSICIÓ *Si $a \in K_E$, aleshores $\sqrt{a} \in K_E$.*

DEMOSTRACIÓ Refem les consideracions que hem fet, a la pàgina 118, en el problema 8.3 de Row. □

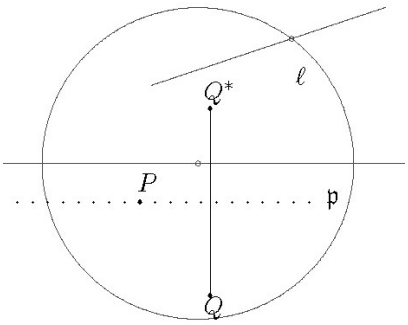


FIGURA 20

8.11 COROL·LARI *El cos dels nombres reals plans és el cos euclidià $\mathbb{E}$.* □

Per acabar aquesta secció, amb la voluntat d'oferir tots els punts de vista possibles, veurem que amb plegaments plans podem determinar els punts de tall d'una recta i d'una circumferència, i de dues circumferències.[69]

8.12 TEOREMA *Suposem que P, Q, P_1, Q_1, P_2, Q_2 són sis punts plans, i ℓ, ℓ_1 i ℓ_2 tres rectes euclidianes.*

1. *Si/ ℓ_1, ℓ_2 són no paral·leles, el punt que determinen és pla.*
2. *Si ℓ talla la circumferència $P(\overline{PQ})$, els punts de tall són plans.*

69 Aquestes construccions les trobem a [24, 63]. La segona consisteix a construir l'*eix radical*.

3. *Si les circumferències $P_1(\overline{P_1Q_1})$ i $P_2(\overline{P_2Q_2})$ es tallen, els punts de tall són punts plans.*

DEMOSTRACIÓ 1. És trivial, per definició de punt pla.

2. Sigui ℓ una recta plana, i P i Q dos punts plans que determinen la circumferència $P(\overline{PQ})$ de centre en P i radi $\overline{PQ}$ (figura 20) (que, de fet, no podem pas dibuixar perquè no disposem de cap compàs).

   Hem de determinar, en canvi, el punt Q^* en què la recta ℓ talla la circumferència inexistent $P(\overline{PQ})$.

   Tot rau a fer el plec $\mathfrak{p}$ que passa per P i porta el punt Q damunt la recta ℓ.

   Aleshores la perpendicular al plec $\mathfrak{p}$ que passa per Q talla la recta ℓ en el punt Q^*, que és el punt que buscàvem.

3. Tot rau a determinar, amb plegaments plans, l'*eix radical* de la parella de circumferències $P_1(\overline{P_1Q_1}), P_2(\overline{P_2Q_2})$ (figura 21).

   a) Tirem la recta $\ell_2 := P_2Q_2$. Per P_1, tirem la recta ℓ_1, paral·lela a ℓ_2. Portem ara el punt Q_1 damunt la recta ℓ_1. Aquest nou punt l'anomenarem també Q_1, com si fos el punt donat damunt la circumferència de centre P_1.[70]

   b) Determinem els punts Q_1', Q_2' que $\overline{P_1Q_1} = \overline{P_1Q_1'}, \overline{P_2Q_2} = \overline{P_2Q_2'}$. Ambdós punts són plans.

   c) Tirem ara les rectes $\overleftrightarrow{Q_1Q_2}$ i $\overleftrightarrow{Q_1'Q_2'}$. Es tallen en un punt E que és el *centre de semblança* de les circumferències.

   d) La recta $\overleftrightarrow{EQ_1'}$ talla la circumferència $P_2(\overline{P_2Q_2})$ en un punt Q_2', i la recta $\overleftrightarrow{EQ_2}$ talla la circumferència $P_2(\overline{P_2Q_2})$ en un segon punt Q_2^*. Aquest punt s'obté fent la perpendicular a la recta $\overleftrightarrow{Q_1Q_2}$ des del punt Q_2'.

   e) Anàlogament, des del punt Q_1 fem la perpendicular ℓ a la recta $\overleftrightarrow{Q_1'Q_2'}$. Obtenim el punt pla Q_1^*.

   f) Hi ha una circumferència que passa pels quatre punts Q_1^*, Q_2^*, Q_1 i Q_2'.

   g) Considerem ara les cordes $\ell := \overleftrightarrow{Q_2^*Q_2'}$ i $\ell' := \overleftrightarrow{Q_1^*Q_1}$. Es tallen en un punt F que pertany a l'eix radical de les dues circumferències donades.[71]

   h) Tirem ara la perpendicular $\mathfrak{p}$ a la recta $\overleftrightarrow{P_1P_2}$ des del punt F. És l'eix radical.[72]

   i) Ara podem aplicar la part (2) a $\mathfrak{p}$ i a una de les circumferències donades $P_i(\overline{P_iQ_i}), i = 1, 2$.

   Amb això s'acaba la demostració. □

70 Qualsevol punt pla de la circumferència de centre P_1 i radi $\overline{P_1Q_1}$ serveix igualment com a punt Q_1.

71 La potència de F a la circumferència $P_i(\overline{P_iQ_i}), i = 1, 2$, és la potència de F a la circumferència que passa pels quatre punts Q_1^*, Q_2^*, Q_1 i Q_2'. Per tant, és un punt que té la mateixa potència amb les dues circumferències donades. És, doncs, un punt de l'eix radical.

72 L'eix radical de dues circumferències és perpendicular a la recta que n'uneix els centres.

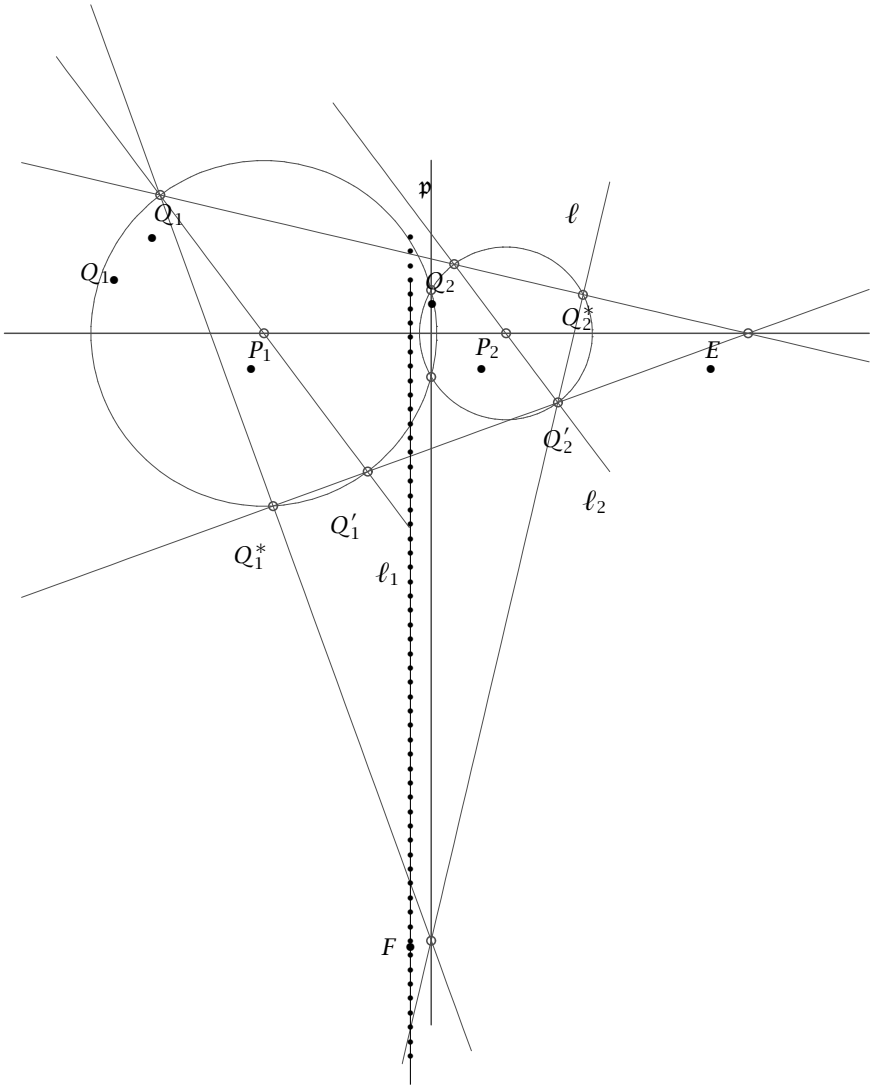


FIGURA 21

8.13 COROL·LARI *El cos dels nombres reals plans coincideix amb el cos euclidià* $\mathbb{E}$.

DEMOSTRACIÓ És una conseqüència de l'observació que segueix la definició 8.4 i del teorema 8.12, i proporciona una demostració alternativa —de tipus geomètric— a la més algèbrica del corol·lari 7.8. □

9 La papiroflèxia parabòlica

Hem vist que la papiroflèxia plana genera el cos euclidià $\mathbb{E}$. També hem vist que genera alguns punts d'una paràbola de paràmetre ja construït.

Com hem comentat a la introducció, tallant paràboles i circumferències, podem trisecar l'angle i doblar el cub. De fet, com dèiem a la pàgina 85, tot rau a saber doblar el cub —que, segons el resultat d'Hipòcrates de Quiós,[73] equival a trobar dues mitjanes proporcionals— i trisecar els angles. Ara bé, no ho podrem pas aconseguir amb la papiroflèxia plana. Caldrà, en tot cas, una papiroflèxia més potent.

La idea intuïtiva la proporciona un fet que trobem exposat i desenvolupat a l'obra de Row, segons la qual no cal disposar de la paràbola, n'hi ha prou amb les tangents a la paràbola.[74] De fet, diu:

PROBLEMA *Donada una recta ℓ i un punt $P \notin \ell$, considerem* tots *els plecs $\mathfrak{p}$ tals que $P^{\mathfrak{p}} \in \ell$. És una família de rectes. La seva* envolupant *és la paràbola que té com a directriu la recta ℓ i com a focus el punt P.*[75]

Ja hem resolt aquest problema a la part iii) del teorema 4.7.

Per tal de copsar quina potència ha de tenir la nova papiroflèxia res millor que començar a l'inrevés. Veurem com podem doblar el cub i trisecar l'angle fent servir plecs, una mica en la línia que hem seguit en analitzar com, amb el mètode suggerit per Row, podíem fer arrels quadrades arbitràries.

Un cop ho hàgim aconseguit, mirarem d'extreure'n el mínim necessari per poder donar la papiroflèxia parabòlica, en la qual, com en els casos anteriors, caldrà especificar l'operació de plegament genèric $\mathbf{O}_2$.

Pel que fa a la *duplicació del cub*, usarem el mètode atribuït a Plató (429–348 aC).[76]

9.1 TEOREMA (TEOREMA DE PLATÓ) *El mètode que s'exposa a continuació proporciona —en la manera de parlar dels geòmetres grecs— dues mitjanes proporcionals entre els segments a i b.*

DEMOSTRACIÓ Considerem dues rectes perpendiculars ℓ_1 i ℓ_2. Sigui O el punt en què es tallen. Hi considerem els punts $P = \langle 0, -a\rangle$ i $Q = \langle -b, 0\rangle$.[77]

Ara imaginem un enginy format per dues eles, és a dir, dues rectes perpendiculars en R i S, respectivament, de manera que, recolzant-se l'una en l'altra en el braç comú $\mathfrak{p}$, es puguin desplaçar. És l'anomenat enginy de Plató perquè, com ja hem dit abans, s'atribueix a l'eminent filòsof.

Tal com indica la figura 22, situem la primera ela de manera que un braç passi per P i el vèrtex S estigui damunt de l'eix vertical, condició que s'ha de mantenir en els moviments ulteriors. Desplacem l'altra ela fins que el braç paral·lel al de la primera que passa per P passi per Q, condició que s'ha de mantenir també d'ara endavant. Cal, tanmateix, que el vèrtex R de la segona ela es situï damunt de l'horitzontal.

73 Vegeu la nota 20.

74 Vegeu la nota 64.

75 Cal indicar que ara, a aquests plecs, no els imposem cap restricció. És a dir, de moment no cal que passin per cap punt. De fet, no són pas plecs en cap dels sentits indicats en les dues papiroflèxies anteriors.

76 Vegeu [9, I, 255–258].

77 Hi hem transportat, de fet, segments de longituds a i b.

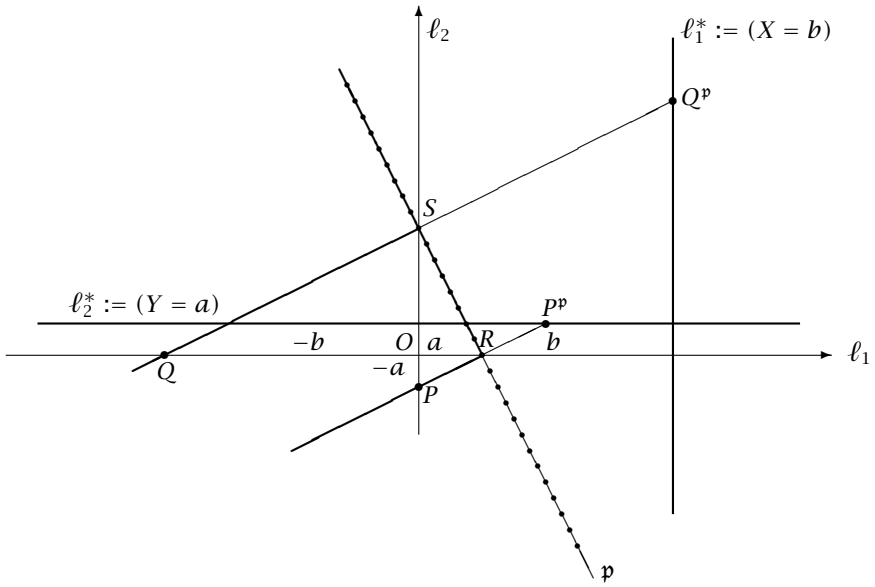


FIGURA 22

És obvi que els segments OR i OS proporcionen les dues mitjanes proporcionals entre OP i OQ, perquè és evident que els triangles $\triangle POR, \triangle ROS$ i $\triangle SOQ$ són semblants. Per tant,

$$\frac{OP}{OR} = \frac{OR}{OS} = \frac{OS}{OQ}.$$

Així, doncs, donats els segments OP i OQ, hem determinat dues mitjanes proporcionals entre ells, tal com volíem. □

Voldria indicar, per ajudar el lector a comprendre els passos que vaig seguir en aquest procés, que, de tot això, me'n vaig adonar en observar que, amb tangents adequades a paràboles adequades, s'aconseguia aquest resultat.[78]

DEMOSTRACIÓ Tal com indica la figura 23, agafem $O := \langle 0, 0\rangle, S := \langle b, 0\rangle$. Ara sigui $P := \langle 0, -a\rangle$, i $Q := \langle -b, 0\rangle$. Els punts P i Q són punts construïbles, un cop donats els valors a i b com a coordenades de punts construïbles. Considerem ara les rectes $\ell_1 := (Y = a)$ i $\ell_2 := (X = b)$.

Necessitem la paràbola de focus P i directriu ℓ_1, i la paràbola de focus Q i directriu ℓ_2. Aquestes dues paràboles tenen una tangent comuna $\mathfrak{p}$. És el plec buscat. És a dir, és un plec que porta el punt P damunt la recta ℓ_1 i el punt Q damunt la recta ℓ_2. És a dir, $P^{\mathfrak{p}} \in \ell_1$ i $Q^{\mathfrak{p}} \in \ell_2$.

Aquest plec $\mathfrak{p}$ talla la recta ℓ_X en el punt R. És fàcil provar que $R := \langle \sqrt[3]{a^2 b}, 0\rangle$. Per tant, R és un punt construïble amb el plec $\mathfrak{p}$ que determina el

78 Tanmateix, com hem vist en el teorema de Plató, tot plegat és molt més simple.

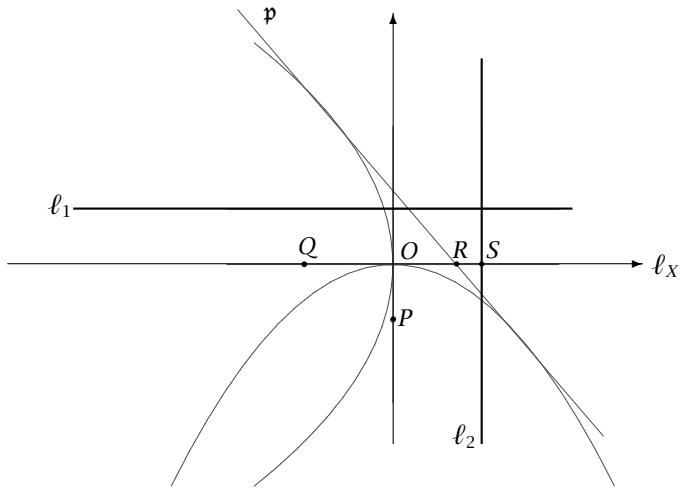


FIGURA 23

punt $P_{\sqrt[3]{a^2b}}$. En el cas particular en què $a = 1$, tenim un segment la longitud del qual és $\sqrt[3]{b}$.

En efecte. Les paràboles són, respectivament, $X^2 = 4aY$ i $Y^2 = 4bX$. A ambdues els imposem que $Y' = m$. Els punts respectius de tangència són $\langle 2am, am^2\rangle$ i $\langle \frac{b}{m^2}, \frac{2b}{m}\rangle$. Obtenim, doncs, les tangents respectives $Y - mX + am^2 = 0$, $mY - m^2X - b = 0$, que han de ser la mateixa. És a dir, $m^3 = -\frac{b}{a}$. Aquesta recta talla l'eix ℓ_X en el punt de coordenades $X = \sqrt[3]{a^2b}, Y = 0$, tal com volíem. □

Si ens fixem novament en la figura 22, ens adonem que, donats els punts P i Q, la recta $\mathfrak{p} = \overleftrightarrow{RS}$ es comporta com un plec que els transporta, respectivament, damunt les rectes $\ell_1^* := (X - b = 0)$ i $\ell_2^* := (Y - a = 0)$ que són paral·leles als eixos i disten, respectivament, del punt O el mateix que els punts P i Q.

A la vista d'aquest cas, necessitem, doncs, una mena de plecs que, donats dos punts i dues rectes (en principi perpendiculars), portin de cop un punt damunt d'una recta i l'altre damunt l'altra recta.

Tot quedarà, doncs, resolt si trobem una trisecció geomètrica de l'angle que es pugui resoldre amb aquesta mena de plecs. Fem, doncs, l'anàlisi de la trisecció de l'angle:

Considerem un angle agut $\angle BOC$, trisecat per les rectes OC_1 i OC_2 (figura 24a). Tirem la perpendicular OV a la base OB de l'angle. Fem una simetria per a la recta $\overleftrightarrow{VW}$, perpendicular a la recta $\overleftrightarrow{OC_1}$ des d'un punt arbitrari V. Tindrem les rectes perpendiculars $\overleftrightarrow{VM}$ i $\overleftrightarrow{WM}$. En resulta que la recta $\overleftrightarrow{OC_2}$ és perpendicular a la recta $\overleftrightarrow{VM}$, atès que els angles $\angle BOC_1$, $\angle C_1OC_2$ i $\angle WMO$ són

iguals —$\angle BOC_1 = \angle C_1OC_2$ i $\angle C_1OC_2 = \angle WMO$— i, per tant, les rectes $\overleftrightarrow{WM}$ i $\overleftrightarrow{OC_2}$ són paral·leles. Per construcció, la recta $\overleftrightarrow{OC_2}$ divideix l'angle $\angle C_1OC$ en dues meitats.

Això fa que la recta $\overleftrightarrow{OC_2}$ sigui la mediana del segment MN, atès que és alhora bisectriu i alçada del triangle $\triangle MON$. Per tant, els segments NR i MR, on R és el punt en què la recta $\overleftrightarrow{OC_2}$ talla la base MN del triangle esmentat, són iguals.

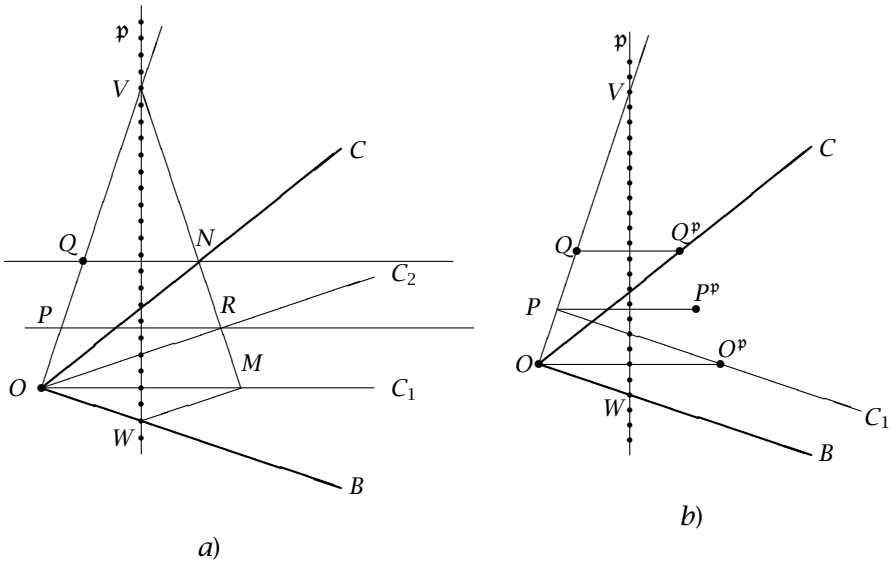


FIGURA 24

Ara, per N i R tirem rectes paral·leles a la recta OC_1. Determinem els punts P i Q damunt la recta OV de manera que $\overline{OP} = \overline{PQ}$. □

D'aquesta anàlisi en resulta que només cal un plec —el plec $\mathfrak{p} = \overleftrightarrow{VW}$— que transporti el vèrtex O de l'angle donat damunt la recta paral·lela a la base OB i el punt Q damunt l'altre costat de l'angle, el costat OC.

És a dir, cal considerar la situació de la figura 24b que permet establir el teorema següent:

9.2 TEOREMA *És possible trisecar un angle fent servir plecs.*

DEMOSTRACIÓ Considerem un angle agut $\angle BOC$. Tirem una perpendicular OV a la base OB i, hi considerem els punts P i Q tals que $\overline{OP} = \overline{PQ}$. Ara fem un plec $\mathfrak{p}$ que porti O damunt la recta OC_1, paral·lela a OB per P, i el punt Q damunt el costat OC de l'angle donat.

Aquest plec talla la base de l'angle i la seva perpendicular en els punts W i V, respectivament.

Ara tirem les rectes $\overleftrightarrow{OC_1}$ i $\overleftrightarrow{OC_2}$ que uneixen el vèrtex O amb els punts imatge $O^{\mathfrak{p}}$ i $P^{\mathfrak{p}}$. En resulta que els punts $O^{\mathfrak{p}}$, $P^{\mathfrak{p}}$ i $Q^{\mathfrak{p}}$ estan alineats. Tirem la recta que passa per aquests tres punts. Tallarà el plec $\mathfrak{p}$ en el punt V pel fet que és un plec. I, per fi, unim el punt W amb el punt $O^{\mathfrak{p}}$ (figura 25).

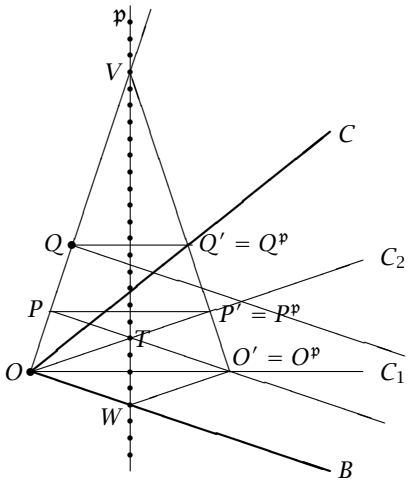


FIGURA 25

Hem de veure que les rectes OC_1 i OC_2 divideixen l'angle donat $\angle BOC$ en tres parts iguals.

Per simplificar les notacions, fem $O' := O^{\mathfrak{p}}, P' := P^{\mathfrak{p}}$ i $Q' := Q^{\mathfrak{p}}$. De la simetria resulta que els segments $\overline{O'P'}$ i $\overline{P'Q'}$ són iguals, atès que, per construcció, $\overline{OP}$ i $\overline{PQ}$ ho són. El punt T en què es tallen els segments $\overline{OP'}$ i $\overline{O'P}$ els divideix en parts iguals. Per tant, $\overline{PT} = \overline{TO'}$ i $\overline{OT} = \overline{TP'}$. La recta $\overleftrightarrow{OP'}$ és perpendicular a la recta $\overleftrightarrow{O'Q'}$.

En resulta que $\overleftrightarrow{OP'}$ és alhora alçada i mediatriu del costat $O'Q'$ del triangle $\triangle Q'OO'$. D'on resulta que és la bisectriu de l'angle $\angle O'OQ'$. En definitiva, doncs, $\angle Q'OP' = \angle P'OO'$.

D'altra banda, el quadrilàter $OWO'T$ és un paral·lelògram atès que, per construcció, les rectes $\overleftrightarrow{OB}$ i $\overleftrightarrow{PO'}$ són paral·leles. Aleshores, per simetria, $\overleftrightarrow{WO'}$ i $\overleftrightarrow{OP'}$, també són paral·leles. D'on $\overline{O'W} = \overline{OT}$. Per tant, les diagonals del quadrilàter $OWO'T$ són ortogonals i la recta OO' divideix l'angle $\angle C_2OB$ en dos angles iguals $\angle C_2OC_1$ i $\angle C_1OB$. Per tant,

$$\angle COC_2 = \angle C_2OC_1 = \angle C_1OC,$$

tal com volíem.

Atès que l'angle recte és trisecable, el teorema val també per als obtusos.□

En definitiva, doncs, si disposem d'una operació de plegament que, donades dues rectes concurrents, no necessàriament perpendiculars,[79] i dos punts, permet portar cada un dels punts damunt d'una de les rectes, podrem doblar cubs i trisecar angles i, per tant, resoldre totes les cúbiques i quàrtiques els coeficients de les quals corresponguin a valors de punts-plec ja construïts.

És a dir, podem ja definir amb precisió la *papiroflèxia parabòlica* o *vietana*. Només cal especificar l'operació $\mathbf{O}_2$ de la definició 6.1 que correspon a aquesta mena de papiroflèxia.

9.3 DEFINICIÓ *Un plegament genèric de la definició 6.1 esdevé un* plegament parabòlic *quan, en l'operació $\boldsymbol{O}_2$, les rectes ℓ i ℓ' tenen almenys un punt en comú. És a dir, una recta $\mathfrak{p}$ és un* plec parabòlic *si, i només si, donats dos plecs ℓ i ℓ', no paral·lels, i dos punts P i Q arbitraris (ja construïts), $P^{\mathfrak{p}} \in \ell$ i $Q^{\mathfrak{p}} \in \ell'$.*

Aquest plegament, juntament amb el plegament lineal, proporciona la papiroflèxia parabòlica.

Els plecs que s'obtenen aplicant qualsevol d'ambdós tipus de plegaments els anomenarem plecs *(o* rectes*)* parabòlics.

Un punt parabòlic *és el que s'obté tallant dues rectes parabòliques.*

Un nombre real a l'anomenarem nombre real parabòlic*, si el punt P_a s'obté tallant rectes parabòliques.*

L'operació $\mathbf{O}_2$ del plegament parabòlic és tan potent que implica l'operació $\mathbf{O}_1$ o plegament lineal.[80]

9.4 PROPOSICIÓ *Siguin P, Q dos punts ja construïts. Aleshores, aplicant l'operació $\boldsymbol{O}_2$ del plegament parabòlic, podem construir el plec $\ell := \overleftrightarrow{PQ}$.*

DEMOSTRACIÓ (figura 26). Siguin P i Q dos punts parabòlics. Existeixen dues parelles de rectes parabòliques ℓ_P i ℓ'_P i ℓ_Q i ℓ'_Q que determinen, respectivament, P i Q.

Per tant, una de les que passen per P en talla una de les que passen per Q. Suposem que són ℓ_P i ℓ_Q. Considerem el plec $\mathfrak{p}$ que deixa el punt P en ℓ_P i el punt Q en ℓ_Q. És el plec que passa per P i Q. □

Ara veurem que, amb aquest tipus de plegaments, podem realitzar plegaments plans.

9.5 PROPOSICIÓ *Siguin P, Q dos punts i ℓ una recta ja construïts. Aleshores podem fer el plec pla que passa per P i porta el punt Q damunt de la recta ℓ.*

DEMOSTRACIÓ (figura 27). El plec ℓ conté, almenys, dos punts parabòlics. Sigui $P' \in \ell$, amb $P' \neq P$. Agafem com a recta ℓ' la recta $\overleftrightarrow{PP'}$. Considerem ara els plecs $\mathfrak{p}$ tals que $P^{\mathfrak{p}} \in \ell'$ i $Q^{\mathfrak{p}} \in \ell$.

Un d'aquests plecs parabòlics passa per P i, per definició, és un plec pla. □

79 És possible limitar-se a rectes perpendiculars, però aleshores cal afegir l'operació que, donats dos punts, hi hagi un plec que passi per ells, quelcom que nosaltres podem deduir com s'explicita a l'apèndix B.

80 Vegeu la proposició 8.9.

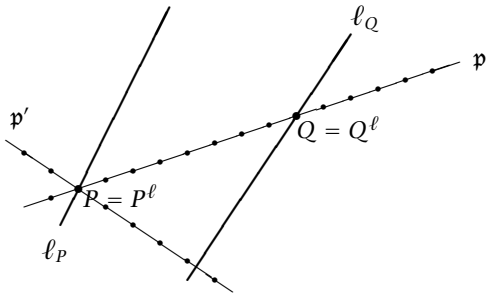


FIGURA 26

Per tant, si disposem de l'operació parabòlica $\mathbf{O}_2$, disposem també de l'operació $\mathbf{O}_2$ plana.

9.6 TEOREMA *Tot punt de* $\mathbb{V}$ *és parabòlic.*

DEMOSTRACIÓ És un corol·lari de tot el que hem fet fins ara, perquè un punt de $\mathbb{V}$ s'obté usant regle i compàs, doblant cubs i trisecant angles. Per tant, és un punt parabòlic.[81] □

Ara cal veure el recíproc. Tot punt parabòlic pertany a $\mathbb{V}$. O, dit en unes altres paraules, la papiroflèxia parabòlica no supera la potència que proporciona la resolució de cúbiques i quàrtiques.

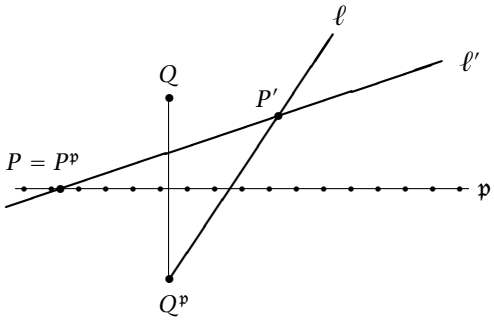


FIGURA 27

9.7 TEOREMA *Tot punt parabòlic pertany a* $\mathbb{V}$.

DEMOSTRACIÓ Suposem que tenim dos plecs parabòlics ℓ i ℓ', no paral·lels, i dos punts parabòlics P i Q. Volem veure que el plec $\mathfrak{p}$ que fa que $P^{\mathfrak{p}} \in \ell$ i $Q^{\mathfrak{p}} \in \ell'$ s'obté, en el pitjor dels casos, resolent una cúbica.

81 En definitiva, hem vist que $\mathbb{Q} \subsetneq \mathbb{P} \subsetneq \mathbb{E} \subsetneq \mathbb{V} \subsetneq \mathcal{A} \subsetneq \mathbb{R}$.

Per qüestions de claredat, distingirem dos casos, encara que això no és indispensable.

Cas 1. Suposem que $P \in \ell$ i $Q \in \ell'$. (Figura 28), els únics plecs parabòlics possibles són:

1. $\mathfrak{p}_1 :=$ la perpendicular a ℓ' que passa per P,
2. $\mathfrak{p}_2 :=$ la perpendicular a ℓ que passa per Q,
3. $\mathfrak{p}_3 :=$ la recta $\overleftrightarrow{PQ}$.

És a dir, si $P := \langle x_1, y_1 \rangle$, $Q := \langle x_2, y_2 \rangle$, $\ell := \alpha X + \beta Y + \gamma$, i $\ell' := \alpha' X + \beta' Y + \gamma'$, amb $x_1, x_2, y_1, y_2, \alpha, \alpha', \beta, \beta', \gamma, \gamma' \in \mathbb{V}$ i $\alpha\beta' - \alpha'\beta \neq 0$, aleshores $\mathfrak{p}_1 := \beta' X - \alpha' Y + (\alpha' y_1 - \beta' x_1) = 0$; $\mathfrak{p}_2 := \beta X - \alpha Y + (\alpha y_2 - \beta x_2) = 0$;

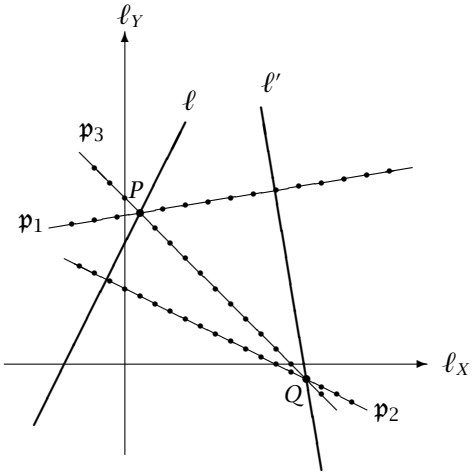


FIGURA 28

$$\mathfrak{p}_3 := \begin{vmatrix} X & Y & 1 \\ x_1 & y_1 & 1 \\ x_2 & y_2 & 1 \end{vmatrix} = (y_1 - y_2)X - (x_1 - x_2)Y + x_1 y_2 - x_2 y_1 = 0.$$

Tots els coeficients que resulten són, doncs, nombres parabòlics i, per tant, en tallar dues rectes, només obtindrem nombres parabòlics. Les coordenades dels punts són, doncs, nombres parabòlics.

Cas 2. Suposem que $P \notin \ell$. (Figura 29), podem suposar que $P := \langle 0, 0\rangle$ i l'equació de la recta ℓ és $Y = 2$.[82] La recta ℓ' talla la recta $Y - 2 = 0$. Per tant, és de la forma

$$X + rY + s = 0.$$

Sigui $Q := \langle u, v\rangle$. El plec $\mathfrak{p}$ no és perpendicular a la recta ℓ, atès que el punt $P \notin \ell$. Per tant, és de la forma

$$Y = mX + b.$$

Usem ara l'expressió dels punts simètrics (vegeu la proposicio 4.3) respecte de la recta $mX - Y - b = 0$. Volem que $P^{\mathfrak{p}} \in \ell$. Per tant, cal que

$$2 = y' = y - \frac{2(-1)(mx - y + b)}{m^2 + 1}, \text{ amb } x = 0, y = 0.$$

Això fa que $b = m^2 + 1$. Ara suposem que $Q^{\mathfrak{p}} := \langle u^{\mathfrak{p}}, v^{\mathfrak{p}}\rangle$. Cal que $Q^{\mathfrak{p}} \in \ell$. Per tant,

$$u^{\mathfrak{p}} + rv^{\mathfrak{p}} + s = 0.$$

Però,

$$u^{\mathfrak{p}} = u - \frac{2m(mu - v + m^2 + 1)}{m^2 + 1},$$
$$v^{\mathfrak{p}} = v - \frac{2(-1)(mu - v + m^2 + 1)}{m^2 + 1}.$$

Per tant,

$$(m^2 + 1)u - 2m^2u + 2mv - 2m^3 - 2m + \\ + r\big((m^2 + 1)v + 2mu - 2v + 2m^2 + 2\big) + s = 0.$$

És una cúbica en m. Hi ha, doncs, a tot estirar tres plecs que ho compleixen, però tots tres són parabòlics. □

9.8 Corol·lari *El cos $\mathbb{V}$ és el més petit cos vietà o parabòlic.* □

Ara, tot reproduint els passos que normalment se segueixen en la demostració del teorema de Wantzel,[83] demostrarem el teorema de Wantzel relatiu a la papiroflèxia parabòlica.

9.9 Definició *Un cos K' és una* extensió parabòlica simple *de K si, i només si, K' és el més petit cos que conté una extensió quadràtica K_1 de K i, a més, conté les coordenades dels punts parabòlics produïts pel plec $\mathfrak{p}(P, Q; \ell, \ell')$ —un dels*

82 Equival a fer translacions i girs; és a dir, sumes, restes, multiplicacions, divisions i extraccions d'arrels quadrades, i tot això són operacions parabòliques que transformen nombres de $\mathbb{V}$ en nombres $\mathbb{V}$.

83 Vegeu el teorema 3.15.

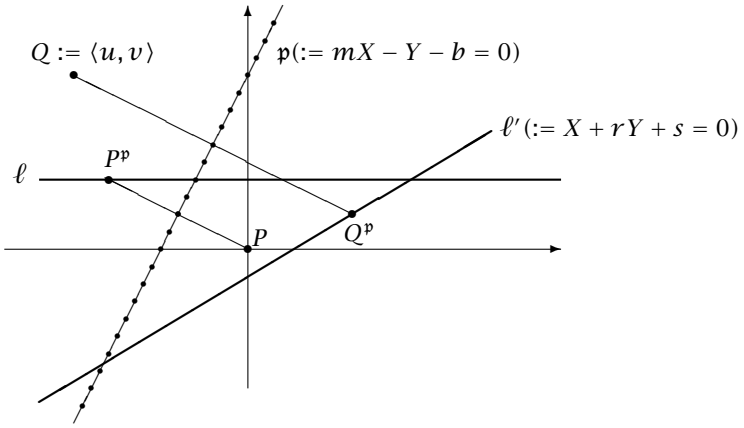


FIGURA 29

plecs parabòlics $\mathfrak{p}$ *tals que* $P^{\mathfrak{p}} \in \ell$ *i* $Q^{\mathfrak{p}} \in \ell'$ *—, on* P *i* Q *són dos* K_1*-punts, i* ℓ *i* ℓ' *dues* K_1*-rectes, quan talla les rectes de* K_1*.*[84]

Un cos K' *és* extensió parabòlica iterada *d'un cos* K *si, i només si, és el terme final de la cadena d'extensions parabòliques*

$$K_0 = K \subseteq K_{01} \subseteq K_1 \subseteq K_{11} \subseteq K_2 \subseteq \cdots \subseteq K_{n-1} \subseteq K_{(n-1)1} \subseteq K_n, \qquad (1)$$

on cada subcadena $K_{i-1} \subseteq K_{(i-1)1} \subseteq K_i$ *és la cadena de l'extensió parabòlica simple* K_i *de* K_{i-1}*,* $i = 1, \ldots, n$*, on* $K_{(i-1)1}$ *designa l'extensió quadràtica intermèdia.*

9.10 PROPOSICIÓ *Si* K' *és una extensió parabòlica iterada de* $\mathbb{Q}$*, aleshores el grau* $[K' : \mathbb{Q}] = 2^m \times 3^n$*, on* m *i* n *poden ser nuls.*

DEMOSTRACIÓ És trivial, atès que, per a cada índex i de la cadena (1), en la qual considerem que $K_0 = \mathbb{Q}$, $[K_{(i-1)1} : K_{i-1}] \leq 2$ i $[K_i : K_{(i-1)1}] \leq 3$. Per tant, $[K_i : K_i] = 2^m \times 3^n$, on m i n poden ser nuls. □

D'on resulta

9.11 COROL·LARI (TEOREMA DE WANTZEL PARABÒLIC) *Si* a *és un real parabòlic sobre* $\mathbb{Q}$*, aleshores* $gr_{\mathbb{Q}}(a) = 2^r \times 3^s$*.*[85]

DEMOSTRACIÓ Tenim que $a \in K$, on K és una extensió parabòlica de $\mathbb{Q}$. Per tant,

$$[K : \mathbb{Q}] = [K : \mathcal{K}(a)] \times [\mathcal{K}(a) : \mathbb{Q}] = 2^m \times 3^n.$$

Per tant, $[\mathcal{K}(a) : \mathbb{Q}] = \mathrm{gr}_{\mathbb{Q}}(a) = 2^r \times 3^s$, on r i s poden ser nuls. □

84 Imposem que contingui una extensió quadràtica perquè sigui tancat pel gir d'eixos que permet aplicar el teorema 9.7.

85 Vegeu l'apèndix C.

És clar que el recíproc és fals. No tota arrel real d'un polinomi irreductible el grau del qual sigui de la forma $2^r \times 3^s$ és un real parabòlic. N'hi ha prou de considerar una sèxtica que no sigui resoluble per radicals.[86]

* * *

Amb aquest resultat s'acaba l'objectiu inicial d'aquest treball que era fer una presentació de les possibilitats geomètriques de les papiroflèxies traduïdes al llenguatge de l'àlgebra dels polinomis.

Tanmateix, el col·lega i amic Ignasi Mundet, que assistia a l'exposició que vaig fer a la Trobada Matemàtica de la Societat Catalana de Matemàtiques l'any 2002, em va preguntar si, amb aquesta papiroflèxia, hom podia construir l'heptàgon i l'enneàgon. En ambdós casos la resposta és afirmativa i senzilla, però, com podem veure en les proposicions següents, no és pas de la mateixa naturalesa atès que el nombre de costats en un cas és primer i en l'altre és compost.

9.12 PROPOSICIÓ *L'heptàgon i l'ennèagon són construïbles amb papiroflèxia parabòlica.*

DEMOSTRACIÓ *Construcció de l'enneàgon.* És evident, atès que l'única cosa que cal fer és trisecar l'angle del triangle equilàter. Però el triangle equilàter i la trisecció d'un angle ja construït es poden realitzar amb papiroflèxia parabòlica.

Construcció de l'heptàgon. Dibuixar l'heptàgon equival a dibuixar les arrels del polinomi $Z^7 - 1 = 0$. Les no trivials són les que corresponen al polinomi ciclotòmic $\frac{Z^7-1}{Z-1} = Z^6 + Z^5 + Z^4 + Z^3 + Z^2 + Z + 1 = 0$. El canvi de variables estàndard en el cas dels polinomis simètrics $X = Z + \frac{1}{Z}$ transforma el polinomi ciclotòmic en el polinomi $X^3 + X^2 - 2X - 1 = 0$.[87]

Cal, doncs, resoldre una cúbica i això és possible fer-ho amb papiroflèxia parabòlica. □

Això no obstant, la pregunta plantejava una qüestió molt més general que calia resoldre i que exposo en l'apèndix següent.

---

86 Per exemple, la sèxtica $X^6 - X^2 + 2X = 0$. Recordem que, en $\mathbb{C}$, la trisecció de l'angle equival a l'extracció d'arrels cúbiques.

87 Aquesta observació m'ha estat suggerida pel *referee*, arran de la proposta que jo havia fet, més complexa, però amb la qual volia posar de manifest com juguen en tota aquesta transformació els cosinus de l'angle θ a fi de motivar la proposició A.1.

És a dir, la meva proposta era: els afixos complexos z de l'heptàgon regular són els que resolen l'equació polinòmica $Z^7 - 1 = 0$. Per convertir-los en nombres reals fem $z + z^2 = 2\cos\theta$, $z^2 + z^5 = \cos 2\theta$, i $z^3 + z^4 = 2\cos 3\theta$. Per tant, hem de resoldre l'equació $2\cos\theta + 2\cos 2\theta + 2\cos 3\theta + 1 = 0$, que, desenvolupant, dóna $2\cos\theta + 2(2\cos^2\theta - 1) + 2(4\cos^3\theta - 3\cos\theta) + 1 = 0$, i operant: $8\cos^3\theta + 4\cos^2\theta - 4\cos\theta - 1 = 0$. Finalment, $x^3 + x^2 - 2x - 1 = 0$, on $x = 2\cos\theta$.

O bé, alternativament i de manera més breu: $\cos 7\theta = \cos(3\theta + 4\theta) = 64\cos^7\theta - 112\cos^5\theta + 56\cos^3\theta - 7\cos\theta$, que implica $x^7 - 7x^5 + 14x^3 - 7x - 2 = (x^3 + x^2 - 2x - 1)^2(x - 2) = 0$. Vegeu també la proposició A.1.

Apèndixs

A El teorema de Gauss-Wantzel per a polígons regulars parabòlics

Recordem que el teorema de Gauss-Wantzel relatiu als polígons regulars construïbles amb papiroflèxia plana —*polígons regulars plans*— diu:

TEOREMA DE GAUSS-WANTZEL *Un polígon regular de n costats és construïble amb papiroflèxia plana si, i només si, $n = 2^m \times p_1 \times \cdots \times p_k$, on els p_i, $i = 1, \ldots, k$, són primers de Fermat diferents.*[88]

En aquest apèndix volem generalitzar-lo als polígons regulars construïbles amb papiroflèxia parabòlica —*polígons regulars parabòlics*— i, per tant, establir el teorema següent:

TEOREMA GENERAL DE GAUSS-WANTZEL *Un polígon regular de n costats és construïble amb papiroflèxia parabòlica si, i només si, $n = 2^{m_1} \times 3^{m_2} \times p_1 \times \cdots \times p_k$, on els p_i, $i = 1, \ldots, k$, són primers de Pierpont diferents.*[89]

Ho farem en dues parts. En la primera establirem el teorema de Wantzel relatiu als polígons regulars parabòlics[90] i, en la segona, el teorema de Gauss corresponent.[91]

A.1 Teorema de Wantzel generalitzat a polígons regulars parabòlics

Calen algunes proposicions prèvies que establim a continuació i algunes qüestions generals d'àlgebra relatives a les extensions de cossos, que recordem a l'apèndix C.

A.1 PROPOSICIÓ *Si q és un enter senar > 1, aleshores els nombres reals*

$$\tan\frac{360^\circ}{q}, \tan\frac{2\times 360^\circ}{q}, \ldots, \tan\frac{(n-2)\times 360^\circ}{q}, \tan\frac{(n-1)\times 360^\circ}{q},$$

són les arrels de l'equació polinòmica, amb coeficients enters,

$$P_q(X) := x^{q-1} - \binom{q}{2}x^{q-3} + \binom{q}{4}x^{q-5} - \cdots + (-1)^{\frac{q-1}{2}}\binom{q}{q-3}x^2 + (-1)^{\frac{q+1}{2}}q = 0.$$

88 Recordem que, si un nombre $p = 2^r + 1, r > 0$, és primer aleshores necessàriament $r = 2^s, s \geq 0$. Els nombres de la forma $2^{2^r} + 1$ són els *nombres de Fermat* i, quan són primers, són els *nombres primers de Fermat.*

89 Un nombre de la forma $p = 2^r \times 3^s + 1$, $r > 1, s \geq 0$, és un *nombre de Pierpont* i, quan és primer, és un *nombre primer de Pierpont.*

D'acord amb el treball d'Andrew M. Gleason de 1988, els nombres primers de Pierpont més petits que 1.000.000 són: 2, 3, 5, 7, 13, 17, 19, 37, 73, 97, 109, 163, 193, 257, 433, 487, 577, 769, 1.153, 1.297, 1.459, 2.593, 2.917, 3.457, 3.889, 10.369, 12.289, 17.497, 18.433, 39.367, 52.489, 65.537, 139.969, 147.457, 209.953, 331.777, 472.393, 629.857, 746.497, 839.809, 995.329.

90 Ens hem inspirat en [11, 117–125] .

91 Ens hem inspirat en [8, 106–114] .

DEMOSTRACIÓ Tot es basa en les fórmules trigonomètriques de Viète següents:[92]

$$\begin{aligned}
\sin q\theta &= \sum_{j=1}^{\frac{q+1}{2}} (-1)^{j-1} \binom{q}{2j-1} \cos^{q-2j+1}\theta \sin^{2j-1}\theta = \\
&= \frac{q}{1}\cos^{q-1}\theta\sin\theta - \binom{q}{3}\cos^{q-3}\theta\sin^3\theta + \binom{q}{5}\cos^{q-5}\theta\sin^5\theta - \cdots \\
&\quad \cdots + (-1)^{\frac{q-1}{2}}\sin^q\theta; \\
\cos q\theta &= \sum_{j=1}^{\frac{q+1}{2}} (-1)^{j-1} \binom{q}{2j-2} \cos^{q-2j+2}\theta \sin^{2j-2}\theta = \\
&= \cos^q\theta - \binom{q}{2}\cos^{q-2}\theta\sin^2\theta + \binom{q}{4}\cos^{q-4}\theta\sin^4\theta - \cdots \\
&\quad \cdots + (-1)^{\frac{q-1}{2}}\binom{q}{q-1}\cos\theta\sin^{q-1}\theta.
\end{aligned}$$

Ara dividim $\sin q\theta$ per $\cos^q\theta$.[93] Aleshores fem $x = \tan\theta$ i obtenim el resultat desitjat. □

A.2 PROPOSICIÓ *Suposem que els polígons regulars de $p \geq 3$ i $q \geq 3$ costats són construïbles, amb $\langle p, q\rangle = 1$. Fem $n = p \times q$.*[94] *Aleshores el polígon regular de n costats també és construïble.*

DEMOSTRACIÓ Per la identitat d'Etienne Bézout [1730–1783],[95] tenim que

$$1 = ap + bq.$$

Per tant,

$$\frac{1}{n} = \frac{1}{pq} = \frac{a}{q} + \frac{b}{q}.$$

D'on:

$$\frac{360^\circ}{n} = \frac{360^\circ}{pq} = a \times \frac{360^\circ}{q} + b \times \frac{360^\circ}{q}.$$

Atès que els polígons regulars de p i q costats són construïbles, ho són els angles $\frac{360^\circ}{p}$ i $\frac{360^\circ}{q}$. Per tant, també ho és, amb el mateix tipus de giny, l'angle $\frac{360^\circ}{n}$. □

92 Una manera senzilla de demostrar-les —que no és la que féu servir Viète— és fer inducció sobre q.

93 Observem que $\sin q\theta = 0$ per a tots els angles $k \times \frac{360^\circ}{q}$ $(k = 0, \ldots, q-1)$ en els quals $\cos\theta \neq 0$. Per tant, en aquests angles, podem dividir $\sin q\theta$ per $\cos^q\theta$.

94 Queden exclosos els nombres n que són primers o potències de primers.

95 En el cas dels nombres enters ja havia estat enunciada per Claude-Gaspar Bachet de Méziriac (1581–1638). Bézout la va estendre als polinomis.

A.3 PROPOSICIÓ *Suposem que $n = p \times q$, amb $\langle p, q\rangle = 1$, i que el polígon regular de n costats és construïble; aleshores els polígons regulars de p i q costats també han de ser-ho, de construïbles.*

DEMOSTRACIÓ Si $\frac{360^\circ}{n}$ és un angle construïble, aleshores els angles $p \times \frac{360^\circ}{n}$ i $q \times \frac{360^\circ}{n}$, també ho són, de construïbles, i amb el mateix giny. □

Ara hem de veure què passa amb els nombres primers i amb les potències de nombres primers, perquè la resta de nombres la podem descompondre en factors p i q, primers entre si. I, a la vista del corol·lari 9.11, caldrà considerar els nombres primers de la forma $2^r \times 3^s + 1$ que, com hem vist, generalitzen el cas ben conegut del regle i el compàs.

A.4 PROPOSICIÓ *Si $n = 2$, $n = 3$, $n = 2^k$, o $n = 3^\ell$, podem dividir la circumferència en n parts iguals amb papiroflèxia parabòlica.*

DEMOSTRACIÓ Els angles de 180° i 120° són, ambdós, construïbles amb regle i compàs.

Tots els angles, ja construïts, poden ser subdividits en dues parts iguals, amb regle i compàs.

Tots els angles, ja construïts, poden ser subdividits en tres parts iguals, amb papiroflèxia parabòlica.[96] □

A.5 DEFINICIÓ *Anomenarem* nombre primer pla (euclidià, *o* de Fermat) *tot nombre primer senar de la forma $2^{2^k} + 1$, on k és un enter no negatiu.*[97]

Anomenarem nombre primer parabòlic (vietà, *o* de Pierpont) *tot nombre primer senar ≥ 1 de la forma $2^r \times 3^s + 1$, on $r > 0$ i $s \geq 0$ són enters.*[98]

A.6 TEOREMA *Si p és un nombre primer senar i, amb papiroflèxia parabòlica, és possible dividir el cercle en p parts iguals, aleshores p és un nombre primer parabòlic.*

DEMOSTRACIÓ Suposem que l'angle $\theta = \frac{360^\circ}{p}$ fos construïble amb papiroflèxia parabòlica; aleshores també ho fóra $\tan\theta$. En resulta que

$$P_p(\tan\theta) = \sum_{j=1}^{\frac{p+1}{2}} (-1)^{j-1} \binom{p}{2j-1} \tan^{2j-2}\theta = 0.$$

Ara bé, pel criteri d'Eisenstein [1823–1852], el polinomi $P_p(X)$ és irreductible sobre $\mathbb{Q}$, atès que, quan p és primer, tots els nombres combinatoris $\binom{p}{j}$, $j = 1, \ldots, p-1$, són múltiples de p. A més, el terme independent $\pm p$ no és divisible per p^2. En resulta que $\tan\theta$ és la solució d'un polinomi irreductible

96 Si només disposem del regle i el compàs, aquesta darrera construcció, en general, no és possible.

97 Vegeu la nota 88.

98 Vegeu la nota 89.

de grau $p-1$. Pertany, doncs, a l'extensió algèbrica generada per $\tan\theta$, que, com podem veure a l'apèndix C, és un espai vectorial de dimensió $p-1$.

Ara bé, atès que $\tan\theta$ és un nombre real parabòlic, pertany també a una extensió parabòlica iterada K^* de $\mathbb{Q}$. Tenim, doncs, la cadena

$$\mathbb{Q} \subsetneq \mathcal{K}(\tan\theta) \subseteq K^*.$$

En resulta que

$$[K^*:\mathbb{Q}] = [K^*:\mathcal{K}(\tan\theta)][\mathcal{K}(\tan\theta):\mathbb{Q}].$$

Aleshores, atès que $[K^*:\mathbb{Q}] = 2^r \times 3^s$, resulta que $p-1 = [\mathcal{K}(\tan\theta):\mathbb{Q}] = 2^{r'} \times 3^{s'}$. Per tant, cal que p sigui un primer parabòlic, tal com volíem. □

A.7 TEOREMA *Si p és un nombre primer senar i h és un enter positiu més gran que* 1*, no és possible dividir el cercle en p^h parts iguals amb papiroflèxia parabòlica.*[99]

DEMOSTRACIÓ 1) Si $h > 2$ i és possible construir el polígon regular de p^h costats, també ho és, de possible, construir el polígon regular de

$$\frac{360^\circ}{p^2} = p^{h-2} \times \frac{360^\circ}{p^h}.$$

Per tant, l'única cosa que hem de fer és veure que no podem construir cap polígon regular de p^2 costats, si p és un nombre primer senar.

2) A més, solament certs polígons regulars de p^2 costats són construïbles amb papiroflèxia parabòlica, precisament aquells pels quals p és un nombre primer parabòlic. En efecte, suposem que el polígon regular de p^2 costats fos construïble; aleshores també ho fóra el de p costats: $\frac{360^\circ}{p} = p \times \frac{360^\circ}{p^2}$.

3) Suposem que el polígon regular de p^2 costats és construïble amb papiroflèxia parabòlica. Cal examinar el polinomi $P_q(X)$, amb $q = p^2$, i p primer senar parabòlic.

3.1) $P_{p^2}(X)$ es descompon en $\mathbb{Q}$: per la proposició A.1 sabem que $P_{p^2}(X) = 0$ té les $p-1$ arrels següents:

$$\tan\frac{k \times p \times 360^\circ}{p^2} = \tan\frac{k \times 360^\circ}{p} \quad (k = 1,\dots,p-1),$$

així com altres $p^2 - p$ arrels. Aleshores, per la *regla de Ruffini* [1765–1822], tenim que

99 En la demostració, Karanikoff comet un error, perquè afirma que els nombres combinatoris $\binom{p^2}{j}$, $j = 1,\dots,p^2-1$, són múltiples de p^2 (vegeu, per exemple, [11, 123–124]), que és fals, com podem constatar amb el cas $\binom{9}{3} = \frac{9\times8\times7}{1\times2\times3} = 84$. Però l'error no té importància perquè, de fet, l'única cosa que cal és que els nombres combinatoris $\binom{p^2}{j}$, $j = 1,\dots,p^2-1$, siguin divisibles per p, i això és cert.

$$P_{p^2}(X) =$$
$$= \left(X - \tan\frac{360^\circ}{p}\right)\left(X - \tan\frac{2\times 360^\circ}{p}\right)\cdots\left(X - \tan\frac{(p-1)\times 360^\circ}{p}\right)\times P(X)$$

per a un polinomi $P(X)$ de grau $p^2 - p = p^2 - 1 - (p-1)$.

Novament per la proposició A.1 i la regla de Ruffini, tenim que

$$P_p(X) = \left(X - \tan\frac{360^\circ}{p}\right)\left(X - \tan\frac{2\times 360^\circ}{p}\right)\cdots\left(X - \tan\frac{(p-1)\times 360^\circ}{p}\right).$$

D'on resulta la identitat de polinomis $P_{p^2}(X) = P_p(X)\times P(X)$.

Ara ens interessa analitzar el polinomi $P(X)$. Atès que $\tan\frac{360^\circ}{p^2}$ no és cap dels nombres $\tan\frac{k\times 360^\circ}{p}$, $(k = 1,\ldots,p-1)$ i $P_{p^2}(\tan\frac{360^\circ}{p^2}) = 0$, resulta que $P(\tan\frac{360^\circ}{p^2}) = 0$.

Observem que els coeficients de $P(X)$ són enters, perquè els de $P_{p^2}(X)$ i $P_p(X)$ ho són, i el coeficient principal de $P_p(X)$ és igual a 1. A més, el terme independent és p, divisible per p, però no per p^2.

Finalment, tots els coeficients de $P_{p^2}(X)$, llevat del principal, són divisibles per p. Per tant, $P_{p^2}(X) = X^{p^2-1} - pA(X)$, on $A(X)$ és un polinomi amb els coeficients enters. Anàlogament $P_p(X) = X^{p-1} - pB(X)$, on $B(X)$ és un poinomi amb els coeficients enters.

Suposem ara que $P(X) = X^{p^2-p} + C(X)$. Volem veure que tots els coeficients de $C(X)$ són divisibles per p. Fem càlculs:

$$X^{p^2-1} - pA(X) = \big(x^{p-1} - pB(X)\big)\big(X^{p^2-p} + C(X)\big).$$

Multipliquem i aïllem:

$$X^{p-1}C(X) = p\big(B(X)X^{p^2-p} + B(X)C(X) - A(X)\big).$$

Pel criteri d'Eisenstein, $P(X)$ és un polinomi irreductible sobre $\mathbb{Q}$ de grau p^2-p. Ara bé, $p^2 - p = p(p^2-1) = \big(2^r\times 3^s + 1\big)\times\big((2^r\times 3^s)^2 - 1\big) \neq 2^u\times 3^v$. D'acord amb el teorema 9.11 en resulta que $\tan\frac{360^\circ}{p^2}$ no és un nombre parabòlic. Això contradiu la hipòtesi segons la qual $\tan\frac{360^\circ}{p^2}$ era un nombre real parabòlic, atès que, com hem vist, $P(\tan\frac{360^\circ}{p^2}) = 0$.[100] □

100 Hi ha un camí més simple per fer-ho, usant les arrels primitives de $Z^n - 1 = 0$. Sabem que són arrels del polinomi irreductible $\Phi_n(X) = 0$ el grau del qual és $\varphi(n)$. Suposem que $n = 2^r\times 3^s\times p_1^{n_1}\times\cdots\times p_k^{n_k}$. Aleshores

$$\varphi(n) = 2^r\times 3^{s-1}\times p_1^{n_1-1}\times(p_1-1)\times\ldots p_k^{n_k-1}\times(p_k-1).$$

Perquè sigui un nombre parabòlic cal que $p_i^{n_i-1} = 1$, $i = 1,\ldots,k-1$. És a dir, $n_i = 1$, $i = 1,\ldots,k$. Nosaltres, no obstant això, hem adoptat el mètode exposat per N. D. Karanikoff perquè és més escolar i, per tant, entenedor fins i tot per a estudiants de batxillerat.

D'aquests resultats deduïm, com a simple corol·lari, el teorema general de Wantzel:

A.8 COROL·LARI (TEOREMA GENERAL DE WANTZEL) *Si un polígon regular de n costats és construïble amb papiroflèxia parabòlica, aleshores $n = 2^{m_1} \times 3^{m_2} \times p_1 \times \cdots \times p_k$, on els p_i, $i = 1, \ldots, k$, són primers parabòlics diferents.* □

A.9 COROL·LARI (TEOREMA DE WANTZEL) *Si un polígon regular de n costats és construïble amb papiroflèxia plana, aleshores $n = 2^{m_1} \times p_1 \times \cdots \times p_k$, on els p_i, $i = 1, \ldots, k$, són primers plans diferents.* □

A.2 Teorema de Gauss generalitzat a polígons regulars parabòlics

Ara, seguint les petjades de Gauss, volem veure que, si p és un nombre primer parabòlic, aleshores el polígon regular de p costats és construïble amb papiroflèxia parabòlica.

Per aconseguir-ho, observem en primer lloc que els vèrtexs del polígon regular de p costats són els afixos complexos de les solucions de l'equació polinòmica

$$Z^p - 1 = 0.$$

Si fem $z_1 = \cos\frac{360^\circ}{p} + i\sin\frac{360^\circ}{p}$, les $p-1$ arrels, diferents d'1, de l'equació anterior són:

$$z_k = z_1^k \cos\left(\frac{360^\circ}{p} \times k\right) + i\sin\left(\frac{360^\circ}{p} \times k\right), \quad k = 1, 2, \ldots, p-2, p-1.$$

Aleshores, si fem $z_{-k} = z_{p-k} = \cos\left(\frac{360^\circ}{p} \times (p-k)\right)$, en resulta que $Z_k = z_k + z_{-k} = 2\cos\left(\frac{360^\circ}{p} \times k\right) \in \mathbb{R}$ i, per tant, les Z_k són arrels reals d'un polinomi el grau del qual convé que sigui 2.

Aquestes observacions, juntament amb el corol·lari C.17, suggereixen a Gauss, en el cas en què p és un nombre primer de Fermat, reordenar les arrels z_k segons una altra llei d'índexs.

Per aconseguir-ho, Gauss recorre a una arrel primitiva ξ de la unitat.[101] Les potències successives ξ^k, $k = 1, \ldots, p-1$, li proporcionen tots els índexs, però en un ordre adequat per als seus objectius. És a dir, obté el conjunt

$$S = \left\{z_{\xi^1}, z_{\xi^2}, \ldots, z_{\xi^{\frac{p-1}{2}}}; z_{\xi^{\frac{p-1}{2}+1}}, \ldots, z_{\xi^{p-1}}\right\} =$$
$$= \left\{z_{\xi^1}, z_{\xi^2}, \ldots, z_{\xi^{\frac{p-1}{2}}}; z_{-\xi^1}, z_{-\xi^2}, \ldots, z_{-\xi^{\frac{p-1}{2}}}\right\},$$

que és del tipus de conjunts que analitzarem al corol·lari C.17.

Nosaltres volem multiplicar i elevar a una potència les arrels z_{ξ^k}. Això fa que l'única cosa que ens interessi sigui el comportament dels exponents, atès

101 Vegeu la definició C.15.

que al producte li corresponen sumes d'exponents, i a la potència, productes. Per aquesta raó ens referirem a z_{ξ^k} com a $[\xi^k]$ o, més breument, en lloc de z_h, escriurem $[h]$, on h és de la forma ξ^k. Aleshores $z_{h_1} \cdot z_{h_2} = z_{\xi^{k_1}} \cdot z_{\xi^{k_2}} = z_{\xi^{k_1+\xi^{k_2}}}$ serà $[h_1 + h_2]$, i $z_h^k = \left(z_{\xi^m}\right)^k = z_{\left(\xi^m\right)\cdot k}$ l'indicarem $[h \cdot k]$.

Per tal de fer més entenedors els raonaments d'aquesta secció, farem alguns exemples en els quals p serà un primer parabòlic.

EXEMPLE 1 Suposem que $p = 7$. Aleshores una arrel primitiva de la unitat mòdul 7 és 3. Tenim que

$$3^1 \equiv 3,\ 3^2 \equiv 2,\ 3^3 \equiv 6,\ 3^4 \equiv 4 \equiv -3,\ 3^5 \equiv 5 \equiv -2,\ 3^6 \equiv 1 \equiv -6 \pmod 7.$$

Per tant, $S = \{z_3, z_2, z_6; z_4, z_5, z_1\}$

$$= \{z_3, z_2, z_6; z_{-3}, z_{-2}, z_{-6}\} = \{[3], [2], [6]; [4], [5], [1]\}.$$

Considerem ara els conjunts S_1, S_2, S_3, que s'obtenen de S agafant els seus elements alternativament, un de cada tres, respectant l'ordre:

$$S_1 = \{[3], [4]\};\ S_2 = \{[2], [5]\};\ S_3 = \{[6], [1]\}.$$

Ara, dins d'aquests conjunts, n'agafem un de cada dos:

$$S_{11} = \{[3]\}, S_{12} = \{[4]\};\ S_{21} = \{[2]\}, S_{22} = \{[5]\};\ S_{31} = \{[6]\}, S_{32} = \{[1]\}.$$

Aleshores considerem les respectives sumes i productes dels elements:

$$\eta_1 = z_3 + z_4 = [3] + [4],\ \eta_2 = z_2 + z_5 = [2] + [5],\ \eta_3 = z_6 + z_1 = [6] + [1].$$

Atès que els productes $z_3 \cdot z_4 = [3] \cdot [4]$, etc., són tots iguals a $[0] = 1$, perquè són inversos, si podem determinar $\eta_i, i = 1, 2, 3$, en coneixerem les sumes i els productes i seran arrels de polinomis de segon grau. Tot rau, doncs, a veure si podem determinar els $\eta_i, i = 1, 2, 3$ com a arrels d'equacions polinòmiques cúbiques. Cal veure, doncs, quins són

$$\eta_1 + \eta_2 + \eta_3;\ \eta_1 \cdot \eta_2 + \eta_2 \cdot \eta_3 + \eta_3 \cdot \eta_1;\ \eta_1 \cdot \eta_2 \cdot \eta_3.$$

Calculem, doncs:

$$\begin{aligned} \eta_1 + \eta_2 + \eta_3 &= z_3 + z_2 + z_6 + z_4 + z_5 + z_1 \\ &= [3] + [2] + [6] + [4] + [5] + [1] = -1;^{102} \end{aligned}$$

$$\eta_1 \cdot \eta_2 = \left\{ \begin{matrix} [5] + [2] \\ [6] + [1] \end{matrix} \right\};\ \eta_2 \cdot \eta_3 = \left\{ \begin{matrix} [1] + [6] \\ [3] + [4] \end{matrix} \right\};\ \eta_3 \cdot \eta_1 = \left\{ \begin{matrix} [2] + [5] \\ [3] + [4] \end{matrix} \right\}.^{103}$$

102 És conseqüència del fet que $\sum_{i=0}^{6} z_i = 0$.

103 La clau és una forma breu de designar la suma. Així, $\left\{ \begin{matrix} [1] + [6] \\ [3] + [4] \end{matrix} \right\}$ és $[1] + [6] + [3] + [4]$.

Per tant,

$$\eta_1\cdot\eta_2+\eta_2\cdot\eta_3+\eta_3\cdot\eta_1=(\eta_2+\eta_3)+(\eta_3+\eta_1)+(\eta_3+\eta_1)=2(\eta_1+\eta_2+\eta_3)=-2.$$

Calculem ara:

$$\eta_1\cdot\eta_2\cdot\eta_3=\left\{\begin{array}{l}[4]+[3]\\ [6]+[1]\\ [0]+[0]\\ [2]+[5]\end{array}\right\}=(\eta_1+\eta_2+\eta_3)+2=1.$$

Les arrels de l'equació polinòmica cúbica $H^3+H^2-2H-1=0$ són η_1,η_2, i η_3, mentre que z_3,z_4; z_2,z_5; z_6,z_1 ho són, respectivament, de les equacions polinòmiques quadràtiques $Z^2-\eta_1Z+1=0$, $Z^2-\eta_2Z+1=0$, $Z^2-\eta_3Z+1=0$.

En definitiva, doncs, els afixos z_1,z_2,z_3,z_4,z_5 i z_6 són nombres complexos parabòlics.[104]

EXEMPLE 2 Suposem que $p=13$. Aleshores una arrel primitiva de la unitat mòdul 13 és 2. Per tant,

$$S=\{[2],[4],[8],[3],[6],[12];[11],[9],[5],[10],[7],[1]\}.$$

$$S_1=\{[2],[3];[11],[10]\};\qquad S_{11}=\{[2];[11]\},\qquad S_{12}=\{[3];[10]\}.$$

$$S_2=\{[4],[6];[9],[7]\};\qquad S_{21}=\{[4];[9]\},\qquad S_{22}=\{[6];[7]\}.$$

$$S_3=\{[8],[12];[5],[1]\};\qquad S_{31}=\{[8];[5]\},\qquad S_{32}=\{[12];[1]\}.$$

D'on
$$\left\{\begin{array}{lll}\eta_1=[2]+[3]+[11]+[10]; & \eta_{11}=[2]+[11], & \eta_{12}=[3]+[10].\\ \eta_2=[4]+[6]+[9]+[7]; & \eta_{21}=[4]+[9], & \eta_{22}=[6]+[7].\\ \eta_3=[8]+[12]+[5]+[1]; & \eta_{31}=[8]+[5], & \eta_{32}=[12]+[1].\end{array}\right.$$

Aleshores

$$\eta_1+\eta_2+\eta_3=-1;$$
$$\eta_1\cdot\eta_2=\left\{\begin{array}{l}[6]+[9]+[7]+[4]\\ [8]+[12]+[5]+[1]\\ [11]+[10]+[2]+[3]\\ [9]+[7]+[4]+[6]\end{array}\right\}=\eta_1+\eta_3+\eta_1+\eta_2.$$

Per tant, $\eta_1\cdot\eta_2+\eta_2\cdot\eta_3+\eta_3\cdot\eta_1=4(\eta_1+\eta_2+\eta_3)=4$.

104 Per les característiques ja indicades dels conjunts S,S_1,S_2 i S_3, és clar que $\eta_2\cdot\eta_3=(\eta_1\cdot\eta_2)\cdot 3,\eta_3\cdot\eta_1=(\eta_1\cdot\eta_2)\cdot 3^2$. Per tant, $\eta_1\cdot\eta_2+\eta_2\cdot\eta_3+\eta_3\cdot\eta_1=(\eta_1\cdot\eta_2)(1+3+3^2)$ formen una classe completa de complementaris. D'altra banda, $\eta_1\cdot\eta_2\cdot\eta_3=\eta_1+\eta_1\cdot 3+\eta_1\cdot 3^2$, $\eta_2\cdot\eta_3\cdot\eta_1=\eta_2+\eta_2\cdot 3+\eta_2\cdot 3^2=(\eta_1+\eta_1\cdot 3+\eta_1\cdot 3^2)\cdot 3$, $\eta_3\cdot\eta_1\cdot\eta_2=\eta_3+\eta_3\cdot 3+\eta_1\cdot 3^2=(\eta_1+\eta_1\cdot 3+\eta_1\cdot 3^2)\cdot 3^2$ i $\eta_1\cdot\eta_2\cdot\eta_3=\eta_2\cdot\eta_3\cdot\eta_1=\eta_3\cdot\eta_1\eta_2$. Per tant, és invariant enfront de l'arrel primitiva. És a dir, és una classe completa o la suma de classes completes. Consulteu el corol·lari C.17 i la definició C.18.

$$\eta_1\cdot\eta_2\cdot\eta_3=\left\{\begin{array}{llll}[1]+&[8]+&[12]+&[5]\\ [4]+&[6]+&[9]+&[7]\\ [2]+&[3]+&[11]+&[10]\\ [5]+&[1]+&[8]+&[12]\\ &&&\\ [3]+&[11]+&[10]+&[2]\\ [9]+&[7]+&[4]+&[6]\\ [0]+&[0]+&[0]+&[0]\\ [9]+&[7]+&[4]+&[6]\\ &&&\\ [6]+&[9]+&[7]+&[4]\\ [5]+&[1]+&[8]+&[12]\\ [10]+&[2]+&[3]+&[11]\\ [11]+&[10]+&[2]+&[3]\\ &&&\\ [4]+&[6]+&[9]+&[7]\\ [2]+&[3]+&[11]+&[10]\\ [12]+&[5]+&[1]+&[8]\\ [1]+&[8]+&[12]+&[5]\end{array}\right\}=5(\eta_1+\eta_2+\eta_3)-4=-1.$$

Per tant, η_1,η_2,η_3 són les arrels de la cúbica $H^3+H^2+4H+1=0$.

Aleshores $\eta_{i1}+\eta_{i2}=\eta_i$ i $\eta_{i1}\cdot\eta_{i2}=\eta_j$, on $j\equiv i+2 \pmod 4$. Per tant, cada $\eta_{ik}, k=1,2,3$, és l'arrel de $U^2-\eta_iU+\eta_j=0$, amb $i=1,2,3$. Però els η_{ik} són els nombres complexos $z_s, s=1,2,\ldots,z_{12}$.

EXEMPLE 3 Suposem que $p=19$. Aleshores una arrel primitiva de la unitat mòdul 19 és 2. Per tant,

$$\begin{aligned}S=\{&[2],[4],[8],[16],[13],[7],[14],[9],[18];\\ &[17],[15],[11],[3],[6],[12],[5],[10],[1]\},\end{aligned}$$

$$S_1=\{[2],[16],[14];[17],[3],[5]\}\ ;\quad\left\{\begin{array}{l}S_{11}=\{[2],[17]\},\\ S_{12}=\{[16],[3]\},\\ S_{13}=\{[14],[5]\}.\end{array}\right.$$

$$S_2=\{[4],[13],[9];[15],[6],[10]\}\ ;\quad\left\{\begin{array}{l}S_{21}=\{[4],[15]\},\\ S_{22}=\{[13],[6]\},\\ S_{23}=\{[9],[10]\}.\end{array}\right.$$

$$S_3=\{[8],[7],[18];[11],[12],[1]\}\ ;\quad\left\{\begin{array}{l}S_{31}=\{[8],[11]\},\\ S_{32}=\{[7],[12]\},\\ S_{33}=\{[18],[1]\}.\end{array}\right.$$

D'on:

$$\eta_1=[2]+[16]+[14]+[17]+[3]+[5]\ ;\quad\left\{\begin{array}{l}\eta_{11}=[2]+[17],\\ \eta_{12}=[16]+[3],\\ \eta_{13}=[14]+[5].\end{array}\right.$$

$$\eta_2 = [4] + [13] + [9] + [15] + [6] + [10]\,; \quad \begin{cases} \eta_{21} = [4] + [15], \\ \eta_{22} = [13] + [6], \\ \eta_{23} = [9] + [10]. \end{cases}$$

$$\eta_3 = [8] + [7] + [18] + [11] + [12] + [1]\,; \quad \begin{cases} \eta_{31} = [8] + [11], \\ \eta_{32} = [7] + [12], \\ \eta_{33} = [18] + [1]. \end{cases}$$

Aleshores

$$\eta_1 + \eta_2 + \eta_3 = -1; \quad \eta_1 \cdot \eta_2 + \eta_2 \cdot \eta_3 + \eta_3 \cdot \eta_1 = -6; \quad \eta_1 \cdot \eta_2 \cdot \eta_3 = -8$$

són les solucions de l'equació cúbica $H^3 + H^2 - 6H + 8 = 0$. Ara fem $\eta_{1i} = \theta_i, \eta_{2i} = \xi_i, \eta_{3i} = \sigma_i, i = 1, 2, 3$. Tenim que

$$\theta_1 + \theta_2 + \theta_3 = \eta_1; \quad \theta_1 \cdot \theta_2 + \theta_2 \cdot \theta_3 + \theta_3 \cdot \theta_1 = \eta_3 + \eta_1; \quad \theta_1 \cdot \theta_2 \cdot \theta_3 = \eta_2.$$

Són, doncs, les solucions de la cúbica $T^3 - \eta_1 T^2 + (\eta_3 + \eta_1)T - \eta_2 = 0$.

Els altres dos casos són anàlegs i s'obtenen per simple permutació.

Per fi, les tres parelles de nombres complexos conjugats z_2, z_{17}; z_{16}, z_3; z_{14}, z_5 són, respectivament, les arrels de les equacions quadràtiques $Z^2 - \theta_i Z + 1 = 0$, $i = 1, 2, 3$.

Per tant, les arrels complexes $z_1, \ldots, z_{18}$ són parabòliques, que és el que volíem.

* * *

Ara, un cop hem vist que els exemples funcionen i com funcionen, podem fer la demostració del cas general, que es basa en el que hem vist en aquests casos.

Suposem que $p = 2^r \times 3^s + 1$ és un nombre primer de Pierpont i que ζ és una arrel primitiva de la unitat mòdul p. Aleshores el conjunt

$$S = \left\{[k_0], [k_0 \cdot h_0], [k_0 \cdot h_0^2], [k_0 \cdot h_0^3], \ldots, [k_0 \cdot h_0^{p-3}], [k_0 \cdot h_0^{p-2}], [k_0 \cdot h_0^{p-1}]\right\},$$

on $k_0 = \zeta, h_0 = \zeta$, és el 0-conjunt. Els subconjunts

$$\begin{aligned} S_1 &= \left\{[k_1], [k_1 \cdot h_1^3] \ldots, [k_1 \cdot h_1^{f_1-4}]\right\}, \\ S_2 &= \left\{[k_1 \cdot h_1], [k_1 \cdot h_1^4] \ldots, [k_1 \cdot h_1^{f_1-3}]\right\}, \\ S_3 &= \left\{[k_1 \cdot h_1^2], [k_1 \cdot h_1^5] \ldots, [k_1 \cdot h_1^{f_1-2}]\right\}, \end{aligned}$$

on $k_1 = k_0$, $h_1 = h_0$ i $f = 1 + \frac{p-1}{3}$, són els tres 1-subconjunts ternaris de S. I, en general, si $S_{i_1 \cdots i_{m-1} j} = \left\{[k], [k \cdot h], [k \cdot h^2], [k \cdot h^3], \ldots, [k \cdot h^{f-3}], [k \cdot h^{f-2}]\right\}$, amb $i_k \in \{1, 2, 3\}$, és un m-conjunt ternari i el cardinal $f - 1$ és divisible per

3,[105] on $h = \zeta^{3^m}$ i $f := f_{m+1} = 1 + \frac{p-1}{3^m}$, considerem els tres $(m+1)$-conjunts ternaris

$$\begin{aligned}
T_1^{m+1} &= S_{i_1\cdots i_{m-1}j1} = \left\{[k], [k\cdot h^3]\ldots, [k\cdot h^{f-4}]\right\},\\
T_2^{m+1} &= S_{i_1\cdots i_{m-1}j2} = \left\{[k\cdot h], [k\cdot h^4]\ldots, [k\cdot h^{f-3}]\right\} = S_{i_1\cdots i_{m-1}j1} * h,\\
T_3^{m+1} &= S_{i_1\cdots i_{m-1}j3} = \left\{[k\cdot h^2], [k\cdot h^5]\ldots, [k\cdot h^{f-2}]\right\} =\\
&= S_{i_1\cdots i_{m-1}j2} * h = S_{i_1\cdots i_{m-1}j1} * h^2.
\end{aligned}$$

Aquí hem emprat la notació $S * t$ per a denotar el conjunt que s'obté de S multiplicant cada índex per t.

Aleshores considerem l'$(m+1)$-*període*:[106]

$$\eta_r^* = \eta_{i_1\cdots i_{m-1}jr} = \sum_{[t]\in S_{i_1\cdots i_{m-1}jr}} [t] = \left\{[k\cdot h^{r-1}], [k\cdot h^{r+2}], \ldots, [k\cdot h^{r+(f-5)}]\right\},$$

amb $r = 1, 2, 3$.

En resulta fàcilment que $\eta_1^* + \eta_2^* + \eta_3^* = \eta^* = \eta_{i_1\cdots i_{m-1}j}$, que és un m-període.

El problema rau a veure que $\eta_1^*\cdot\eta_2^* + \eta_2^*\cdot\eta_3^* + \eta_3^*\cdot\eta_1^*$ i $\eta_1^*\cdot\eta_2^*\cdot\eta_3^*$ són combinacions lineals amb coeficients enters de m-períodes més o menys un enter, on el 0-període val -1, perquè és la suma de totes les arrels complexes, no trivials, de $Z^p - 1 = 0$.

És clar que, si multipliquem el primer element de T_1^{m+1} per tots els de T_2^{m+1}, els col·loquem en columna i els sumem, després el segon element de T_1^{m+1} per tots els de T_2^{m+1}, els col·loquem en columna, el primer a baix de tot i després els altres des de dalt i els sumem, i així successivament començant cada cop a col·locar-los en una posició un lloc més elevat, obtindrem el conjunt $\eta_1^*\,\eta_2^*$ que és igual al conjunt

$$\left\{\begin{array}{rcccl}
[k+k\cdot h] + & [k\cdot h^3 + k\cdot h^4] & + \cdots + & [k\cdot h^{f-4} + k\cdot h^{f-3}] & +\\
[k+k\cdot h^4] + & [k\cdot h^3 + k\cdot h^7] & + \cdots + & [k\cdot h^{f-4} + k\cdot h] & +\\
[k+k\cdot h^7] + & [k\cdot h^3 + k\cdot h^{10}] & + \cdots + & [k\cdot h^{f-4} + k\cdot h^4] & +\\
\vdots & \vdots & & \vdots & \\
[k+k\cdot h^{f-6}] + & [k\cdot h^3 + k\cdot h^{f-3}] & + \cdots + & [k\cdot h^{f-4} + k\cdot h^{f-9}] & +\\
[k\cdot h^{f-4} + k\cdot h^{f-3}] + & [k\cdot h^{f-4} + k\cdot h] & + \cdots + & [k\cdot h^{f-4} + k\cdot h^{f-6}]. &
\end{array}\right\}$$

Els elements d'una fila s'obtenen multiplicant l'anterior per h^3; cada fila és, doncs, la suma d'un conjunt ternari d'ordre $(m+1)$, però no necessàriament els que s'han multiplicat.

105 Quan el cardinal sigui parell, no divisible per tres, tot funciona igual, amb complementaris binaris, com podem veure a [8, 106–114]. Així arribem a conjunts amb dos elements que són conjugats i permeten tancar tot el procés.

106 En virtut del corol·lari C.17, els períodes són nombres reals.

Ara bé, $T_2^{m+1} = T_1^{m+1} * h$ i $T_3^{m+1} = T_2^{m+1} * h = T_1^{m+1} * h^2$. Això fa que $\eta_2^* \cdot \eta_3^* = (\eta_1^* \cdot \eta_2^*) * h$, $\eta_3^* \cdot \eta_1^* = (\eta_2^* \cdot \eta_3^*) * h = (\eta_1^* \cdot \eta_1^*) * h^2$. Per tant, $\eta_1^* \cdot \eta_2^* + \eta_2^* \cdot \eta_3^* + \eta_3^* \cdot \eta_1^* = (\eta_1^* \cdot \eta_2^*) * (1 + h + h^2)$. Això significa que cada fila d'un producte $(m+1)$-ari va amb els seus dos complementaris ternaris. Per tant, les sumes $\eta_1^*, \eta_2^*, \eta_3^*$ dels tres conjunts conjugats ternaris d'ordre $(m+1)$, T_1^{m+1}, T_2^{m+1}, T_3^{m+1} hi són totes tres el mateix nombre a de vegades. Això fa que la suma η de tots tres —que correspon a la suma dels termes d'un conjunt ternari d'ordre $m, S_{i_1 \cdots i_{m-1} j}$— hi sigui a vegades, com volíem veure.[107]

D'altra banda, si analitzem el comportament de $\eta_1^* \cdot \eta_2^* \cdot \eta_3^*$, escrivint, com abans, les columnes, observem que cada fila s'obtené de l'anterior multiplicant-la per h^3, i la primera de la darrera atès que ζ és una arrel primitiva de la unitat mòdul p. Aleshores, observant que

$$(\eta_1^* \cdot \eta_2^* \cdot \eta_3^*) * h = \eta_2^* \cdot \eta_3^* \cdot \eta_1^*; \ (\eta_1^* \cdot \eta_2^* \cdot \eta_3^*) * h^2 = \eta_3^* \cdot \eta_1^* \cdot \eta_2^*,$$

en resulta que $\eta_1^* \cdot \eta_2^* \cdot \eta_3^*$ és invariant per h i h^2. Això significa, com abans,[108] que cada conjunt ternari de $(m+1)$ va acompanyat dels seus dos complementaris; per tant, si un conjunt ternari d'ordre $(m+1)$ hi és b vegades, el conjunt d'ordre m que l'ha generat també, tal com destjàvem.

Això acaba la demostració en el cas dels conjunts que són de cardinal divisible per tres; per als conjunts que són de cardinal parell-parell —en el sentit euclidià de la paraula—[109] tot va igual.[110] □

Com a corol·lari en resulta

---

107 Hom pot demostrar, seguint les petjades de [8, 111–112], que cap dels conjunts m —obtinguts per subdivisió en tres d'un d'ordre $(m-1)$— no correspon a la solució trivial $z_0 = 1$.

Suposem que el $(m-1)$-conjunt és $S^* = \left\{[k], [k \cdot h^2], \ldots, [k \cdot h^{f-2}]\right\}$, on $f = \frac{p-1}{3^{m-1}} + 1$. Per tant, $h^{f-1} = \left(\zeta^{3^{m-1}}\right)^{\frac{p-1}{3^{m-1}}} = \zeta^{p-1} \equiv 1 (\mathrm{mod}\ p)$, i tornem a començar amb el mateix conjunt.

Aleshores els conjunts ternaris conjugats són:

$$S_1^* = \left\{[k], [k \cdot h^3], \ldots, [k \cdot h^{f-4}]\right\},$$
$$S_2^* = \left\{[k \cdot h^2], [k \cdot h^4], \ldots, [k \cdot h^{f-3}]\right\},$$
$$S_3^* = \left\{[k \cdot h^2], [k \cdot h^5], \ldots, [k \cdot h^{f-2}]\right\}.$$

Cada fila del producte $\eta_1^* \cdot \eta_2^*$ anterior s'obté de l'anterior multiplicant-la per h^3. Per veure que cap exponent no és congruent amb zero, mòdul p, n'hi ha prou de fer-ho per als de la primera columna, que són de la forma $k + k \cdot 3^{i+j}$, on $j = 1, 2, 1 \leq 3i + j \leq f - 3$.

Així, doncs, si $k + k \cdot h^{3i+1} \equiv 0 (\mathrm{mod}\ p)$, tindríem que $h^{3i+j} \equiv -1 (\mathrm{mod}\ p)$. Per tant, $h^{6i+2j} \equiv 1 (\mathrm{mod}\ p)$. És a dir, $1 \equiv \zeta^{3^{m-1}(6i+2j)} (\mathrm{mod}\ p)$. D'on: $(p-1) \mid 3^{m-1}(6i + 2j)$. Ara bé,

$$3 \leq 6i + 2j \leq 6i + t \leq 3f - 8 \leq 3f - 3 = \frac{p-1}{3^{m-2}} - 3, \text{ amb } t = 3, 4.$$

Aleshores $3^{m-1}(6i + 2j) \leq 3(p-1) - 3^{m-1} < 3(p-1)$. D'on: $\lambda(p-1) = (3^{m-1})(6i+2) = 3^{m-1} \times 2 \times (3i+1) = 2^r \times 3^s$, $\lambda = 1, 2$. Impossible, atès que $m \leq s$.

108 Ara, però, hi pot haver productes que donin z_0, com veiem en els exemples.

109 És a dir, potències de 2.

110 Vegeu [8, 106–112].

A.10 COROL·LARI (TEOREMA GENERAL DE GAUSS) *Un polígon regular de p costats, on p és un nombre primer de Pierpont, és construïble amb papiroflèxia parabòlica.* □

Aquest resultat implica el teorema de Gauss.

A.11 COROL·LARI (TEOREMA DE GAUSS) *Un polígon regular de p costats, on p és un nombre primer de Fermat, és construïble amb papiroflèxia parabòlica.* □

En síntesi, doncs, hem vist que els polígons regulars de ≤ 100 costats es poden classificar de la manera següent:

Polígons construïbles amb papiroflèxia pitagòrica. Els polígons de n costats, amb $n = 3, 4, 6, 8, 12, 16, 24, 32, 48, 64, 96$.

Polígons construïbles amb papiroflèxia plana (a Grècia). Els polígons de n costats, amb $n = 5, 10, 15, 20, 30, 40, 60, 80$.

Polígons construïbles amb papiroflèxia plana (segons Gauss). Els polígons de n costats, amb $n = 17, 34, 51, 68, 85$.

Polígons construïbles amb papiroflèxia parabòlica. Els polígons de n costats, amb $n = 7, 9, 13, 14, 18, 19, 21, 26, 27, 28, 35, 36, 37, 38, 39, 42, 45, 52, 54, 56, 57, 63, 65, 70, 72, 73, 74, 76, 78, 81, 84, 90, 91, 95, 97$.

Això respon, a bastament, la pregunta de l'amic Ignasi Mundet i justifica aquest apèndix.

B Equivalència de dues papiroflèxies parabòliques

Ara veurem que hi ha equivalència entre la nostra papiroflèxia parabòlica i la papiroflèxia parabòlica en la qual l'operació $\mathbf{O}_2$ s'aplica a rectes ℓ i ℓ' perpendiculars, si se li afegeixen els plecs lineals; és a dir, els que proporciona l'operació $\mathbf{O}_1$.[111]

Volem establir que, en l'una i en l'altra, tenim els mateixos plecs de tipus $\mathbf{O}_2$. Per veure-ho considerarem les representacions *a*) i *b*) de la figura 30.

En *a*) disposem de la papiroflèxia parabòlica definida a la pàgina 122. Aleshores, donades dues rectes concurrents ℓ i ℓ', i dos punts P i Q, el plec $\mathfrak{p}$ que garanteix l'operació $\mathbf{O}_2$ admet la recta perpendicular $\overleftrightarrow{PP^{\mathfrak{p}}}$ —atès que, com hem vist a la proposició 9.5, disposem de la papiroflèxia plana—, la qual determina el punt parabòlic $P^{\mathfrak{p}}$. Tirem la perpendicular ℓ'' a la recta ℓ que passa per $P^{\mathfrak{p}}$ i resulta que el plec $\mathfrak{p}$ correspon a les dues rectes perpendiculars ℓ i ℓ'', i als punts P i Q.

Suposem ara, com en *b*), que l'operació $\mathbf{O}_2$ s'aplica a les rectes perpendiculars ℓ i ℓ', i als punts P i Q. S'obté el plec $\mathfrak{p}$. Aleshores, si també disposem dels plecs lineals, disposem del regle i, per tant, podem fer la perpendicular a ℓ' que passa per P. Aquesta recta determina amb ℓ' el punt $P^{\mathfrak{p}}$. La recta ℓ, a

111 És la papiroflèxia parabòlica que defineix Martin a [12, 151].

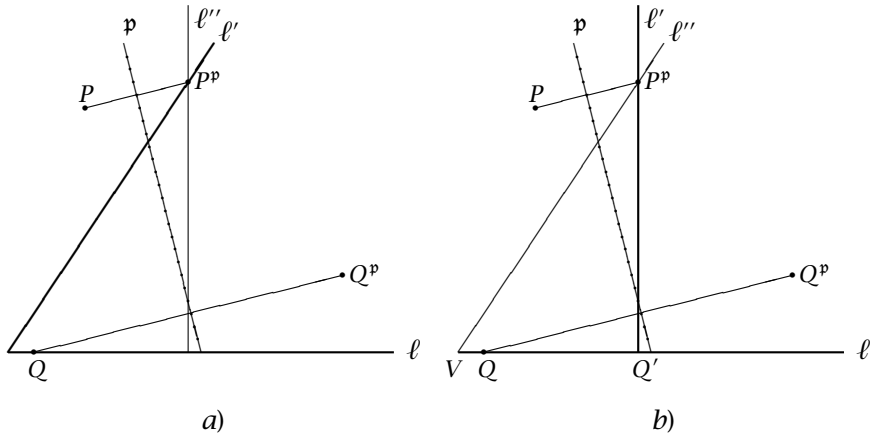


FIGURA 30

banda del peu Q' de ℓ' sobre ℓ, té un altre punt V —que podem agafar igual a Q o no, sempre que sigui un punt ja construït. Ara, amb el regle, els unim i obtenim la recta ℓ'' que talla ℓ, però sense ser-li perpendicular. Per tant, el plec $\mathfrak{p}$ correspon a les rectes ℓ i ℓ'', no ortogonals, i als punts P i Q, tal com volíem. □

Com a exemple d'aquesta equivalència donem una trisecció de l'angle, alternativa a la del teorema 9.2. Suposem que C, O i B són tres punts donats que formen un angle agut $\angle BOC$ (figura 31). Sigui M el punt mitjà del segment $\overline{OC}$. Sigui ℓ la perpendicular des de M a la recta $\overleftrightarrow{OB}$, i ℓ' la recta perpendicular a ℓ que passa per M.

Considerem una recta $\mathfrak{p}$ tal que $C' = C^{\mathfrak{p}} \in \ell$, $O' = O^{\mathfrak{p}} \in \ell'$. La recta $\overleftrightarrow{OO'}$ talla ℓ en el punt U. Aleshores, els triangles $\triangle CMC'$ i $\triangle OMU$ són iguals, i $\overline{MC} = \overline{MO}$. Per tant, $\overline{C'M} = \overline{MU}$. Però els triangles $\triangle C'MO' = \triangle UMO'$ són iguals. Per tant, $\angle C'O'M = \angle MO'O = \angle O'OC'$. Ara bé, $\angle C'O'O = \angle COO'$, atès que $\mathfrak{p}$ és un eix de simetria i, per tant, $\overline{LO'} = \overline{LO}$, on L és el punt en què $\mathfrak{p}$ talla el costat OC de l'angle donat. D'on $\angle MOO' = 2\,\angle OO'B$.

El teorema val també per a angles obtusos, atès que l'angle recte és trisecable. □

C Resultats algèbrics i aritmètics

D'entrada recordarem, de manera breu i sintètica, alguns resultats generals d'àlgebra relatius a les extensions de cossos, ben coneguts.[112]

En aquest apartat el cos base serà el cos $\mathbb{Q}$ i establirem les definicions i els resultats ben coneguts següents:

112 El lector interessat a aprofundir-los pot consultar [8] o bé [18].

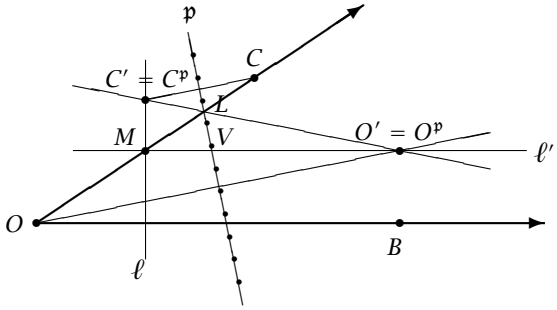


FIGURA 31

C.1 DEFINICIÓ *Un nombre real α és* algèbric sobre $\mathbb{Q}$ *si, i només si, és el zero d'un polinomi $P(X) = a_0 + a_1X + \ldots + a_nX^n$ de $\mathbb{Q}[X]$; és a dir, si, i només si, existeixen nombres racionals $a_0, a_1, a_2, \ldots, a_{n-1}, a_n \in \mathbb{Q}$, amb $a_n \neq 0$ i $n \geq 1$, tal que*

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

Altrament, diem que α és transcendent.

C.2 TEOREMA *Si $\alpha \in \mathbb{R}$ (o $\alpha \in \mathbb{C}$) és un nombre algèbric sobre $\mathbb{Q}$, existeix un polinomi* mònic irreductible *$M_\alpha(X) \in \mathbb{Q}[X]$ tal que $M_\alpha(\alpha) = 0$.*

A més, si $F(X) \in \mathbb{Q}[X]$ és un polinomi que compleix $F(\alpha) = 0$, aleshores $F(X)$ és un múltiple de $M_\alpha(X)$. I, recíprocament, per a tot múltiple $F(X)$ de $M_\alpha(X)$, $F(\alpha) = 0$.

DEMOSTRACIÓ Atès que α és un nombre algèbric sobre $\mathbb{Q}$, existeix un polinomi $P(X) \in \mathbb{Q}[X]$, de grau $n \geq 1$, amb $a_n \neq 0$, tal que $P(\alpha) = 0$. Agafem-ne un de grau mínim i dividim-lo per a_n. Obtenim el polinomi mònic *minimal* $M_\alpha(X)$ tal que $M_\alpha(\alpha) = 0$.

Òbviament és irreductible perquè, si no ho fos, hi hauria un altre polinomi mònic de grau més petit $N(X)$ que compliria $M_\alpha(X) = N(X)Q(X)$, amb $\operatorname{gr}(Q(X)) \geq 1$ i, per tant, $\operatorname{gr}(N(X)) \leq \operatorname{gr}(M_\alpha(X))$.

Si $F(X) \in \mathbb{Q}[X]$ és un polinomi que compleix $F(\alpha) = 0$, aleshores considerem la divisió:

$$F(X) = M_\alpha(X)Q(X) + R(X), \text{ amb } \operatorname{gr}(R(X)) < \operatorname{gr}(M_\alpha(X)).$$

Aleshores $R(\alpha) = 0$. Impossible.

La darrera afirmació és trivial. □

C.3 DEFINICIÓ *Sigui α un nombre algèbric sobre $\mathbb{Q}$. El polinomi mònic irreductible $M_\alpha(X)$ del teorema anterior l'anomenarem el* polinomi relatiu a α *o* polinomi minimal de α.

C.4 DEFINICIÓ *El* grau *d'un nombre algèbric α sobre $\mathbb{Q}$, $gr_{\mathbb{Q}}(\alpha)$, és el grau del polinomi M_α relatiu a α. És a dir, $gr_{\mathbb{Q}}(\alpha) = gr(M_\alpha(X))$.*

Amb aquestes definicions podem enunciar el corol·lari següent del teorema C.2:

C.5 COROL·LARI *Si α és un nombre algèbric de grau n i $\sum_{j=0}^{n-1} a_j \alpha^j = 0$, aleshores $a_j = 0$, $j = 0, 1, \ldots, n$. Dit altrament, els nombres $1, \alpha, \alpha^2, \ldots, \alpha^{n-2}, \alpha^{n-1}$ són linealment independents sobre $\mathbb{Q}$.* □

C.6 TEOREMA *Si α és un nombre algèbric sobre $\mathbb{Q}$, aleshores*

$$\mathcal{K}(\alpha) = \{F(\alpha) \colon F(X) \in \mathbb{Q}[X]\}$$

és un cos.

DEMOSTRACIÓ És clar que $0 = 0 \cdot \alpha^0$, $1 = 1 \cdot \alpha^0$.

La suma $S(X)$, la diferència $D(X)$ i el producte $P(X)$ de dos polinomis de $F_1(X), F_2(X) \in \mathbb{Q}[X]$ són, respectivament, polinomis de $\mathbb{Q}[X]$.

Sigui, doncs, $F(X) \in \mathbb{Q}[X]$ tal que $F(\alpha) \neq 0$. Hem de veure que $\frac{1}{F(\alpha)} \in \mathcal{K}(\alpha)$.

Atès que $F(\alpha) \neq 0$, d'acord amb el teorema C.2, $F(X)$ no és múltiple de $M_\alpha(X)$, on $M_\alpha(X)$ és el polinomi relatiu a α. Per tant, per la identitat de Bézout, aplicada a polinomis,

$$1 = F(X) \cdot U(X) + M_\alpha(X) \cdot V(X).$$

Substituïm X per α. Obtenim

$$1 = F(\alpha) \cdot U(\alpha) + M_\alpha(\alpha) \cdot V(\alpha) = F(\alpha) \cdot U(\alpha).$$

D'on $\frac{1}{F(\alpha)} = U(\alpha)$. Existeix, doncs, un polinomi $U(X) \in \mathbb{Q}[X]$ tal que $\frac{1}{F(\alpha)} = U(\alpha)$ i, per tant, $\frac{1}{F(\alpha)} \in \mathcal{K}(\alpha)$. □

C.7 PROPOSICIÓ *El cos $\mathcal{K}(\alpha)$ del teorema anterior és el cos generat per α sobre $\mathbb{Q}$; és a dir, és el més petit subcòs de $\mathbb{R}$ (o de $\mathbb{C}$) que conté α i $\mathbb{Q}$.*

DEMOSTRACIÓ D'una banda, tot subcòs K de $\mathbb{R}$ (o de $\mathbb{C}$), que conté α i $\mathbb{Q}$, conté $\mathcal{K}(\alpha)$, perquè conté totes les expressions de la forma $a_0 + a_1\alpha + \cdots + a_n\alpha^n$. D'altra banda, el cos $\mathcal{K}(\alpha)$ conté α i $\mathbb{Q}$. □

C.8 DEFINICIÓ *Un* cos algèbric *és un cos $\mathcal{K}(\alpha)$ generat per un nombre algèbric α.*

C.9 DEFINICIÓ *Sigui $\mathcal{K}(\alpha)$ el cos algèbric generat per α. El* grau de $\mathcal{K}(\alpha)$ *és $gr_{\mathbb{Q}}(\alpha)$.*

C.10 PROPOSICIÓ *Sigui α un nombre algèbric sobre $\mathbb{Q}$ de grau n. Aleshores el conjunt*

$$\mathcal{B} = \left\{1, \alpha, \alpha^2, \ldots, \alpha^{n-2}, \alpha^{n-1}\right\}$$

és una base de $\mathcal{K}(\alpha)$ com a espai vectorial sobre $\mathbb{Q}$.

DEMOSTRACIÓ Si $F(\alpha) \in \mathcal{K}(\alpha)$ i $M_\alpha(X)$ és el polinomi relatiu a α, aleshores

$$F(X) = M_\alpha(X)Q(X) + R(X), \text{ amb } \operatorname{gr}\big(R(X)\big) < \operatorname{gr}\big(M_\alpha(X)\big).$$

Aleshores,

$$F(\alpha) = M_\alpha(\alpha)Q(\alpha) + R(\alpha), \text{ amb } M_\alpha(\alpha) = 0.$$

D'on $F(\alpha) = R(\alpha)$ i $\operatorname{gr}\big(R(X)\big) < \operatorname{gr}\big(M_\alpha(X)\big) = n$. □

C.11 TEOREMA *Si $\mathcal{B} = \{1, \alpha, \alpha^2, \ldots, \alpha^{n-2}, \alpha^{n-1}\}$ és una base sobre $\mathbb{Q}$ —és a dir, n nombres de $\mathbb{R}$ (o de $\mathbb{C}$) linealment independents—, aleshores l'espai vectorial sobre $\mathbb{Q}$, generat per $\mathcal{B}$, és $\mathcal{K}(\alpha)$.*

DEMOSTRACIÓ L'expressió

$$\alpha^n = a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}$$

proporciona un polinomi mònic amb coeficients en $\mathbb{Q}$ i no hi ha cap més polinomi $F(X) \in \mathbb{Q}[X]$, de grau més petit, que faci $F(\alpha) = 0$, atès que, d'acord amb el corol·lari C.5, els nombres $1, \alpha, \alpha^2, \ldots, \alpha^{n-2}, \alpha^{n-1}$ són linealment independents. □

C.12 LEMA *Si E és un cos que alhora és un espai vectorial sobre un cos K de dimensió finita m i K és un espai vectorial sobre un cos k de dimensió finita n, aleshores E és un espai vectorial sobre k de dimensió finita $m \times n$.*

DEMOSTRACIÓ És un exercici d'àlgebra lineal. □

Acabem amb un lema que hem usat reiteradament en el text:

C.13 LEMA *Suposem que α és un nombre algèbric construïble, $\mathcal{K}(\alpha)$ és el cos algèbric engendrat per α i K és una extensió parabòlica iterada de $\mathbb{Q}$ que conté α. Aleshores existeix un subconjunt finit $\mathcal{B} = \{v_1, \ldots, v_n\}$ tal que*

i) $\mathcal{B} = \{v_1, \ldots, v_n\}$ són linealment independents sobre $\mathcal{K}(\alpha)$, i

ii) cada element de K es pot expressar com una combinació lineal d'elements de $\mathcal{B}$ amb coeficients en $\mathcal{K}(\alpha)$.

DEMOSTRACIÓ Distingim dues possibilitats: 1) Si la base de K sobre $\mathbb{Q}$ és formada per elements que són linealment independents sobre $\mathcal{K}(\alpha)$,[113] hem acabat. 2) Si no ho són, considerem $\{v_1\} \in \mathcal{B}$. És clar que $a \cdot v_1 = 0$, amb $a \in \mathcal{K}(\alpha)$, implica, multiplicant per l'invers $\frac{1}{v_1}$ de l'element no nul v_1, $a = \sum_{j=0}^{n-1} \lambda_j \alpha^j = 0$, amb $\lambda_j \in \mathcal{K}(\alpha)$. Aleshores $\lambda_j = 0$, per a tot $j = 0, \ldots, n-1$. Per tant, $a = 0$.

113 La base existeix perquè cada extensió parabòlica és generada per un polinomi irreductible de grau ≤ 4.

Sigui ara $m \geq 1$ el màxim nombre d'elements de $\mathcal{B}$ que són linealment independents sobre $\mathcal{K}(\alpha)$. Sigui, doncs, $\mathcal{B}^* = \{v_1, \ldots . v_m\}$ un conjunt màxim d'elements de $\mathcal{B}$ linealment independents sobre $\mathcal{K}(\alpha)$.

Volem veure que tot element $e \in K$ és una combinació lineal de $v_1, \ldots, v_m$ sobre $\mathcal{K}(\alpha)$. Per aconseguir-ho, agafem un element $e \in \mathcal{B}$, tal que $e \notin \mathcal{B}^*$. Aleshores els elements de $\mathcal{B} \cup \{e\}$ són linealment dependents sobre $\mathcal{K}(\alpha)$. És a dir, existeixen $a_1, \ldots, a_m, a \in \mathcal{K}(\alpha)$, no tots nuls, que

$$\sum_{j=1}^{m} a_j v_j + ae = 0, \text{ amb } e \neq 0.$$

D'on resulta que $e = -\sum_{j=1}^{n} \frac{a_j}{a} v_j$.

Finalment, atès que tot element $e \in K$ és una combinació lineal sobre $\mathbb{Q}$ de $\{v_1, \ldots, v_m, e_1, \ldots, e_r\}$, resulta que

$$e = \sum_{j=1}^{m} \lambda_j v_j + \sum_{k=1}^{r} \mu_k e_k = \sum_{j=1}^{m} \lambda_j v_j + \sum_{k=1}^{r} \mu_k \sum_{j=1}^{n} \frac{a_{kj}}{a_k} v_j.$$

Això acaba la demostració. □

C.14 Corol·lari *En resulta que* $[K : \mathbb{Q}] = [K : \mathcal{K}(\alpha)] \times [\mathcal{K}(\alpha) : \mathbb{Q}]$. □

* * *

Ara establim un teorema de Gauss que hem necessitat a A.2. Abans, però, una definició:

C.15 Definició *Una* arrel primitiva ξ de la unitat mòdul p *és un nombre* $1 < \xi \leq p - 1$ *que compleix* $\xi^{p-1} \equiv 1 (\text{mod } p)$ *mentre que, per a tot* $0 < k < p - 1$, $\xi^{p-1} \not\equiv 1 \pmod{p}$.

C.16 Teorema *Si* p *és un nombre primer, existeix una arrel* p*-èsima primitiva* ξ *de la unitat mòdul* p.[114]

Demostració Fem la segona de les demostracions originals de Carl Friedrich Gauss (1777–1855).[115] Suposem que $p - 1 = q_1^{m_1} q_2^{m_2} \cdots q_k^{m_k}$, on $q_1, \ldots, q_k$ són nombres primers diferents.

El polinomi X^{r_1}, amb $r_1 = \frac{p-1}{q_1}$, té el grau $< p - 1$. Per tant, pel teorema de Joseph-Louis Lagrange (1736–1813),[116] l'equació polinòmica diofàntica $X^{r_1} \equiv 1 \pmod{p}$ té, com a màxim, r_1 arrels del conjunt dels residus principals $\{1, 2, \ldots, p-2, p-1\}$. Això garanteix l'existència d'un nombre $\eta \in \{1, 2, \ldots,$

114 Si p no és primer, no podem pas garantir-ne l'existència.

115 Com diu Gauss: «és més comprensible que no pas la primera» (vegeu [6, 52–53]).

116 És fàcil demostrar-lo per inducció.

$p-2, p-1\}$ tal que $\eta^{r_1} \not\equiv 1 \pmod{p}$. Considerem ara $\xi \equiv \eta^{s_1}$, amb $s_1 = \frac{p-1}{q_1^{m_1}}$. És clar que

$$\xi^{q_1^{m_1}} \equiv \eta^{s_1 \cdot q_1^{m_1}} \equiv \eta^{p-1} \equiv 1 \pmod{p}.$$

D'altra banda,

$$\xi^{q_1^{m_1-1}} \equiv \eta^{\frac{p-1}{q_1}} = \eta^{r_1} \not\equiv 1 \pmod{p}.$$

En resulta que, per a tot nombre $1 < i < m_1$,

$$\xi^{q_1^{m_1-i}} \not\equiv 1 \pmod{p}.$$

Ara, per a cada q_j, agafem el corresponent ξ_j. És clar que $\xi = \xi_1 \cdots \xi_k$ satisfà l'equació polinòmica diofàntica $X^{p-1} \equiv 1 \pmod{p}$.

Sigui ara un t, amb $1 \leq t < p-1$, tal que $\xi^t \equiv 1 \pmod{p}$. Aleshores, $t \mid (p-1)$. Per tant, $\frac{p-1}{t} > 1$. Suposem que $q_j \mid \frac{p-1}{t}$. Aleshores, $t \mid \frac{p-1}{q_j}$. Per tant, $\xi^{\frac{p-1}{q_j}} \equiv 1 \pmod{p}$.

D'altra banda,

$$\xi^{\frac{p-1}{q_j}} = \xi_1^{\frac{p-1}{q_j}} \cdots \xi_j^{\frac{p-1}{q_j}} \cdots \xi_k^{\frac{p-1}{q_j}} \equiv \xi_j^{\frac{p-1}{q_j}} \not\equiv 1 \pmod{p}.$$

Aquesta contradicció acaba la demostració.[117] □

C.17 COROLLARI *Si p és un nombre primer i ξ una arrel p-èsima primitiva de la unitat mòdul p, aleshores el conjunt*

$$\left\{\xi, \xi^2, \xi^3, \ldots, \xi^{\frac{p-1}{2}}, \xi^{\frac{p-1}{2}+1}, \ldots, \xi^{p-2}, \xi^{p-1}\right\}$$

conté un sistema complet de residus no nuls.

A més, és simètric, atès que $\xi^{\frac{p-1}{2}} \equiv -1 \pmod{p}$ i, per tant, és de la forma

$$\left\{\xi, \xi^2, \xi^3, \ldots, \xi^{\frac{p-1}{2}}, -\xi, -\xi^2, \cdots, -\xi^{\frac{p-1}{2}}\right\}.$$

En conseqüència, si $p = 2^r \times 3^s + 1$ i considerem els conjunts que s'obtenen agafant-ne alternativament un de cada tres, o un de cada dos, de manera iterada, obtenim també conjunts simètrics.

DEMOSTRACIÓ Suposem que $p = 2^r \times 3^s + 1$ i fem

$$S = \left\{\xi, \xi^2, \xi^3, \ldots, \xi^{\frac{p-1}{2}}, -\xi, -\xi^2, \ldots, -\xi^{\frac{p-1}{2}}\right\}.$$

Aleshores, agafant-ne alternativament un de cada tres, tenim els tres *conjunts conjugats*:

$$S_1 = \left\{\xi, \xi^4, \ldots, \xi^{2^{r-1}\times 3^s - 2}, -\xi, -\xi^4, \ldots, -\xi^{2^{r-1}\times 3^s - 2}\right\},$$

117 Si fos congruent amb 1, $q_j^{m_j} \mid \frac{p-1}{q_j}$. Impossible.

$$S_2 = \left\{\xi^2, \xi^5, \ldots, \xi^{2^{r-1}\times 3^s-1}, -\xi^2, -\xi^5, \ldots, -\xi^{2^{r-1}\times 3^s-1}\right\},$$
$$S_3 = \left\{\xi^3, \xi^6, \ldots, \xi^{2^{r-1}\times 3^s}, -\xi^3, -\xi^5, \ldots, -\xi^{2^{r-1}\times 3^s}\right\}.$$

Cada un d'aquests conjunts és com el conjunt inicial —i, per tant admet tres conjugats—, mentre el seu cardinal sigui múltiple de tres. Quan això no sigui així, el cardinal serà de la forma 2^r. Aleshores els *conjunts conjugats* s'obtenen agafant-ne un element de cada dos. Si el conjunt en qüestió l'anomenem S^* i suposem que $p = 2^r$, s'obtenen els dos conjunts:

$$S_1^* = \left\{\xi, \xi^3, \ldots, \xi^{2^{r-1}-1}, -\xi, -\xi^3, \ldots, -\xi^{2^{r-1}-1}\right\},$$
$$S_2^* = \left\{\xi^2, \xi^4, \ldots, \xi^{2^{r-1}}, -\xi^2, -\xi^4, \ldots, -\xi^{2^{r-1}-1}\right\}.$$

Això acaba la demostració. □

C.18 DEFINICIÓ *Cada un dels tres subconjunts S_1, S_2, S_3 del conjunt S, quan $p = 2^r \times 3^s, s \geq 1$, l'anomenarem un* subconjunt ternari *de S i direm que S_1, S_2, S_3 són* conjunts ternaris conjugats.

Cada un dels subconjunts S_1, S_2 del conjunt S, quan $p = 2^r$, l'anomenarem un subconjunt binari *de S i direm que S_1, S_2 són* conjunts binaris conjugats.

Observem, per acabar, que cada un d'aquests s'obté de l'anterior multiplicant-lo pel primer element del primer dels subconjunts ternaris o binaris. Això aclareix els punts que quedaven una mica inexplicats a A.2 perquè forneixen els teoremes algèbrics i la nomenclatura necessaris per aclarir-los.

D Noms propis

BOMBELLI, RAFAEL Bolonya, Itàlia, gener de 1526 – Roma, (probablement) en 1572.

DESCARTES, RENÉ La Haye (avui Descartes), Touraine, França, 31 de març de 1596 – Estocolm, Suècia, 11 de febrer de 1650.

EISENSTEIN, FERDINAND GOTTHOLD MAX Berlín, 16 d'abril de 1823 – Berlín, 11 d'octubre de 1852.

FERMAT, PIERRE DE Beaumont de Lomages, 17 d'agost de 1601 – Castres, 12 de gener de 1665.

GAUSS, CARL FRIEDRICH Brunswick, 30 d'abril de 1777 – Göttingen, 23 de febrer de 1855.

HIPÒCRATES DE QUIÓS Quiós, Grècia, ~470 aC – Quiós (?), Grècia, ~410 aC.

LAGRANGE, JOSEPH-LOUIS Torí, Itàlia, 25 de gener de 1736 – París, 10 d'abril de 1813.

PIERPONT, JAMES Matemàtic austríac, doctorat el 1894 (no s'en coneixen més dades).

PLATÓ Atenes, 427 aC – Atenes, 347 aC.

RUFFINI, PAOLO Valentano, 22 de setembre de 1765 – Mòdena, 10 de maig de 1822.

VIÈTE, FRANÇOIS Fontenay-le-Compte, Poitou, França, 1540 – París, França, 13 de desembre de 1603.

WANTZEL, PIERRE-LAURENT París, França, 5 de juny de 1814 – París, França, 21 de maig de 1848.

Referències

[1] Bombelli, R. *L'algebra parte maggiore dell'aritmetica...* Bolonya, 1572. Reeditat l'any 1929.

[2] Carrega, J.-C. *Théorie des corps: La règle et le compas*. París: Hermann, 1981. Reeditat l'any 1989.

[3] Descartes, R. *Le discours de la méthode*. Leiden: 1637. Traducció catalana i edició a cura de P. Lluís Font: *El discurs del mètode*. Barcelona: Edicions 62, 1996.

[4] Descartes, R. *La géométrie*. Leiden: 1637. Traducció catalana a cura de J. Pla i P. Viader: «La geometria». Barcelona: Institut d'Estudis Catalans: Pòrtic: Eumo, 1999.

[5] Euclides *Elements*, a [19, i, 702–980].

[6] Gauss, C. F. *Disquisitiones arithmeticae*. Leipzig: Fleischer, 1801. Traducció catalana i edició a cura de Griselda Pascual: *Disquisicions aritmètiques*. Barcelona: Societat Catalana de Matemàtiques, 1996.

[7] Gleason, Andrew M. «Angle trisection, the heptagon, and the triskaidecagon». *American Mathematical Montly*, 95 (1988), 185–194.

[8] Hadlock, C. R. *Field theory and its classical problems*. Mathematical Association of America, Carus Mathematical Monographs; 19. 1978.

[9] Heath, Sir T. *The history of greek mathematics*. Canadà: General Publishing Company, Ltd., 1921. Reeditat a Dover Publications, Inc., en dos volums. Nova York, 1981.

[10] Hollingsdale, S. *Makers of mathematics*. Londres: Penguin Books, 1989.

[11] Karanikoff, N. D. *Ruler and the round or angle trisection and circle division*. Boston: Prindle, Weber & Schmidt, 1970. Reeditat amb el títol *Ruler and the round: Classic problems in geometric constructions*. Nova York: Dover Publications, Inc., 2003.

[12] Martin, G. E. *Geometric constructions*. Nova York: Springer, 1991.

[13] Pappos d'Alexandria. iii *Collecció Matemàtica*. A: [19, ii, 919–1018].

[14] Pierpont, J. «On an undemonstrated theorem of the Disquisitiones Arithmeticæ». *Bulletin of the American Mathematical Society*, 2 (1985), 77–83.

[15] Rey Pastor, J.; Babini, J. *Historia de la matemática*. Buenos Aires: Espasa-Calpe, 1951. Reeditat en dos volums. Barcelona: Gedisa, 1985.

[16] Row, T. S. *Geometrical exercices in paper folding*. Madràs: 1893. Traducció anglesa de W. W. Beman i D. E. Smith. Chicago, 1901. Reeditat a Nova York: The Open Court Publishing Company, 1905. També a Nova York: Dover Publications, Inc., 1966.

[17] Smith, D. E. *History of mathematics*. Canadà: General Publishing Company, 1925. Reeditat en dos volums. Nova York: Dover Publications, Inc., 1958.

[18] Stillwell, J. *Elements of algebra: Geometry, numbers, equations*. Nova York: Springer-Verlag, 1991.

[19] Vera, F. *Los científicos griegos*. Madrid: Aguilar, 1960.

[20] Viète, F. «De æquationum recognitione et mendatione», 1591. *Opera Mathématica*. [París], (1646), 82–162. Reeditat a Nova York, Georg Olms Verlag, 1970. Traducció anglesa a [23, 159–310].

[21] Viète, F. «Supplementum geometriæ», 1593. *Opera Mathématica*. [París], (1646), 240–257. Reeditat a Nova York: Georg Olms Verlag, 1970. Traducció anglesa a [23, 159–310].

[22] Wantzel, P.-L. «Recherches sur le moyens de reconnaître si un problème de géométrie peut se resoudre avec la règle et le compas». *Journal de Mathématiques*, 2 (1837), 366–372.

[23] Witmer, R. T. *The analytic art*. Ohio, Kent: Kent State University Press, 1983.

[24] Yates, R. C. *Geometrical tools, a mathematical sketch and model book*. Saint Louis: Educational Publishers, 1949.

Departament de Probabilitat, Lògica i Estadística
Facultat de Matemàtiques,
Universitat de Barcelona
Gran Via de les Corts Catalanes 585,
08007 Barcelona
jpla@ub.edu