Gauss i el polígon de 17 costats

Agustí Reventós*

1 Introducció històrica

Comencem reproduint les paraules que Gauss utilitza en una carta al seu amic Gerling, el 6 de gener de 1819, per explicar-li com va descobrir la possibilitat de construir el polígon regular de disset costats amb regle i compàs. Es veu clarament, en aquesta redacció, la molta estima en que Gauss tenia aquest resultat, el primer dels seus que va veure publicat.

> *La història d'aquest descobriment no l'he explicat enlloc fins ara, però puc indicar-la exactament.*
>
> *Va ser el* 29 *de març de* 1796*, i la casualitat no hi va tenir res a veure. Tot estava en dividir les arrels de l'equació*
>
> $$\frac{x^p - 1}{x - 1} = 0$$
>
> *en dos grups [...]*
>
> *A partir d'esforçades meditacions entre les connexions de les arrels i els fonaments de l'aritmètica, feliç per unes vacances a Braunschweig, el matí d'aquell dia, abans de llevar-me, vaig tenir la sort de veure amb gran claredat tota aquesta correlació, de manera que allà mateix i immediatament vaig aplicar a l'heptadecàgon la corresponent confirmació numèrica.*

El resultat va ser enunciat a la columna *Neue Entdeckungen* (Nous descobriments) de *Intellegenzblatt der allgemeinen Litteraturzeitung*, l'1 de Juny de 1796, per A. W. Zimmermann, professor de Gauss al Collegium Carolinum de Braunschweig. Reproduïm l'escrit de Gauss i la presentació de Zimmermann.

> *Com tot principiant en geometria sap, hi ha diversos polígons regulars, per exemple, el triangle, tetràgon, pentàgon,* 15*-gon, i aquells que s'obtenen doblant el nombre de costats d'algun d'ells, que són geomètricament construïbles.*
>
> *Això ja se sabia des del temps d'Euclides, i sembla que s'ha dit des de llavors que el camp de la geometria elemental no va més enllà: almenys jo no conec cap intent reeixit d'estendre els seus límits en aquesta direcció.*

*Nota basada en la conferència pronunciada en el marc del *Dissabte Transfonterer de les Matemàtiques a l'Alt Empordà*, organitzat per les Fundacions Príncep d'Astúries i Ferran Sunyer i Balaguer, Figueres, 1 Febrer 2014.

Amb més raó, el descobriment mereix atenció... que a part d'aquells polígons regulars n'hi ha d'altres, per exemple el 17*-gon, que es poden construir geomètricament. Aquest descobriment és, en realitat, només un cas especial d'una teoria més general, encara no completada, i que es presentarà al públic tan bon punt ho sigui.*[1]

Carl Friedrich Gauss

Estudiant de Matemàtiques a Göttingen

És important remarcar que el Sr. Gauss té ara 18 *anys, i es dedica aquí a Braunschweig amb igual èxit a la filosofia i a la literatura clàssica així com a l'alta matemàtica.*

18 *Abril,* 1796 E. A. W. Zimmermann, *Prof.*

Figura 1: Braunschweig. Detall de l'heptadecàgon estrellat.

[1]Gauss compleix la seva paraula i 5 anys més tard, el 1801, publica les *Disquisitiones Arithmeticae*, [7], on, entre altres moltes coses, respon totalment la pregunta de quins polígons regulars es poden construir amb regle i compàs.

Just l'endemà del seu descobriment, el 30 de març de 1796, Gauss comença el seu famós diari. La primera entrada (Figura 2) diu: *Els principis dels quals depèn la divisió del cercle, i la divisibilitat geomètrica del mateix en disset parts, etc.*

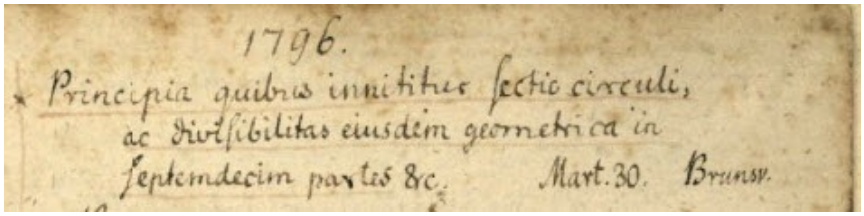

Figura 2: Diari.

Diu la llegenda que així com a la tomba d'Arquimedes hi havia dibuixats una esfera i un cilindre, a Gauss li hagués agradat que a la seva tomba hi figurés l'heptadecàgon. A l'estàtua del seu poble natal, Braunschweig, sí que hi figura aquest polígon. A la tomba, a Gottingen, no (almenys abans que hi passés l'autor d'aquestes notes).

Figura 3: Gottingen.

2 Construccions geomètriques amb regle i compàs

Concretem primerament què entenem per *construir amb regle i compàs*. Suposarem sempre donats (o construïts) dos punts A, B.

Direm que *una recta està construïda* si estan construïts dos dels seus punts. Per tant, de moment tan sols està construïda la recta AB.

Direm que *una circumferència està construïda* si el centre i el radi estan construïts. Construir el radi vol dir construir dos punts, ja que el radi és llavors el segment determinat per aquest dos punts. Per tant, de moment tan sols podem construir la circumferència de centre A i radi AB i la de centre B i radi BA.

Direm que *un punt està construït* si és intersecció de rectes o circumferències ja construïdes. Per exemple, podem construir el segon punt d'intersecció de la recta AB amb la circumferència de centre A i radi AB.

Donem a continuació algunes construccions elementals que utilitzarem més endavant per a la construcció dels polígons regulars.

Transport de segments i d'angles

Les tres primeres Proposicions dels *Elements* d'Euclides, [6], estan dedicades a veure que si tenim construïts un segment AB i una semirecta d'origen P, podem construir amb regle i compàs un punt Q sobre aquesta semirecta de manera que $AB = PQ$. La idea és construir un triangle equilàter de costat AP i, amb centre A girar el segment AB sobre la semirecta OA; a continuació, amb centre O, girar-lo sobre la semirecta OP; i a continuació, amb centre P girar-lo sobre la semirecta donada (Figura 4).

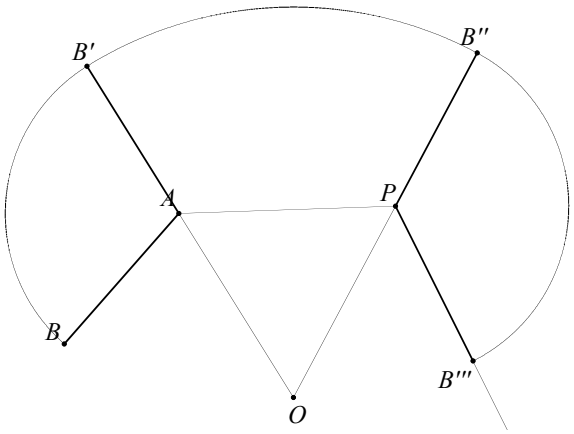

Figura 4: Transport de segments.

Transportar angles és una mica més difícil. Per transportar l'angle BAC (construïm C de manera que $AB = AC$) sobre la semirecta PQ, construïm la circumferència de centre P i radi AB i la circumferència de centre Q i radi BC (Figura 5). Si R és el punt d'interersecció d'aquestes dues circumferències, els triangles ABC i PQR són iguals (criteri[2] C.C.C.), i per tant l'angle $\angle BAC$ és igual a l'angle $\angle QPR$.

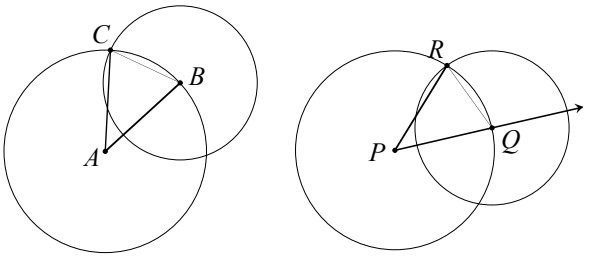

Figura 5: Transport d'angles.

A partir d'aquestes dues construccions que hem fet, transport de segments i transports d'angles, queda clar que *amb regle i compàs podem sumar i restar segments i podem sumar i restar angles.*

Mediatriu

Suposem construït el segment AB. Per construir la seva mediatriu intersequem la circumferència de centre A i radi AB amb la circumferència de centre B i radi AB (Figura 6). La recta determinada pels punts A' i B' que així obtenim és la mediatriu buscada.

[2]Criteri C.C.C. (costat-costat-costat) vol dir que dos triangles amb els costats corresponents iguals són iguals. És a dir, que els angles corresponents també són iguals. Podeu veure el punt de vista axiomàtic a [11].

En efecte, els triangles $\triangle ABA'$ i $\triangle ABB'$ són iguals (criteri C.C.C.) i per tant $\angle A'AO = \angle OAB'$, on O és el punt d'intersecció de les rectes AB i $A'B'$ (i, per tant, construït). Aplicant ara el criteri[3] C.A.C. als triangles $\triangle A'AO$ i $\triangle B'AO$, obtenim que l'angle $\angle A'OA$ és recte. També es veu fàcilment que O és el punt mig del segment AB, i per tant $A'B'$ és la mediatriu buscada.

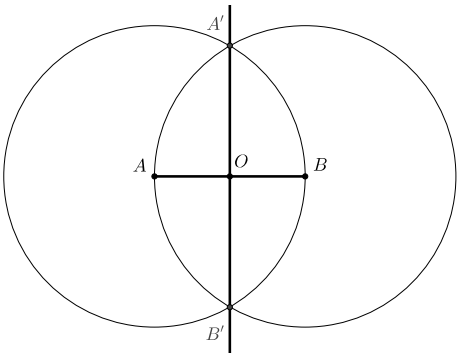

Figura 6: Mediatriu.

Bisectriu

Donat un angle de vèrtex O construïm una circumferència de centre O i radi arbitrari, que tallarà els costats de l'angle en punts respectius A i B (Figura 7).

Observem que el radi arbitrari ha de ser un radi construït prèviament.

Llavors les circumferències de centres A i B i radi OA es tallen en el punt O i en un altre punt O'. Com que els triangles $\triangle AOO'$ i $\triangle BOO'$ són iguals (C.C.C.) la semirecta OO' és la bisectriu buscada.

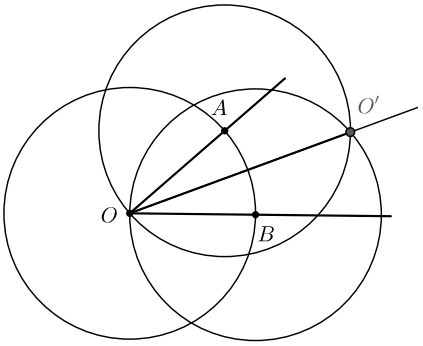

Figura 7: Bisectriu.

Perpendicular

Perpendicular des d'un punt exterior.

Sigui A un punt que no pertany a la recta r. Prenem dos punts arbitraris P i Q de r (Figura 8). Per exemple els que han servit per construir-la. Construïm, un angle $\angle A'PQ$ igual a $\angle APQ$, tal que A i A' estiguin situats a costats diferents respecte r, i tal que $AP = A'P$. Per fer això construïm la circumferència de centre P i radi PA, que talla r en un cert punt B. La circumferència de centre B i radi BA talla l'anterior circumferència en el punt A' buscat, ja que, pel criteri $C.C.C.$ aplicat

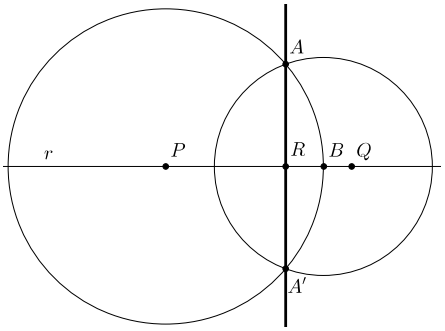

Figura 8: Perpendicular.

[3]Criteri C.A.C. (costat-angle-costat) vol dir que dos triangles amb dos costats corresponents iguals i amb l'angle comprés entre aquests dos costats també igual, són iguals.

als triangles $\triangle APQ$ i $\triangle A'PQ$, els angles $\angle A'PQ$ i $\angle APQ$ són iguals. Aplicant ara el criteri $C.A.C$ als triangles $\triangle APR$ i $\triangle A'PR$ veiem que la recta AA' és perpendicular a r.

Perpendicular per un punt de la pròpia recta.

Es tracta de construir una perpendicular a r que passi per un punt donat P de r. Construïm un punt arbitrari A fora de r (Figura 9). Construïm la circumferència $\mathcal{C}$ de centre P i radi PA. Sigui A' l'altra punt en que $\mathcal{C}$ talla la recta PA. Construïm la perpendicular a r des de A', que talla $\mathcal{C}$ en un segon punt A''. La mediatriu del segment AA'' és la perpendicular buscada.

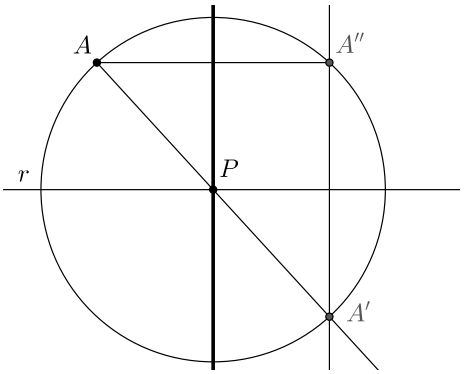

Figura 9: Perpendicular.

Paral·lela

Ara és fàcil, construïda una recta i un punt exterior, construir la paral·lela a la recta per aquest punt. En efecte, és suficient construir la perpendicular a la recta des del punt i a continuació construir la perpendicular a aquesta recta pel punt. Si aquesta darrera recta tallés la primera tindríem un triangle amb dos angles rectes, cosa que no pot ser ja que es pot demostrar que en tot triangle almenys dos angles són aguts, vegeu per exemple [11], Teorema 1.19. Observem que aquesta construcció demostra la existència, però no la unicitat (això ens introduiria en el món de la geometria no euclidiana) de rectes paral·leles per un punt exterior a una recta donada.

Arrel quadrada d'un segment

Per construir l'arrel quadrada d'un segment de longitud a només hem de colocar la unitat de mesura a continuació d'aquest segment i construir la circumferència de diàmetre $a+1$ (Figura 10). La perpendicular a aquest diàmetre en l'extrem del segment té longitud $h = \sqrt{a}$. En efecte, pel teorema de l'altura tenim que

$$\frac{h}{a} = \frac{1}{h}\,.$$

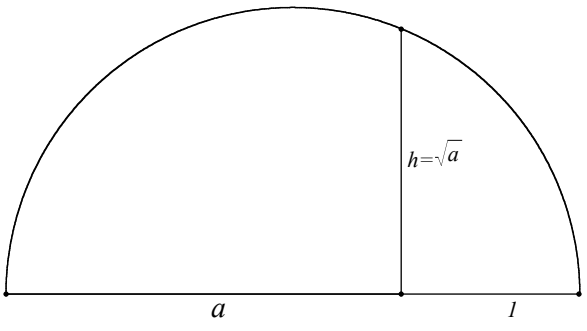

Figura 10: Arrel quadrada.

Invers d'un segment

Donat un segment de longitud a, volem construir un segment de longitud $1/a$. Prenem dues semirectes arbitràries amb origen comú O. Sobre una d'elles prenem punts A i A' tals que $OA = a$, $AA' = 1$ i A estigui entre mig de O i A' (Figura 11).

Sobre l'altra prenem un punt B tal que $OB = 1$. Llavors la paral·lela a AB per A' talla la recta OB en un punt B' tal que $BB' = 1/a$. En efecte, si apliquem el teorema de Tales als triangles $\triangle OAB$ i $\triangle OA'B'$ obtenim

$$\frac{a}{1} = \frac{1}{BB'}.$$

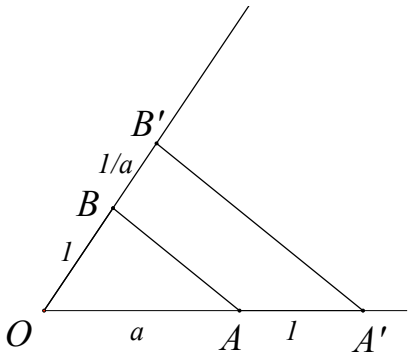

Figura 11: Invers.

Observem que, com sabem construir inversos i sumes, si tenim construït un segment de longitud 1 llavors sabem construir un segment de longitud r per a tot $r \in \mathbb{Q}$. Concretament, si $r = p/q$, només hem de sumar p cops l'invers de q. És a dir, *els nombres racionals són construïbles.*

3 Pentàgon regular

En aquesta secció donarem dues construccions del pentàgon regular. Una d'elles perquè és la més ràpida i senzilla i l'altre perquè ens il·lustrarà el mètode que després utilitzarà Gauss per construir l'heptadecàgon.[4]

Primera construcció. Per explicar aquesta construcció suposem que la circumferència de la Figura 12 és la circumferència de centre $O = (0, 0)$[5] i radi 1. Sigui $A = (0, -1/2)$ i $B = (1, 0)$. Amb centre A i radi AB tracem una circumferència que talla l'eix de les $y's$ en el punt $C = (0, \frac{\sqrt{5}-1}{2})$. El punt de tall de la circumferència inicial amb la circumferència de centre B i radi BC és el primer vèrtex del pentàgon.

La justificació és clara si sabem que el costat del pentàgon regular inscrit a la circumferència de radi 1 val

$$L = \sqrt{\frac{5 - \sqrt{5}}{2}}.$$

Això es demostra fàcilment observant primer que $L = 2 \sin \frac{\pi}{5}$ i observant a continuació que la raó d'or τ val

$$\tau = 2 \cos \frac{\pi}{5}.$$

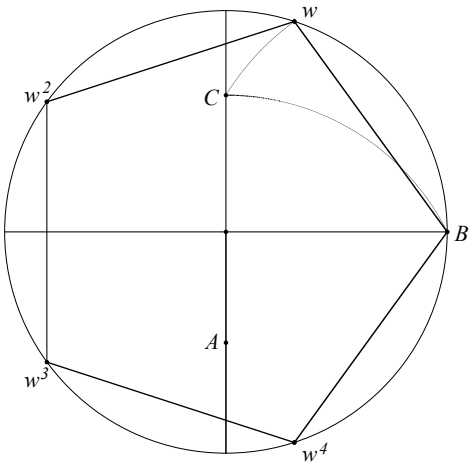

Figura 12: Pentàgon.

Aquesta relació entre la raó d'or τ i el $\cos \frac{\pi}{5}$ es dedueix del triangle auri $\triangle AOB$ que apareix al dibuixar el decàgon regular de costat AB inscrit a la circumferència de centre O (Figura 13).

[4] La idea de que Gauss es va inspirar en el pentàgon per resoldre l'heptadecàgon és només una conjectura meva.

[5] No cal introduir coordenades, només ho fem per comoditat.

Es construeix el punt B', intersecció de la bisectriu de l'angle en el vèrtex B amb el costat OA. Els triangles $\triangle AOB$ i $\triangle B'BA$ de la figura són semblants.

Per tant,

$$\frac{AB}{OA-AB}=\frac{OA}{AB}.$$

Equivalentment

$$\frac{1}{\frac{OA}{AB}-1}=\frac{OA}{AB},$$

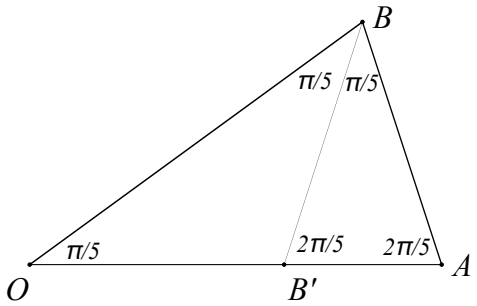

Figura 13: Decàgon.

que implica que el quocient OA/AB és arrel de l'equació $x^2-x-1=0$, i és per tant la raó d'or. És a dir, $\tau=\dfrac{OA}{AB}$. Per altra banda, considerant l'altura des de O veiem que

$$\cos\frac{2\pi}{5}=\frac{AB/2}{OA}=\frac{1}{2\tau}.$$

Aplicant ara la fórmula de l'angle doble obtenim $\tau=2\cos(\pi/5)$. Així

$$L=2\sin\frac{\pi}{5}=2\sqrt{1-\cos^2\frac{\pi}{5}}=\sqrt{4-\tau^2}=\sqrt{\frac{5-\sqrt{5}}{2}}.$$

Segona construcció. Situem-nos en el pla complex. Això pressuposa un canvi conceptual important i un salt en el temps respecte al que hem anat fent fins ara.

Les arrels del polinomi ciclotòmic

$$\frac{z^5-1}{z-1}=z^4+z^3+z^2+z+1,$$

són w,w^2,w^3,w^4 amb $w=e^{2\pi i/5}$. Observem que $1,w,w^2,w^3,w^4$ són els vèrtexs del pentàgon que volem construir (Figura 12). Observem també que

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

Aquesta agrupació s'ha fet perquè els dos números $w+w^4$ i w^2+w^3, que Gauss anomena *períodes*, són números reals (les parts imaginàries de w i w^4, i de w^2 i w^3, són respectivament oposades). El seu producte serà doncs també real. De fet tenim

$$(w+w^4)\cdot(w^2+w^3)=w^3+w^4+w^6+w^7=w^3+w^4+w+w^2=-1.$$

Els dos períodes sumen -1 i el seu producte és -1, per tant són arrels de l'equació de segon grau

$$x^2+x-1=0.$$

Tenint en compte els signes veiem que ha de ser

$$\begin{aligned} w + w^4 &= \frac{1}{\tau}, \\ w^2 + w^3 &= -\tau, \end{aligned}$$

on τ és la raó d'or. Multiplicant per w la primera d'aquestes equacions tenim

$$w^2 + 1 = \frac{1}{\tau} w,$$

igualtat que ens diu que w és arrel del polinomi de segon grau $x^2 - \frac{1}{\tau}x + 1$, que té coeficients que són racionals i coeficients que són extensions quadràtiques de racionals. Així,

$$w = \frac{\frac{1}{\tau} \pm \sqrt{\left(\frac{1}{\tau}\right)^2 - 4}}{2} = \frac{1 \pm \sqrt{1 - 4\tau^2}}{2\tau}.$$

Com que l'arrel és negativa, la part real d'aquest nombre complex és $1/2\tau$, ès a dir

$$\cos \frac{2\pi}{5} = \frac{1}{2\tau}.$$

Com τ és un irracional quadràtic i sabem construir sumes, productes, arrels quadrades i inversos, sabem construir $\cos \frac{2\pi}{5}$, i per tant, el pentàgon.

4 Heptadecàgon regular

El mètode seguit a la segona construcció del pentàgon es pot repetir quasi exactament per a l'heptadecàgon.

En aquest cas les arrels del polinomi ciclotòmic

$$\frac{z^{17} - 1}{z - 1} = z^{16} + z^{15} + \cdots + z^2 + z + 1,$$

són $1, w, w^2, \ldots, w^{16}$ amb $w = e^{2\pi i/17}$. Observem que $1, w, w^2, \ldots, w^{16}$ són els vèrtexs del heptadecàgon que volem construir.[6] Denotarem $w_k = w^k$. Els càlculs que venen a continuació apareixen ja en el *Disquisitiones Arithmeticae*, [7], però els podeu trobar també, per exemple, a [3].

Agrupem[7] de manera màgica les 16 arrels en els dos primers períodes

$$\begin{aligned} u_1 &= w_1 + w_9 + w_{13} + w_{15} + w_{16} + w_8 + w_4 + w_2, \\ u_2 &= w_3 + w_{10} + w_5 + w_{11} + w_{14} + w_7 + w_{12} + w_6. \end{aligned}$$

[6] Com que nosaltres en tindríem prou sabent construir la part real de w es presenta aquí una pregunta interessant que és la següent: si w és arrel del ciclotòmic, quin polinomi satisfà la part real de w? És una pregunta que ens podem fer en general (és a dir, encara que el polinomi no sigui ciclotòmic) i que sembla difícil. Els càlculs de Gauss que venen a continuació són la resposta a aquesta pregunta en el cas particular de l'heptadecàgon.

[7] Justament a aquesta agrupació es refereix Gauss en la seva carta a Gerling comentada a la pàgina 1 quan diu *Tot estava en dividir les arrels de l'equació [..] en dos grups.*

Estan formats per 8 arrels cadascun i són nombres reals, ja que estan formats per parelles de la forma $w_i + w_{17-i}$, i com que aquests dos nombres complexos són conjugats, la seva suma és real. En particular, el seu producte és un nombre real. Direm que u_1 i u_2 són períodes d'ordre 8.

Es veu de seguida que $u_1 \cdot u_2 = -4$, ja que

$$u_1 \cdot u_2 = w_1u_2 + w_9u_2 + w_{13}u_2 + w_{15}u_2 + w_{16}u_2 + w_8u_2 + w_4u_2 + w_2u_2$$

i aquesta expressió no és més que la suma de 8 períodes tals que dos a dos sumen -1.

La manera màgica que va utilitzar Gauss per construir u_1 i u_2 va ser ordenar els elements de $\mathbb{Z}/17$ diferents de zero d'acord amb les potències de 3 (mòdul 17)[8] . Concretament

n	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
3^n	1	3	9	10	13	5	15	11	16	14	8	7	4	12	2	6

Llavors u_1 ha estat la suma de les potències de 3 parells i u_2 ha estat la suma de les potències de 3 imparells.

Així, u_1 i u_2 són dos nombres reals que sumen -1 i tenen producte 4. Això vol dir que són solució de l'equació de segon grau

$$\boxed{x^2 + x - 4 = 0.} \tag{1}$$

Són, doncs, irracionals quadràtics. Ara de cada període en fem dos.

$$\begin{aligned} v_1 &= w_1 + w_{13} + w_{16} + w_4, \\ v_2 &= w_9 + w_{15} + w_8 + w_2, \\ v_3 &= w_3 + w_5 + w_{14} + w_{12}, \\ v_4 &= w_{10} + w_{11} + w_7 + w_6. \end{aligned}$$

Estan formats per 4 arrels cadascun i són nombres reals. Mirem, com abans, les seves sumes i productes. Tenim $v_1 + v_2 = u_1$ (obvi) i $v_1 \cdot v_2 = -1$ (càlcul directe). Per tant v_1 i v_2 són solució de l'equació de segon grau

$$\boxed{x^2 - u_1x - 1 = 0.} \tag{2}$$

Anàlogament v_3 i v_4 són solució de l'equació de segon grau

$$\boxed{x^2 - u_2x - 1 = 0.} \tag{3}$$

[8] Aquesta propietat extraordinària que fa que les potències de 3 generin $Z/(17)$ és conseqüència del teorema del generador o teorema de l'element primitiu, que diu (vegeu, per exemple, [1], p. 342):

Teorema. *El grup multiplicatiu de $\mathbb{Z}/(p)$, amb p primer, és cíclic.*

Això vol dir que hi ha un element g a $\mathbb{Z}/(p)$, anomenat element *primitiu*, tal que

$$\mathbb{Z}/(p) = \{0, g, g^2, \ldots, g^{p-1}\}.$$

Ja hem vist com les potències de 3 generen tos els element no nuls de $\mathbb{Z}/(17)$. Un altre exemple serien les potències de 3 a $\mathbb{Z}/(7)$: $1, 3, 2, 6, 4, 5$. En canvi, per exemple, a la successió de potències de 2 a $\mathbb{Z}/(7)$, que són $1, 2, 4$, no hi apareixen tots els elements no nuls de $\mathbb{Z}/(7)$. S'intueix doncs que tot i que el teorema ens diu que hi ha un element *primitiu* pot ser difícil trobar-lo.

Per tant, *els períodes d'ordre* 4, v_1 *i* v_2, *són arrels d'equacions de segon grau que tenen coeficients racionals i coeficients que són períodes d'ordre* 8.

Novament de cada període en fem dos

$$w_k + w_{17-k} = 2\cos(2k\pi/17), \quad k = 1, \ldots, 8$$

Estan formats per 2 arrels cadascun i són nombres reals. Mirem com abans les seves sumes i producte. Per exemple,

$$(w_1 + w_{16}) + (w_4 + w_{13}) = v_1$$

i

$$(w_1 + w_{16}) \cdot (w_4 + w_{13}) = w_5 + w_{14} + w_3 + w_{12} = v_3.$$

Així, $w_1 + w_{16} = 2\cos\theta$, i $w_4 + w_{13} = 2\cos 4\theta$ són arrels de l'equació de segon grau

$$\boxed{x^2 - v_1 x + v_3 = 0.} \tag{4}$$

Per tant, *els períodes d'ordre* 2, $2\cos\theta$ *i* $2\cos 4\theta$, *són les arrels d'una equació de segon grau que té coeficients racionals i coeficients que són períodes d'ordre* 4.

Resolent les equacions (1), (2), (3) i (4), obtenim successivament

$$\begin{aligned} u_1 &= \frac{-1+\sqrt{17}}{2}, \qquad u_2 = \frac{-1-\sqrt{17}}{2}, \\ v_1 &= \frac{u_1 + \sqrt{u_1^2+4}}{2}, \quad v_3 = \frac{u_2 + \sqrt{u_2^2+4}}{2}, \\ 2\cos\frac{2\pi}{17} &= \frac{v_1 + \sqrt{v_1^2 - 4v_3}}{2}. \end{aligned}$$

Substituint a la última els valors obtinguts a les anteriors obtenim

$$\begin{aligned} \cos\frac{2\pi}{17} &= \frac{1}{16}\Bigg(-1+\sqrt{17}+\sqrt{34-2\sqrt{17}} \\ &+ \sqrt{68+12\sqrt{17}+2(-1+\sqrt{17})\sqrt{34-2\sqrt{17}} - 16\sqrt{34+2\sqrt{17}}}\Bigg). \end{aligned}$$

Com sabem construir sumes, productes, arrels quadrades i inversos, sabem construir $\cos\frac{2\pi}{17}$, i per tant, el heptadecàgon. Però, això si, amb molts més cops de compàs que amb la construcció que va donar Richmond (Figura 14) molts anys més tard (1893).

Expliquem la sorprenent construcció de Richmond sense justificar-la (vegeu [3], pàgina 62). Tots els punts que introduïm a continuació es poden construir amb regle i compàs a partir de O, I.

1) Construïm A de manera que $A = (0, 1/4)$.

2) Construïm B de manera que $\angle OAB = \frac{1}{4}\angle OAI$.

3) Construïm C de manera que $\angle CAB = \frac{\pi}{4}$.

4) Construïm D com el punt d'intersecció de l'eix de les $y's$ amb la circumferència de diàmetre CI.

5) Construïm P_3 i P_5 com els punts d'intersecció amb l'eix de les $x's$ de la circumferència de centre B i radi BD.

6) Construïm M_3 i M_5 com els punts d'intersecció amb la circumferència inicial de les perpendiculars a l'eix de les $x's$ per P_3 i P_5 respectivament. M_3 i M_5 són els vèrtexs 3 i 5 de l'heptàdecàgon.

7) Construïm M_4 com la intersecció amb la circumferència inicial de la mediatriu de M_3M_5. M_4 és el quart vèrtex de l'heptadecàgon, que té costat, doncs, M_3M_4.

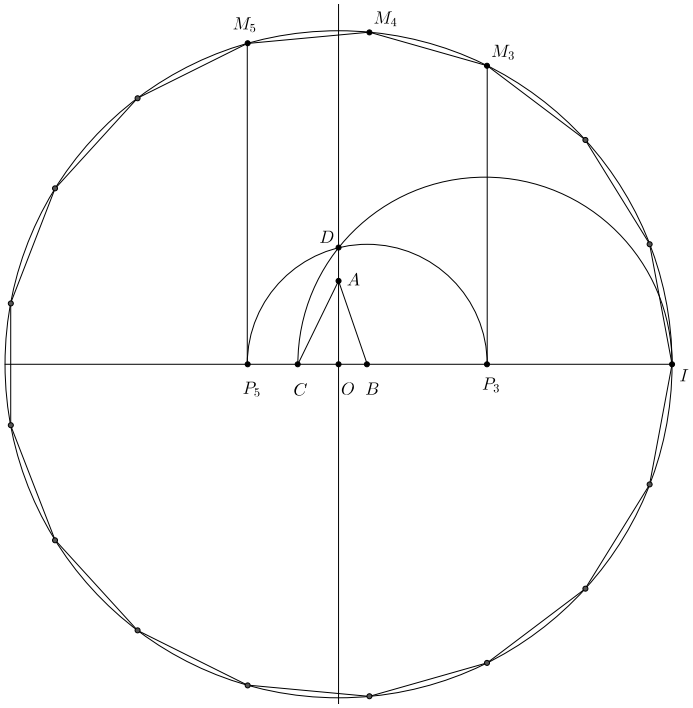

Figura 14: Heptadecàgon.

5 Polígons regulars. La condició suficient de constructibilitat

En el *Disquisitiones Arithmeticae*, [7], Gauss demostra que si el número natural n és producte de potències de dos per primers de Fermat diferents (vegeu la definició de primer de Fermat a la pàgina 16) llavors el polígon regular de n costats es pot construir amb regle i compàs, i enuncia sense demostració que el recíproc és també cert. La fórmula explícita per al $\cos(2\pi/17)$, que demostra que l'heptadecàgon es pot construir, apareix a la secció 365 (la penúltima del *Disquisitiones Arithmeticae*) on també enuncia sense demostració que el polígon de p costats amb p primer i $p-1$ no potència de 2 no es poden construir (en particular, l'heptàgon no es pot construir)[9]. Aquest resultat fou demostrat el 1837 per Wantzel, [14]. A la secció 366 i última del *Disquisitiones Arithmeticae* demostra que les potències de primers no es poden construir i acaba amb la llista dels polígons construïbles amb menys de 300 costats.

Donem ara la idea de la demostració de Gauss. Recomanem [12].

[9]Gauss diu (les majúscules són seves, la negreta de l'editor del Nou Biax): *PODEM DEMOSTRAR AMB TOT RIGOR QUE AQUESTES EQUACIONS ELEVADES NO ES PODEN NI EVITAR NI REDUIR DE CAP MANERA A INFERIORS, encara que els límits d'aquesta obra no permetin transmetre aquí aquesta demostració; cosa, però, que hem considerat que s'ha d'advertir perquè ningú no esperi conduir a construccions geomètriques encara altres seccions excepte les que la nostra teoria suggereix, és a dir, les seccions en* $7, 11, 13, 19$ *etc., parts, i* **consumeixi el temps inútilment**.

Primer pas. Suposem n de la forma $n = 2^k \cdot p$ amb p senar. Com sabem bisecar l'angle, si sabem construir el polígon regular de p costats sabrem construir també el polígon regular de $2^k \cdot p$ costats. I recíprocament, si sabem construir el polígon regular de $2^k \cdot p$ costats sabrem construir unint els vèrtexs de 2^k en 2^k, el polígon regular de p costats. És a dir, el polígon regular de $n = 2^k \cdot p$ es pot construir si i només si el polígon regular de p costats es pot construir. Això redueix el problema de la construcció de polígons regulars al cas en que el número de costats és producte de potències de primers diferents de 2.

Segon pas. Suposem n de la forma $n = p \cdot q$ amb p i q primers entre ells. Si sabem construir el polígon regular de p costats i el polígon regular de q costats sabem construir poligons regulars de $n = p \cdot q$ costats.

En efecte, per la identitat de Bézout, existeixen enters r, s tals que

$$qr + ps = 1.$$

Dividint per pq i multiplicant per 2π tenim

$$r\frac{2\pi}{p} + s\frac{2\pi}{q} = \frac{2\pi}{pq}.$$

Això implica que si sabem construir els angles $\dfrac{2\pi}{p}$ i $\dfrac{2\pi}{q}$ sabrem construir, sumant-los o restant-los (r i s tenen signes oposats), l'angle $\dfrac{2\pi}{pq}$, i per tant el polígon regular de $p \cdot q$ costats.

Per exemple, com sabem construir el triangle equilàter i el pentàgon regular sabem construir el polígon regular de 15 costats, ja que degut a la igualtat

$$2\left(\frac{2\pi}{5}\right) + (-1)\frac{2\pi}{3} = \frac{2\pi}{15},$$

només hem de sumar dues vegades l'angle central del pentàgon i restar-li una vegada l'angle central del triangle equilàter per tenir l'angle central del pentadecàgon.

A la Figura 15 es veu com el costat E_1P_2, format pel primer vèrtex del triangle equilàter i el segon vèrtex del pentàgon, dóna el costat del pentadecàgon.

Notem de passada que val el recíproc, és a dir, que si sabem construir el polígon regular de $p \cdot q$ costats sabem construir el polígon regular de p costats, simplement unint els vèrtexs de q en q, i el de q costats unint els vèrtexs de p en p.

Tercer pas. Com tot nombre n descompon com

$$n = 2^\alpha p_1^{\alpha_1} \dots p_k^{\alpha_k}$$

amb p_i primers imparells diferents, i degut a les observacions anteriors, el problema de saber si podem construir el polígon regular de n

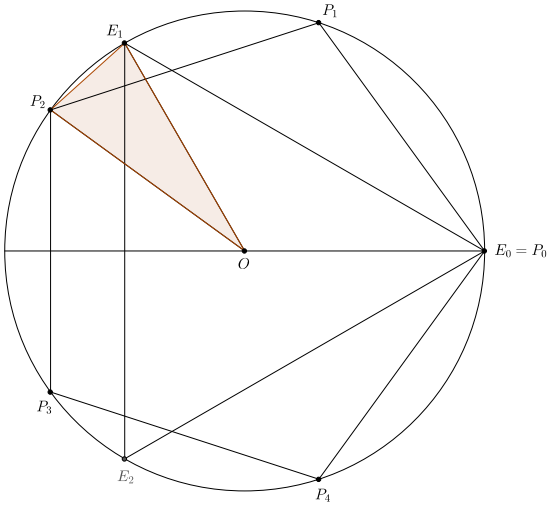

Figura 15: Pentadecàgon.

costats es redueix a saber si sabem construir
els polígons regulars de $p_i^{\alpha_i}$ costats.

Quart pas. Polígons amb un nombre primer de costats. Pels mateixos comentaris fets en estudiar el pentàgon i l'heptadecàgon, sabem que els vèrtexs del polígon que volem construir, pensats com nombres complexos, són el número $1 \in \mathbb{C}$ i les arrels del polinomi ciclotòmic de grau $p-1$, on p és el nombre primer de costats. La observació de que el mètode seguit per a l'heptadecàgon es pot generalitzar està recollida en el teorema següent (vegeu [7] o [4]).

Teorema 5.1. *Si p és un nombre primer de la forma $p = 2^k + 1$, l'equació*

$$z^{p-1} + z^{p-2} + \cdots + z + 1 = 0$$

es pot resoldre per radicals quadràtics (extracció successiva d'arrels quadrades), i per tant, el polígon de p costats es pot construir amb regle i compàs.

Demostració. Considerem el ciclotòmic

$$z^{p-1} + z^{p-2} + \cdots + z + 1 = 0$$

i les seves arrels

$$\omega, \omega^2, \ldots, \omega^{p-1}, \quad \omega = e^{2\pi i/p} = \cos\frac{2\pi}{p} + i\sin\frac{2\pi}{p}.$$

Sigui g un número menor que p tal que

$$g, g^2, \ldots, g^{p-1}$$

donin residu $1, 2, \ldots, p-1$ al ser dividits per p (aquest element g existeix pel teorema de l'element primitiu, que hem recordat en el peu de pàgina 8, pàgina 10). Llavors

$$\omega^g, \omega^{g^2}, \ldots, \omega^{g^{p-1}}$$

reordenats es poden escriure com

$$\omega, \omega^2, \ldots, \omega^{p-1}.$$

Posem ara

$$\begin{aligned}
\eta_1 &= \omega^g + \omega^{g^3} + \cdots + \omega^{g^{p-2}}, \\
\eta_2 &= \omega^{g^2} + \omega^{g^4} + \cdots + \omega^{g^{p-1}}, \\
\eta &= \eta_1 + \eta_2.
\end{aligned}$$

I a continuació

$$\begin{aligned}
\eta_{11} &= \omega^g + \omega^{g^5} + \cdots + \omega^{g^{p-4}}, \\
\eta_{12} &= \omega^{g^3} + \omega^{g^7} + \cdots + \omega^{g^{p-2}}, \\
\eta_1 &= \eta_{11} + \eta_{12}, \\
\eta_{21} &= \omega^{g^2} + \omega^{g^6} + \cdots + \omega^{g^{p-3}}, \\
\eta_{22} &= \omega^{g^4} + \omega^{g^8} + \cdots + \omega^{g^{p-1}}, \\
\eta_2 &= \eta_{21} + \eta_{22}.
\end{aligned}$$

Observem ara que coneixem la suma i el producte de η_1 i η_2. En efecte,

$$\eta_1 + \eta_2 = \omega + \omega^2 + \omega^3 + \cdots + \omega^{p-1} = -1.$$

I

$$\eta_1\eta_2 = \sum_{r,s} \omega^{g^r}\omega^{g^s} = \sum_t \omega^t,$$

amb $1 \leq r, s, t \leq p$, ja que el producte d'arrels és una arrel.

Si a cada terme del sumatori canviem ω per ω^g el valor total no canvia ja que aquest canvi transforma η_1 en η_2 i η_2 en η_1. Això vol dir que cada arrel apareix en el sumatori el mateix número de vegades i per tant

$$\eta_1\eta_2 = \nu\eta = -\nu,$$

amb $\nu \in \mathbb{N}$.

Per tant η_1 i η_2 són arrels de

$$x^2 + x - \nu = 0.$$

Arguments similars ens diuen que η_{11} i η_{12} són arrels de

$$x^2 - \eta_1 x + (\nu_1\eta_1 + \nu_2\eta_2) = 0,$$

amb $\nu_1, \nu_2 \in \mathbb{N}$, vegeu per exemple [5]. I el mateix passa amb η_{21} i η_{22}.

Quan $p-1$ és potència de dos aquest procediment ens porta a que els períodes d'ordre 1, és a dir, les arrels, es poden calcular resolent una equació de segon grau amb coeficients períodes d'ordre 2, els quals es poden calcular resolent una equació de segon grau amb coeficients períodes d'ordre 4, etc. □

Cinquè i últim pas. Polígons amb un nombre arbitrari de costats.

Corol·lari 5.2. *Si $n = 2^\alpha \cdot p_1 \cdot \cdots \cdot p_r$ amb p_i primers i tals que $p_i = 2^{k_1} + 1$, el polígon regular de n costats es pot construir amb regle i compàs.*

Demostració. Conseqüència del Teorema 5.1 i els comentaris anteriors. □

Proposició 5.3. *Si $2^k + 1$ és primer, llavors $k = 2^a$, amb $a \in \mathbb{N}$.*

Demostració. En efecte, suposem que k fos divisible per un número imparell. Tindríem $k = (2m+1)r$. Llavors

$$p = 2^k + 1 = 2^{(2m+1)r} + 1 = (2^r)^{2m+1} + 1.$$

Això vol dir que 2^r és arrel del polinomi

$$x^{2m+1} + 1.$$

Com aquest polinomi admet l'arrel $x = -1$ tenim

$$x^{2m+1} + 1 = (x+1)q(x)$$

per a un cert polinomi $q(x)$. En particular,

$$p = (2^r)^{2m+1} + 1 = (2^r + 1)q(2^r)$$

i p no seria primer. Per tant, k només és divisible per 2, és a dir, $k = 2^a$ amb $a \in \mathbb{N}$. □

Corol·lari 5.4. *Si $n = 2^\alpha \cdot p_1 \cdot \cdots \cdot p_r$ amb p_i primers i tals que $p_i = 2^{2^{a_i}} + 1$, amb $a_i \in \mathbb{N}$, el polígon regular de n costats es pot construir amb regle i compàs.*

Demostració. Conseqüència del Corol·lari 5.2 i la Proposició 5.3. □

Els nombres primers p que s'escriuen de la forma

$$p = 2^{2^k} + 1, \quad k \in \mathbb{N},$$

es diuen *primers de Fermat*. Però no tots els nombres d'aquesta forma són primers. De fet, només es coneixen 5 primers de Fermat, els que corresponen a $k = 0, 1, 2, 3, 4$, és a dir,

$$p = 3, 5, 17, 257, 65537.$$

Gauss comenta en el *Disquisitiones Arithmeticae* que l'il·lustre Euler ja es va adonar que el sisè nombre de Fermat no és primer. Concretament,

$$2^{2^5} + 1 = 2^{32} + 1 = 4294967297 = 641 \cdot 6700417.$$

El Corol·lari 5.4 ens diu que els polígons construïbles amb menys de 300 costats són els de

$$3, 4, 5, 6, 8, 10, 12, 15, 16, 17, 20, 24, 30, 32, 34, 40, 48, 51, 60, 64, 68, 80,$$
$$85, 96, 102, 120, 128, 136, 160, 170, 192, 204, 240, 255, 256, 257, 272$$

costats[10].

6 La condició necessària de constructibilitat

Per a aquesta part necessitem el que es coneix com Teorema de Wantzel però que ja era ben conegut per Gauss, com es veu llegint la secció 365 del *Disquisitiones Arithmeticae* (vegeu el peu de pàgina número 9 de la pàgina 12), però del que no se'n va donar una demostració rigorosa fins el treball de Wantzel de 1837.

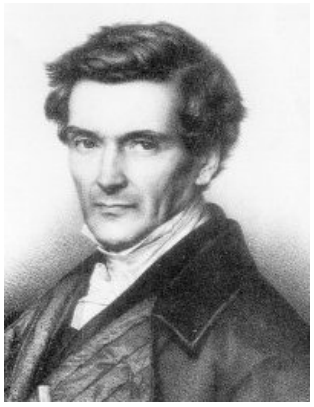

Figura 16: Pierre L. Wantzel (1814-1848)

Hem utilitzat, entre d'altres, l'article de H. S. Carslaw [4], el qual està basat en l'article d'Enriques *Sulle equazioni algebriche risolubili per radicali quadratici e sulla construibilità dei poligoni regolari*, capítol 17, p. 263-305, del llibre [5]. Ni Carslaw ni Enriques citen el treball de Wantzel, que va passar desapercebut durant quasi cent anys. També recomanem el treball de D. Kuh [8]. A la Secció 8, Teorema 8.4, demostrarem el resultat següent.

[10] Com hem dit abans, el *Disquisitiones Arithmeticae* acaba justament amb aquesta llista dels 38 polígons regulars construïbles amb menys 300 costats. Això dóna una idea de la importància que donava Gauss a aquest resultat.

Teorema 6.1 (Wantzel[11]). *Suposem que el punt P del pla Euclidià amb coordenades cartesianes (a, b) ha estat construït. Llavors el polinomi de grau més petit que admet a (o b) com arrel té grau potència de dos.*

La relació entre coordenades cartesianes i punts construïts és la següent (vegeu, per exemple, [3]). Denotem O, I els punts amb els quals iniciem el procés de construcció. Construïm un tercer punt I' com la intersecció de la recta OI (per tant, construïda) i de la circumferència $\mathcal{C}$ de centre O i radi OI (també construïda). Construïm a continuació la mediatriu del segment II'. Denotem J el punt d'intersecció d'aquesta mediatriu amb la circumferència $\mathcal{C}$. Prenem com referència ortonormal del pla la referència $\{O; \overrightarrow{OI}, \overrightarrow{OJ}\}$, és a dir, la referència d'origen O i base $\overrightarrow{OI}, \overrightarrow{OJ}$. Sobre la recta OI agafem com unitat de mesura el segment OI i sobre la recta OJ agafem com unitat de mesura el segment OJ. Els punts de la recta OI a distancia x de O els denotem $(x, 0)$ i els punts de la recta OJ a distancia y de O els denotem $(0, y)$. Es diu llavors que un punt P del pla té coordenades (x, y) si les rectes ortogonals als eixos OI i OJ per P els tallen en els punts $(x, 0)$ i $(0, y)$ respectivament.

A partir del Teorema 6.1, Wantzel demostra la impossibilitat de la trisecció de l'angle i de la duplicació del cub, essencialment com les hem reproduït més endavant a la Secció 7 d'aquestes notes. També diu[12] que es pot provar la impossibilitat de construir un polígon regular amb un nombre de costats igual a la potència d'un primer ja que es pot provar, modificant lleugerament la demostració de Gauss, que el polinomi ciclotòmic corresponent és irreductible. Com que aquesta 'demostració' no és molt satisfactòria[13] nosaltres donarem una demostració d'questa impossiblitat a partir d'una versió una mica diferent del Teorema 6.1. Concretament, identificant com és habitual el pla Euclidià amb el pla complex, demostrarem el resultat següent.

Teorema 6.2. *Suposem que el punt z del pla complex, amb $|z| = 1$, ha estat construït. Llavors el polinomi de grau més petit que admet z com arrel té grau potència de dos.*

Per no anar parlant sempre del polinomi de grau més petit s'introdueix el concepte de *polinomi mínim.*

Definició 6.3. *El* polinomi mínim *sobre $\mathbb{Q}$ de $a \in \mathbb{C}$ és el polinomi mònic de grau més petit, amb coeficients a $\mathbb{Q}$, que té a com arrel.*

Proposició 6.4. *Tot polinomi mònic i irreductible sobre $\mathbb{Q}$ és el polinomi mínim de les seves arrels.*

Demostració. Sigui $P(x) \in \mathbb{Q}[x]$ mònic i irreductible sobre $\mathbb{Q}$ i suposem $P(a) = 0$. Si $P(x)$ no fos el polinomi mínim de a hi hauria un polinomi mònic $m(x) \in \mathbb{Q}[x]$ de grau més petit que

[11] L'enunciat original de Wantzel diu: *L'equation du degree 2^n, $f(x) = 0$, qui donne toutes les solutions d'un problème susceptible d'être résolu au moyen de n équations du second degré, est nécessairement irréductible.* Vegeu [14].

[12] *On peut prouver, en modifiant légèrement la démonstration de M. Gauss que l'equation de degree $(a-1)a^{\alpha-1}$, obtenue en égalant à zéro le quotient de $x^{a^\alpha} - 1$ par $x^{a^{\alpha-1}} - 1$, est irréductible; il faudrait donc que $(a-1)a^{\alpha-1}$ fût de la forme 2^k en même temps que $a - 1$, ce qui est impossible à moins que $a = 2$.*

[13] Wantzel en el seu article treballa amb equacions algèbriques de les que no especifica si les variables són reals o complexes. Però quan pensem els punts del pla Euclidià com complexos $z = (x, y)$ és clar que les circumferències tenen equacions quadràtiques en x i y, però no en z.

el grau de $P(x)$ i tal que $m(a) = 0$. Però llavors el residu $R(x)$ de la divisió de $P(x)$ entre $m(x)$ compliria $R(a) = 0$ i com que $R(x)$ té grau més petit que el grau de $m(x)$ ha de ser $R(x) = 0$ i per tant $P(x) = m(x) \cdot q(x)$, contradicció amb ser $P(x)$ irreductible sobre $\mathbb{Q}$. □

Teorema 6.5. *El polinomi ciclotòmic*

$$z^{p-1} + z^{p-2} + \cdots + z + 1$$

amb p primer, és irreductible sobre $\mathbb{Q}$.

Demostració. Posant $z = x + 1$ el ciclotòmic s'escriu com

$$\frac{(x+1)^p - 1}{x} = \sum_{k=1}^{p} \binom{p}{k} x^{k-1} = x^{p-1} + px^{p-2} + \binom{p}{p-2} x^{p-3} + \cdots + \binom{p}{2} x + p = 0.$$

El criteri d'Eisenstein[14] ens diu que aquest polinomi és irreductible sobre $\mathbb{Q}$, ja que p divideix tots els coeficients (excepte el de x^{p-1}) i p^2 no divideix el terme independent. □

Número de costats igual a un primer no de Fermat

Ara ja podem demostrar el recíproc del Teorema 5.1.

Teorema 6.6. *El polígon regular de p costats, amb p un nombre primer no de Fermat, no es pot construir.*

Demostració. Com el polinomi ciclotòmic corresponent és irreductible sobre $\mathbb{Q}$, és el polinomi mínim de les seves arrels (Teorema 6.5 i Proposició 6.4). Per tant, pel Teorema 6.2, perquè aquestes arrels es puguin construir el grau del polinomi ciclotòmic ha de ser potència de 2, i per tant p ha de ser primer de Fermat. □

Corol·lari 6.7. *Si a la descomposició en factors primers de n hi ha un primer p diferent de* 2 *i no de Fermat, llavors el polígon regular de n costats no es pot construir.*

Demostració. Si es podés construir el polígon regular de n costats amb $n = p \cdot q$, unint els vèrtexs de q en q tindríem construït un polígon regular de p costats, cosa que no pot ser. □

Número de costats igual a la potència d'un primer

Utilitzant el Teorema de Wantzel complex, Teorema 6.2, podem veure que els polígons amb un nombre de costats igual a la potència d'un primer no es poden construir. Concretament tenim:

Teorema 6.8. *El polígon de* p^a *costats, amb p primer diferent de* 2 *i* $a \neq 1$, *no es pot construir.*[15]

[14] **Criteri d'Eisenstein**. *Sigui* $P(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \in \mathbb{Z}[x]$, *i sigui* $p \in \mathbb{N}$ *un nombre primer tal que* $p \mid a_0,\ p \mid a_1,\ \ldots,\ p \mid a_{n-1}, p \nmid a_n, p^2 \nmid a_0$. *Llavors* $P(x)$ *és irreductible sobre* $\mathbb{Q}$. Vegeu, per exemple, [1], p. 220.

[15] A la secció 366 del *Disquisitiones Arithmeticae* Gauss diu: *Si el cercle s'ha de seccionar en* a^α *parts, on a designa un nombre primer, això es pot fer, evidentment, geomètricament, quan* $a = 2$, *però no per a cap altra valor de a, suposat que* $\alpha > 1$; *en efecte, llavors, a part de les equacions que es requereixen per a la secció en a parts, encara en convindrà resoldre necessàriament unes altres* $\alpha - 1$ *de grau a; i tampoc aquestes no es poden resoldre ni evitar ni rebaixar de cap manera. Així, els graus de les equacions necessàries es poden conèixer en general a partir dels factors primers del nombre* $(a-1)a^{\alpha-1}$.

Demostració. Sabem que construir les arrels d'aquest polinomi equival a construir les arrels del polinomi ciclotòmic

$$\frac{z^{p^a}-1}{z-1}.$$

Però

$$\frac{z^{p^a}-1}{z-1}=\frac{z^{p^{a-1}}-1}{z-1}\cdot\frac{z^{p^a}-1}{z^{p^{a-1}}-1}.$$

Observem que la fracció de l'esquerra i la primera de la dreta són els polinomis ciclotòmics del grau corresponent. I la segona fracció de la dreta és un polinomi (els dos polinomis que apareixen són divisibles) que es pot escriure com el ciclotòmic

$$\frac{x^p-1}{x-1},\quad x=z^{p^{a-1}}.$$

Per exemple, si $p=5$ i $a=2$, (polígon de 25 costats), tenim

$$\frac{z^{25}-1}{z-1}=z^{24}+z^{23}+\cdots+z+1=(z^4+z^3+z^2+z+1)(z^{20}+z^{15}+z^{10}+z^5+1).$$

En general, fent el canvi de variable habitual $z=y+1$ que es fa quan es vol aplicar el criteri d'Eisenstein, tenim

$$\frac{z^{p^a}-1}{z^{p^{a-1}}-1}=(y+1)^{p^{a-1}(p-1)}+(y+1)^{p^{a-1}(p-2)}+\cdots+(y+1)^{p^{a-1}}+1.$$

El terme independent és p, ja que és la suma de p uns. Per tant p^2 no divideix el terme independent i en canvi p sí que divideix a tots els coeficients excepte al de major grau que és 1. Això es pot veure aplicant la fórmula del binomi als sumands de l'expressió anterior i recordant les propietats dels números combinatoris. Però es dedueix directament de l'expressió

$$\frac{z^{p^a}-1}{z^{p^{a-1}}-1}=\frac{(y+1)^{p^a}-1}{(y+1)^{p^{a-1}}-1}=\frac{y^{p^a}+\dot{p}+1-1}{y^{p^{a-1}}+\dot{p}+1-1}=y^{p^a-p^{a-1}}+\dot{p},$$

on $\dot{p}$ vol dir múltiple de p.

Per tant, pel criteri d'Eisenstein, aquest polinomi és irreductible sobre $\mathbb{Q}$, i per la Proposició 6.4, és el polinomi mínim de les seves arrels.

Així doncs, si podéssim construir les arrels de

$$\frac{z^{p^a}-1}{z^{p^{a-1}}-1}$$

el grau d'aquest polinomi hauria de ser una potència de dos, és a dir

$$p^a-p^{a-1}=p^{a-1}(p-1)=2^k,$$

per a algun $k\in\mathbb{N}$.

Com estem suposant $a\neq 1$, ha de ser que p divideixi a 2, i com p és primer ha de ser $p=2$. Resumint, els únics polígons construïbles amb p^a costats, amb p primer i $a\neq 1$, són els que corresponen al cas $p=2$. □

Corol·lari 6.9. *Si a la descomposició en factors primers de n hi ha la potència d'un primer diferent de 2, llavors el polígon regular de n costats no es pot construir.*

Demostració. Si es podés construir el polígon regular de n costats amb $n = p^\alpha \cdot q$, unint els vèrtexs de q en q podríem construir el polígon de p^α costats, cosa que no pot ser. □

Resumim, finalment, tot el què hem dit fins aquí en el teorema següent.

Teorema 6.10 (Gauss). *El polígon regular de n costats es pot construir amb regle i compàs si i només si n té una descomposició en factors primers de la forma*

$$n = 2^\alpha (2^{2^{\alpha_1}} + 1) \cdot (2^{2^{\alpha_2}} + 1) \cdots (2^{2^{\alpha_k}} + 1)$$

on $\alpha_1, \alpha_2, ..., \alpha_k$ són enters diferents entre ells.

Demostració. La condició suficient és el Corol·lari 5.4 i la condició necessària és conseqüència dels Corol·laris 6.9 i 6.7. □

Com que la funció φ d'Euler que associa a cada $n \in \mathbb{N}$ el número de coprimers amb n, menors que n, es pot calcular a partir de la descomposició en factors primers de $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ per la fórmula (vegeu, per exemple, [1])

$$\varphi(n) = n \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right)$$

no és difícil veure que l'anterior teorema es pot enunciar dient que *el polígon regular de n costats es pot construir amb regle i compàs si i només si $\varphi(n)$ és potència de 2.*

6.1 L'heptàgon regular

Tot i que ja sabem que l'heptàgon regular no es pot construir (Teorema 6.6), donem-ne una demostració directa que ens permet no recorre al criteri d'Eisenstein.

Teorema 6.11. *L'heptàgon regular no es pot construir amb regle i compàs.*

Demostració. Ja hem comentat que equival a construir el punt $(\cos\frac{2\pi}{7}, \sin\frac{2\pi}{7}) = e^{i\frac{2\pi}{7}}$. Però aquest punt pensat com nombre complex és una arrel setena de la unitat, és a dir, solució del polinomi $z^7 - 1$. Aquest polinomi te 7 arrels, però una d'elles és $z = 1$, de manera que el problema que tenim és construir una arrel del polinomi ciclotòmic

$$\frac{z^7 - 1}{z - 1} = z^6 + z^5 + z^4 + z^3 + z^2 + z + 1.$$

El fet que $z \in \mathbb{C}$ sigui arrel d'aquest polinomi ens diu si la seva part real és solució d'un polinomi similar? Com podem trobar un polinomi que tingui com arrel la part real de z (sent z solució del ciclotòmic)? [16] Doncs molt senzill, només hem d'estudiar les potències de $z + \bar{z} = 2\mathcal{R}(z)$. Observem que com les arrels del ciclotòmic tenen mòdul 1, $\bar{z} = \frac{1}{z}$.

[16] Ja ens hem fet aquesta pregunta en el peu de pàgina 6, pàgina 9.

$$\begin{aligned}(z+\bar{z})^2 &= z^2+\bar{z}^2+2\\ (z+\bar{z})^3 &= z^3+3z+3\bar{z}+\bar{z}^3\end{aligned}$$

Equivalentment

$$\begin{aligned}(z+\bar{z})^2 &= z^2+\frac{1}{z^2}+2\\ (z+\bar{z})^3 &= z^3+3z+3\frac{1}{z}+\bar{z}^3\end{aligned}$$

i, per tant, denotant $w = z+\bar{z}$,

$$z^3(w^3+w^2-2w-1) = z^6+z^5+z^4+z^3+z^2+z+1 = 0.$$

És a dir, el nombre real $w = 2\mathcal{R}(z)$ és arrel del polinomi

$$x^3+x^2-2x-1,$$

de manera que si es pogués construir l'heptàgon podríem construir $\mathcal{R}(z)$, i per tant $2\mathcal{R}(z)$, és a dir, podriem construir l'arrel d'aquest polinomi.

Però x^3+3x^2-2x-1 és irreductible sobre $\mathbb{Q}$. Les seves arrels tenen polinomi mínim de grau 3, que no és potència de 2, i per tant no es poden construir. □

7 Els tres problemes clàssics

Duplicació del cub

Es tracta de construir, amb regle i compàs, un cub de volum doble d'un cub donat. Podem suposar que el cub donat té volum 1. Tenir donat el cub vol dir tenir construïda la seva aresta, que podem suposar doncs que és l'interval unitat OI amb $O = (0,0)$ i $I = (1,0)$.

Construir ara el cub de volum 2 equival a construir el punt $(\alpha, 0)$ amb $\alpha^3 = 2$. Si aquest punt fos construïble, pel Teorema de Wantzel, el polinomi mínim de α sobre $\mathbb{Q}$ tindria grau potència de 2.

Però el polinomi mínim de α sobre $\mathbb{Q}$ és x^3-2. En efecte, és clar que α és arrel d'aquest polinomi. I a més, aquest polinomi és irreductible sobre $\mathbb{Q}$ (i per tant, per la Proposició 6.4, és el polinomi mínim de les seves arrels).

Per veure que x^3-2 és irreductible sobre $\mathbb{Q}$ pensem que si es pogués escriure com producte de dos polinomis de graus més petits, un d'ells tindria grau 1 i per tant x^3-2 tindria una arrel racional. Si aquest nombre racional l'escrivim com p/q amb p i q primers entre ells tindríem

$$p^3 = 2q^3$$

d'on deduiríem primerament que p és parell i, simplificant un 2, que q és parell, el que és una contradicció.

Trisecció de l'angle

Es tracta de construir, amb regle i compàs, un angle igual a la tercera part d'un angle donat. Demostrarem que l'angle de $\pi/3$ de radian, que és construïble, no es pot trisecar. De fet veurem que l'angle $\pi/9$ no es pot construir.

Suposem com sempre donats els punts $O = (0,0), I = (1,0)$. Observem primerament que la construcció de l'angle $\pi/9$ és equivalent a construir el punt $(c,0)$ amb $c = \cos\frac{\pi}{9}$. La perpendicular per $(c,0)$ a la recta OI talla la circumferència de centre $(0,0)$ i radi 1 en un punt C tal que l'angle $\angle COI$ mesura $\frac{\pi}{9}$.

Ara bé, si aquest punt fos construïble, també ho seria el punt $(\beta,0)$ amb $\beta = 2c$.

Utilitzant que

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

tenim

$$\frac{1}{2} = \cos\frac{\pi}{3} = 4\cos^3\frac{\pi}{9} - 3\cos\frac{\pi}{9},$$

és a dir,

$$\beta^3 - 3\beta - 1 = 0, \qquad \text{amb } \beta = 2\cos\tfrac{\pi}{9}.$$

Com que el polinomi $x^3 - 3x - 1$ és mònic i irreductible sobre $\mathbb{Q}$, és el polinomi mínim de β. Per tant β no es pot construir. Tampoc es pot construir doncs $\beta/2 = \cos\frac{\pi}{9}$.

Per veure que $x^3 - 3x - 1$ és irreductible sobre $\mathbb{Q}$ pensem que si es pogués escriure com producte de dos polinomis de graus més petits, un d'ells tindria grau 1 i per tant $x^3 - 3x - 1$ tindria una arrel racional. Si aquest nombre racional l'escrivim com p/q amb p i q primers entre ells tindríem

$$p^3 - 3pq^2 = q^3$$

d'on deduiríem que p divideix q^3, i q^2 divideix p^3. Això implica $p = q = \pm 1$, però ± 1 no és arrel del polinomi.

Observem en particular que cap dels angles $\pi/180, \pi/90, 2\pi/90, \pi/36, \pi/18$ (1-2-4-5-10 graus) és construïble amb regle i compàs, ja que si un d'ells ho fos, podríem construir, sumant-lo repetidament, l'angle $\pi/9$ (20 graus). No obstant $\pi/60$ (3 graus) és construïble, ja que pel Teorema 6.10, el polígon de 120 costats és construïble ja que $120 = 2^3 \cdot 3 \cdot 5$ i 3 i 5 són primers de Fermat. Resumint, l'angle de m graus es pot construir si i només si $m \equiv 0 \pmod 3$.

Quadratura del cercle

Es tracta de construir, amb regle i compàs, un cercle d'àrea igual a l'àrea d'un quadrat donat. Podem suposar que el costat del quadrat donat, és a dir construït, està format pels punts $O = (0,0), I = (1,0)$ de manera que hem de construir un radi R tal que $\pi R^2 = 1$. Construir el radi R vol dir construir un segment de mesura R, o equivalentment construir el punt $(R,0) = (\frac{1}{\sqrt{\pi}},0)$. Però, com sabem construir inversos i elevar al quadrat sabríem construir el punt $(\pi,0)$ a partir de O i I.

Això voldria dir que π és arrel d'un polinomi de grau potència de 2. Però, com va demostrar Lindeman a [9], π no és arrel de cap polinomi.

8 Apèndix. Demostració del Teorema de Wantzel

En aquesta secció donem una demostració original del Teorema de Wantzel volgudament pre Artiniana[17]. En podeu trobar una demostració molt ben explicada pels mètodes habituals a l'article de Josep Pla, [10].

Anem a veure com són les coordenades dels punts que anem construint amb regle i compàs a partir de la referència ortonormal O, I, J construïda al pàgina 17.

Per exemple, anem a construir un primer punt P tallant la circumferència $\mathcal{C}$ de centre I i radi IO amb la recta OI. Clarament $P = (2, 0)$, i podem dir, en particular, que les coordenades de P són nombres enters. Amb un procediment semblant podem construir tots els punts $(m, 0)$ amb $m \in Z$.

Per construir un punt Q fora de la recta OI tallem, per exemple, l'anterior circumferència $\mathcal{C}$ amb la circumferència de centre O i radi OI.

Resolent el sistema

$$\begin{aligned} x^2 + y^2 &= 1 \\ (x-1)^2 + y^2 &= 1 \end{aligned}$$

obtenim $Q = (\frac{1}{2}, \frac{\sqrt{3}}{2})$.

Les coordenades de Q ja no són nombres enters. La primera coordenada és racional però la segona no. Podríem dir simplement que la segona coordenada és un nombre real, però serem una mica més precisos i direm que les coordenades de Q pertanyen a un conjunt que està entre $\mathbb{Q}$ i $\mathbb{R}$, que denotem $\mathbb{Q}(\sqrt{3})$, i que està format per tots els nombres reals que es poden escriure com

$$\mathbb{Q}(\sqrt{3}) = \{p + q\sqrt{3}, \quad p, q \in \mathbb{Q}\}.$$

Dona la casualitat de que quan sumem o multipliquem elements de $\mathbb{Q}(\sqrt{3})$ obtenim elements de $\mathbb{Q}(\sqrt{3})$. En efecte, si $a, b, c, d \in \mathbb{Q}$,

$$(a + b\sqrt{3}) \cdot (c + d\sqrt{3}) = ac + 3bd + (ad + bc)\sqrt{3}, \quad ac + 3bd, ad + bc \in \mathbb{Q},$$

I que l'invers d'un element de $\mathbb{Q}(\sqrt{3})$ és també un element de $\mathbb{Q}(\sqrt{3})$. En efecte, multiplicant pel 'conjugat' tenim,

$$\frac{1}{a + b\sqrt{3}} = \frac{a - b\sqrt{3}}{a^2 - 3b^2} = \alpha + \beta\sqrt{3}, \quad \alpha, \beta \in \mathbb{Q}.$$

Per això es diu $\mathbb{Q}(\sqrt{3})$ és un cos, o més concretament que és un subcos de $\mathbb{R}$.

[17] El 1942 Emil Artin va reformular la teoria de Galois que es coneixia en el seu dia en llenguatge d'espais vectorials, vegeu [2]. Però el preu que es va pagar va ser un elevat grau d'abstracció i una dificultat per als estudiants que perdien l'origen i la motivació. A més, alguns punts molt importants com la resolvent de Lagrange o la resolvent del propi Galois quedaven amagats. En particular no he volgut utilitzar la fórmula dels graus, la que diu que si $K \subset L \subset M$ són tres cossos llavors $[M : K] = [M : L][L : K]$ (recordem que $[M : K]$ vol dir la dimensió de M com a K-espai vectorial). Si aquests cossos provenen de K adjuntant primer l'arrel d'un polinomi amb coeficients a K, $L = K(\alpha)$, i adjuntant a continuació l'arrel β d'un polinomi a coeficients $K(\alpha)$, $M = K(\alpha)(\beta)$ la fórmula dels graus ens diu que el grau del polinomi mínim de β sobre K, $P(x)$, és el producte del grau del polinomi mínim de β sobre $K(\alpha)$ pel grau del polinomi mínim de α sobre K, però no ens diu qui és el polinomi $P(x)$. Vegeu la Proposició 8.3 i els teoremes posteriors.

Observem que tots els elements de $\mathbb{Q}(\sqrt{3})$ es poden construir amb regle i compàs. En efecte, ja hem vist que els racionals i $\sqrt{3}$ són construïbles i per construir el producte $(p/q)\sqrt{3}$ només hem de saber dividir un segment construït (en aquest cas $\sqrt{3}$) en q parts iguals. Això és fàcil de fer utilitzant el teorema de Tales.

Observem finalment que el paper jugat per $\sqrt{3}$ pot ser jugat per qualsevol altre número real que sigui arrel d'una equació de segon grau. Concretament, si $\alpha \in \mathbb{R}$ te polinomi mínim de grau 2 sobre $\mathbb{Q}$, podem considerar el subcos de $\mathbb{R}$ format pel conjunt d'expressions $a + b\alpha$, amb $a, b \in \mathbb{Q}$, amb el producte induït pel polinomi mínim de α. És a dir, si el polinomi mínim de α és $x^2 + px + q = 0$, amb $p, q \in \mathbb{Q}$, llavors

$$(a + b\alpha)(c + d\alpha) = ac + (ad + bc)\alpha + bd(-p\alpha - q).$$

Aquest cos el denotarem per $\mathbb{Q}(\alpha)$.

8.1 Cos associat a un conjunt de punts construïts

Generalitzem l'exemple anterior a la construcció de diversos punts.

Sigui C_0 un conjunt de punts del pla construïts amb regle i compàs. Associem a C_0 el subcòs $\mathbb{K}_0$ de $\mathbb{R}$ generat per les coordenades, tant la x com la y, de tots els punts de C_0. Quan diem 'subcos generat' volem dir el conjunt format per tots els nombres reals que podem obtenir sumant, multiplicant, i fent inversos amb les coordenades dels punts de C_0.

Per exemple, si considerem que C_0 és el conjunt format únicament pels punts $O = (0, 0)$ i $I = (1, 0)$, llavors $K_0 = \mathbb{Q}$, ja que el 0 i l'1, per sumes, productes i inversos generen $\mathbb{Q}$.

Si considerem que C_0 és el conjunt format pels punts O, I, Q de l'exemple anterior, llavors $K_0 = \mathbb{Q}(\sqrt{3})$, ja que el 0, l'1, i $\sqrt{3}$ per sumes, productes i inversos generen $\mathbb{Q}(\sqrt{3})$.

Definició 8.1. *Direm que un punt $P = (x_1, y_1)$ és* construïble en un pas a partir de C_0 *si es pot obtenir per intersecció de figures (rectes o circumferències) construïdes amb els punts de C_0.*

Les rectes que podem construir són les determinades per dos punts de C_0, i les circumferències les que tenen centre en un punt de C_0 i radi un segment format per dos punts de C_0.

Un cop el conjunt C_0 ha quedat ampliat amb la construcció d'un nou punt P, el cos associat al nou conjunt $C_1 = C_0 \cup P$ és també una ampliació del cos K_0, obtinguda afegint als elements de K_0 les coordenades de P i totes les sumes, productes i inversos necessaris per obtenir un cos. Aquest nou cos, el més petit que conté $\mathbb{K}_0, x_1, y_1$ es denota per $\mathbb{K}_1 = \mathbb{K}_0(x_1, y_1)$. Observem que $\mathbb{K}_1$ podria eventualment coincidir amb $\mathbb{K}_0$.

Així definim inductivament cossos

$$\mathbb{K}_i = \mathbb{K}_{i-1}(x_i, y_i)$$

que corresponen al procés d'adjuntar a $\mathbb{K}_{i-1}$ les coordenades d'un punt construït en un pas a partir de C_{i-1}.

Proposició 8.2. *Les coordenades x_i i y_i d'un punt construït en un pas a partir de C_{i-1} són zeros de polinomis lineals o quadràtics a coeficients $\mathbb{K}_{i-1}$.*

Demostració. Estudiem primerament el cas *recta* $\cap$ *circumferència* ja que el cas *recta* $\cap$ *recta* és molt simple. Siguin A, B, C punts de coordenades $(p, q), (r, s), (t, u)$ ja construïts, és a dir del conjunt C_{i-1}. Per definició, les coordenades pertanyen a $\mathbb{K}_{i-1}$. Tallar la recta AB amb la circumferència de centre C i radi ρ, donat per la distància entre punts de C_{i-1}, equival a resoldre el sistema

$$\begin{aligned} \frac{x-p}{r-p} &= \frac{y-q}{s-q}, \\ (x-t)^2+(y-u)^2 &= \rho^2. \end{aligned}$$

Aïllant y a la primera equació, i substituint a la segona tenim

$$(x-t)^2+(\frac{s-q}{r-p}(x-p)+q-u)^2=\rho^2. \tag{5}$$

Com ρ és la distància entre punts de C_{i-1}, tenim que $\rho^2 \in \mathbb{K}_{i-1}$, i per tant x (i també y, ja que depèn linealment de x) és zero d'un polinomi de grau 2 a coeficients $\mathbb{K}_{i-1}$.

Estudiem ara el cas *circumferència* $\cap$ *circumferència*. Per les mateixes consideracions que anteriorment hem de resoldre un sistema del tipus

$$\begin{aligned} (x-s)^2+(y-v)^2 &= \eta^2, \\ (x-t)^2+(y-u)^2 &= \rho^2, \end{aligned}$$

amb $s, t, u, v, \rho^2, \eta^2 \in \mathbb{K}_{i-1}$.

Aïllant[18] y a la primera equació, i substituint a la segona tenim

$$(x-t)^2+\left(v-u+\sqrt{\eta^2-(x-s)^2}\right)^2=\rho^2.$$

Equivalentment

$$(x-t)^2+(v-u)^2+\eta^2-(x-s)^2+2(v-u)\sqrt{\eta^2-(x-s)^2}=\rho^2.$$

I el que fa que les 'coses funcionin' és justament que el terme x^2 d'aquesta equació desapareix, de manera que aquesta equació es pot escriure com

$$A+Bx=2(v-u)\sqrt{\eta^2-(x-s)^2}, \quad A, B \in \mathbb{K}_{i-1}.$$

Elevant al quadrat

$$(A+Bx)^2=4(v-u)^2(\eta^2-(x-s)^2) \tag{6}$$

tenim el resultat, és a dir, x és zero d'un polinomi quadràtic amb coeficients a K_{i-1}. $\square$

Observem que si $v \neq u$ aquesta darrera fórmula ens diu que y depèn $\mathbb{K}_{i-1}$-linealment de x, concretament

$$A+Bx=2(v-u)(y-v)$$

de manera que $\mathbb{K}_{i-1}(x, y)=\mathbb{K}_{i-1}(x)$. Si $v=u$, x és un zero d'un polinomi lineal a coeficients $\mathbb{K}_{i-1}$ i per tant $x \in \mathbb{K}_{i-1}$, i $\mathbb{K}_{i-1}(x, y)=\mathbb{K}(y)$. Això vol dir que en cada pas, és a dir, per a cada punt que es construeix, el cos ampliat és una extensió simple del cos anterior obtinguda adjuntant l'abscissa x o l'ordenada y del punt construït.

[18] Restant les dues equacions de les circumferències aquest cas es redueix a l'anterior.

8.2 Punts construïts en dos passos

Suposem que a partir d'un conjunt de punts construïts C_{i-1} hem passat, per un pas, a un conjunt de punts construïts C_i, i que novament per un pas hem passat a un conjunt de punts construïts C_{i+1}. Això ens ha donat lloc als tres cossos

$$\mathbb{K}_{i-1} \subseteq \mathbb{K}_i \subseteq \mathbb{K}_{i+1},$$

generats per les coordenades dels punts construïts.

Ja hem vist que podem considerar que aquestes extensions són simples, és a dir,

$$\mathbb{K}_i = \mathbb{K}_{i-1}(\alpha_{i-1}) \quad \text{i} \quad \mathbb{K}_{i+1} = \mathbb{K}_i(\alpha_i),$$

on α_{i-1} és l'abscissa o l'ordenada del primer punt construït i α_i l'abscissa o l'ordenada del segon punt construït. I sabem que el polinomi mínim de α_i sobre $\mathbb{K}_i$ té grau 1 o 2.

Proposició 8.3. *Sigui $\mathbb{K}$ el cos associat a un conjunt C de punts construïts amb regle i compàs. Sigui α l'abscissa o l'ordenada d'un punt A construït a partir de C en un pas. Sigui β l'abscissa o l'ordenada d'un punt B construït a partir de $C \cup A$ en un pas. Llavors el polinomi mínim de β sobre $\mathbb{K}$ té grau potència de 2 (1, 2 o 4).*

Demostració.[19] Sabem que el polinomi mínim de α sobre $\mathbb{K}$ té grau 1 o 2. I sabem també que el polinomi mínim de β sobre $\mathbb{K}(\alpha)$ té grau 1 o 2.

Estudiem únicament el cas en que tots dos polinomis mínims tenen grau 2. Els altres cassos són similars.

Sigui

$$P(x) = x^2 + (a + b\alpha)x + (c + d\alpha), \quad a, b, c, d \in \mathbb{K},$$

el polinomi mínim de β sobre $\mathbb{K}(\alpha)$. L'escrivim com

$$P(x) = P_2(x) + \alpha P_1(x),$$

amb

$$P_2(x) = x^2 + ax + c \in \mathbb{K}[x], \quad P_1(x) = bx + d \in \mathbb{K}[x].$$

Podem suposar que $P_1(x)$ no és el polinomi zero ja que llavors $P(x) \in \mathbb{K}[x]$, i per tant el polinomi mínim de β sobre $\mathbb{K}$ té grau 2 i hem acabat. Suposarem, doncs, a partir d'ara, que b o d són diferents de zero.

Sigui α' la segona arrel del polinomi mínim $x^2 + px + q$ de α sobre $\mathbb{K}$. És a dir, $\alpha + \alpha' = -p$, $\alpha \cdot \alpha' = q$. El fet de ser $\alpha \notin \mathbb{K}$ implica $\alpha \neq \alpha'$. Denotem $P'(x) = P_2(x) + \alpha' P_1(x)$.

Afirmem que el polinomi mínim de β sobre $\mathbb{K}$ és

$$P_4(x) = P(x)P'(x).$$

En efecte, hem de veure que aquest polinomi compleix tres coses: que admet β com arrel, que els seus coeficients estan a $\mathbb{K}$, i que és irreductible sobre $\mathbb{K}$.

[19] És una demostració directa, sense usar el llenguatge Artinià d'espais vectorials, de la fórmula dels graus $[\mathbb{K}(\alpha, \beta) : \mathbb{K}] = [\mathbb{K}(\alpha, \beta) : \mathbb{K}(\alpha)][\mathbb{K}(\alpha) : \mathbb{K}]$ on s'expliciten els polinomis mínims.

1) $P_4(x)$ *admet* β *com arrel.* Això és evident, ja que $P(\beta) = 0$.

2) *Els coeficients de* $P_4(x)$ *pertanyen a* $\mathbb{K}$, i.e. $P_4(x) \in \mathbb{K}[x]$. Això es veu directament, ja que en efectuar el producte de $P(x)$ per $P'(x)$ obtenim

$$P_4(x) = P_2(x)^2 - p\,P_2(x)\,P_1(x) + q\,P_1(x)^2$$

i $p, q \in \mathbb{K}$. Observem doncs que $P_4(x)$ *és un polinomi de* $\mathbb{K}[x]$ *que és producte de dos polinomis de* $\mathbb{K}(\alpha)[x]$.

3) $P_4(x)$ *és irreductible sobre* $\mathbb{K}$. Per veure això suposem, per l'absurd, que $P_4(x)$ fos reductible. Llavors tindríem

$$P_4(x) = A(x) \cdot B(x), \quad A(x), B(x) \in \mathbb{K}[x],$$

amb ni $A(x)$ ni $B(x)$ constants, i β hauria de ser arrel d'un d'aquests polinomis. Suposem que ho és de $A(x)$, i.e. $A(\beta) = 0$.

Com $\mathbb{K} \subset \mathbb{K}(\alpha)$ podem pensar que tant $A(x)$ com $P(x)$ són polinomis a coeficients $\mathbb{K}(\alpha)$. Com $P(x)$ és el mínim de β sobre $\mathbb{K}(\alpha)$, ha de ser

$$A(x) = \mu(x) \cdot P(x) \quad \text{amb} \quad \mu(x) \in \mathbb{K}(\alpha)[x],$$

ja que *sí un polinomi té una arrel en comú amb el polinomi mínim és un múltiple d'aquest.*

Sigui β' l'arrel de $P'(x)$ que s'obté canviant formalment en l'expressió quadràtica de β, α per α'. Concretament, si

$$\beta \;=\; \frac{-a - b\alpha + \sqrt{(a+b\alpha)^2 - 4(c+d\alpha)}}{2}$$

llavors

$$\beta' \;=\; \frac{-a - b\alpha' + \sqrt{(a+b\alpha')^2 - 4(c+d\alpha')}}{2}$$

Com que estem suposant b o d diferents de zero es pot veure que $\beta \neq \beta'$. Observem que $P'(x)$ és el polinomi mínim de β' sobre $\mathbb{K}(\alpha)$. Això implica que $P(\beta') \neq 0$, ja que si β' fos arrel de $P(x)$ aquest seria múltiple de $P'(x)$, cosa que no pot ser.

Com que $P_4(\beta') = 0$, tenim dos casos segons β' sigui arrel de $A(x)$ o de $B(x)$:

Primer cas. β' és arrel de $B(x)$. Llavors $B(x) = \lambda(x)P'(x)$ per ser $P'(x)$ el polinomi mínim de β'. Però llavors tindríem

$$P(x)P'(x) = A(x)B(x) = \mu(x)\lambda(x)P(x)P'(x)$$

la qual cosa implica que $\mu(x) = \lambda(x) = 1$, és a dir $A(x) = P(x)$, cosa que no pot ser ja que $P(x) \notin \mathbb{K}[x]$.

Segon cas. β' és arrel de $A(x)$. Llavors ha de ser $\mu(\beta') = 0$. Això implica, coma abans, que $\mu(x) = \nu(x)P'(x)$. Però llavors tindríem

$$P(x)P'(x) = A(x)B(x) = \nu(x)P'(x)P(x)B(x)$$

la qual cosa implica que $\nu(x) \cdot B(x) = 1$, contradicció, ja que grau $B(x) \geq 1$.

Com en els dos casos hem arribar a contradicció això vol dir que $P_4(x)$ és irreductible sobre $\mathbb{K}$. Per tant és el polinomi mínim de les seves arrels. És a dir, el polinomi mínim de β sobre $\mathbb{K}$ té grau 4, com volíem demostrar. $\square$.

8.3 Punts construïts en k passos

Denotem $\mathbb{K}_0 = \mathbb{Q}$ el cos associat al conjunt $C_0 = \{(0,0),(1,0)\}$, i definim inductivament cossos $\mathbb{K}_{i+1} = \mathbb{K}_i(\alpha_i)$ adjuntant a cada cos $\mathbb{K}_i$ l'abscissa o l'ordenada $\alpha_i \in \mathbb{R}$ d'un punt construït a partir de C_i per un pas. Recordem que el cos estès amb l'abscissa i l'ordenada del punt construït coincideix amb el cos estès amb l'abscissa o l'ordenada del punt. És a dir, sempre podem pensar que tenim extensions simples.

Observem que tota α_j és una expressió 'racional quadràtica' de $\alpha_0, \alpha_1, \ldots, \alpha_{j-1}$. És a dir, una expressió formada per sumes, productes i radicals quadràtics d'expressions $\mathbb{Q}$-lineals en les α_l anteriors.

Teorema 8.4 (Wantzel). *Sigui α_{j+k} l'abscissa o l'ordenada d'un punt construït en $k+j$ passos a partir de $C_0 = \{(0,0),(1,0)\}$.*

Per a tot $j \in \mathbb{N}$, i per a tot $k \in \mathbb{N}$, α_{j+k} té polinomi mínim de grau potència de dos sobre $\mathbb{K}_j$.

En particular, prenent $j = 0$, veiem que el polinomi mínim sobre $\mathbb{Q}$, tant de l'abscissa com de l'ordenada d'un punt construit en k passos a partir de $\mathcal{C}_0$, té grau potència de dos.

Demostració. Per inducció sobre k. Si $k = 0$ hem de demostrar que per a tot $j \in \mathbb{N}$, α_j té polinomi mínim de grau potència de dos sobre $\mathbb{K}_j$, la qual cosa és certa per la definició d'α_j.

Suposem, per hipòtesi d'inducció, el resultat cert fins a k.

Volem demostrar que per a tot $j \in \mathbb{N}$, α_{j+k+1} té polinomi mínim de grau potència de dos sobre $\mathbb{K}_j$.

Apliquem la hipòtesi d'inducció per a $j+1$. Això vol dir que α_{j+1+k} té polinomi mínim de grau potència de dos sobre $\mathbb{K}_{j+1}$. Denotem aquest polinomi per

$$P(x) = x^{2^{k+1}} + \Sigma a_r x^r, \quad a_r \in \mathbb{K}_{j+1} = \mathbb{K}_j(\alpha_j).$$

I ara l'escrivim com

$$P(x) = P_2(x) + \alpha_j P_1(x), \quad P_2(x), P_1(x) \in \mathbb{K}_j[x],$$

simplement tenint en compte que $a_r = b_r + c_r\alpha_j$, amb $b_r, c_r \in \mathbb{K}_j$.

Afirmem que el polinomi mínim de α_{j+k+1} sobre $\mathbb{K}_j$ és

$$R(x) = (P_2(x) + \alpha_j P_1(x)) \cdot (P_2(x) + \alpha_j' P_1(x)).$$

En efecte, hem de veure que aquest polinomi compleix tres coses: que admet α_{j+k+1} com arrel, que els seus coeficients estan a $\mathbb{K}_j$, i que és irreductible sobre $\mathbb{K}_j$.

1) *$R(x)$ admet α_{j+k+1} com arrel.* Això és evident, ja que $P(\alpha_{j+k+1}) = 0$.

2) *Els coeficients de $R(x)$ pertanyen a $\mathbb{K}_j$*, i.e. $R(x) \in \mathbb{K}_j[x]$. Això es veu directament, ja que en efectuar el producte indicat obtenim

$$R(x) = P_2(x)^2 - pP_2(x)P_1(x) + qP_1(x)P_1(x) \in \mathbb{K}_j[x],$$

amb

$$p = \alpha_j + \alpha_j' \in \mathbb{K}_j, \ q = \alpha_j\alpha_j' \in \mathbb{K}_j.$$

Observem doncs que $R(x)$ *és un polinomi de* $\mathbb{K}_j[x]$ *que és producte de dos polinomis de* $\mathbb{K}_{j+1}[x]$.

3) $R(x)$ *és irreductible sobre* $\mathbb{K}$. Mateixos arguments que a la demostració de la proposició 8.3.

Com $R(x)$ té grau potència de 2, hem acabat. □

Finalment donem la idea de la demostració del teorema 6.2, que hem anomenat Teorema de Wantzel complex.

Teorema 8.5. *Suposem que el punt z del pla complex, amb $|z| = 1$, ha estat construït. Llavors el polinomi de grau més petit que admet z com arrel té grau potència de dos.*

Demostració. Posem $z = a + bi$. Si hem construït z també podem construir a i, pel Teorema de Wantzel, a és arrel d'un polinomi $P(x) \in \mathbb{Q}[x]$ de grau m igual a potència de 2. Observem que z és arrel del polinomi

$$T(x) = x^2 - 2ax + 1 \in \mathbb{Q}(a)[x].$$

Siguin $a = r_1, r_2, \ldots, r_m$ les arrels de $P(x)$. Llavors el polinomi

$$S(x) = \prod_{i=1}^{m} (x^2 + 1 - 2xr_i) \in \mathbb{Q}[x]$$

té grau $2m$, per tant potència de 2, admet z com arrel, i és irreductible sobre $\mathbb{Q}$ (això s'ha de provar, pero és essencialment el mateix raonament que a la demostració de la proposició 8.3). Per tant, és el polinomi mínim de z sobre $\mathbb{Q}$.

Que $S(x) \in \mathbb{Q}[x]$, és a dir, que els seus coeficients són racionals, és conseqüència de que a l'efectuar els productes indicats van apareixen les funcions simètriques elementals de les r_i, que pertanyen a $\mathbb{Q}$, ja que són els coeficients de $P(x)$.

Per exemple, si $m = 2$, posant $M = M(x) = x^2 + 1 \in \mathbb{Q}[x]$ i $N = N(x) = 2x \in \mathbb{Q}[x]$ tenim

$$(M - r_1 N)(M - r_2 N) = M^2 - (r_1 + r_2)MN - r_1 r_2 N^2 \in \mathbb{Q}[x]$$

ja que $r_1 + r_2$ i $r_1 r_2$ són racionals. □

Observem que el teorema de Wantzel no diu que les arrels de polinomis de grau potència de 2 i coeficients racionals es puguin construir. Per exemple, es pot veure sense massa dificultat que el polinomi $x^4 - x - 1$ té almenys una arrel real no construïble, vegeu per exemple [10] o [3].

Agraïments. Estic molt agraït a Rosa Camps per les moltes i molt útils converses al voltant de Teoria de Galois que hem mantingut durant la preparació d'aquest treball. I també a Eduard Gallego, Judit Abardia i Ferran Cedó per haver fet una primera lectura del mateix.

Departament de Matemàtiques
Universitat Autònoma de Barcelona
08193 Bellaterra (Cerdanyola del Vallès).
agusti@mat.uab.cat.

Referències

[1] R. Antoine, R. Camps, J. Moncasi (2007). *Introducció a l'Àlgebra abstracta*. Manuals UAB, Vol. 46.

[2] E. Artin (1970). *La Teoria de Galois*. Vicens-Vives. Primera edició (1942): Galois Theory. Lectures Delivered at the University of Notre Dame, Notre Dame Mathematical Lectures, 2.

[3] J. C. Carrega (1981). *Théorie des Corps. La règle et le Compas*. Hermann, París.

[4] H. S. Carslaw (1909). Gauss's Theorem on the Regular Polygons which can be constructed by Euclid's Method. *Proceedings of the Edinburgh Mathematical Society,* 121-128.

[5] F. Enriques (1900). *Questioni riguardanti la Geometria Elementare*. Nicola Zanichelli, Bologna. Federigo Enriques és l'editor i autor d'alguns dels capítols d'aquesta obra en dos volums. Hi participen entre d'altres U. Amaldi, E. Baroni, R. Bonola, B. Calò, G. Castelnuovo, A. Conti, E. Daniele, A. Giacomini, A. Guarducci, G. Vitale.

[6] Euclides (s. III aC). *Elements*. Podeu consultar *The Thirteen Books of Euclid's Elements*, Dover Publications (1956), comentats per T. L. Heath, o bé [13], p. 702-980.

[7] C. F. Gauss (1801). *Disquisitiones Arithmeticae*. Lipsiae, Gerh. Fleisher. Traducció catalana a càrrec de Griselda Pascual Xufré, *Disquisicions Aritmètiques*, Societat Catalana de Matemàtiques (1996).

[8] D. Kuh (2013). Constructible regular n-gons. *Senior Project Archive 2013, Withman College, USA,* 1-36.

[9] F. Lindeman (1882). Über die Zahl π. *Mathematische Annalen, 20,* 213-225.

[10] J. Pla (2006). L'àlgebra de la papiroflexia. *Butlletí de la Societat Catalana de Matemàtiques, 21,* 81-155.

[11] A. Reventós (1993). *Geometria axiomàtica*. Institut d'Estudis Catalans, vol. CVI. Segona Edició a càrrec de la Societat Catalana de Matemàtiques (2010), vol. 5.

[12] I. Stewart (2004). *Galois Theory*. Chapman and Hall. Tercera edició. Primera edició 1973.

[13] F. Vera (1970). *Científicos griegos*. Aguilar.

[14] P. L. Wantzel (1837). Recherches sur le moyens de reconnaître si un Problème de Géométrie peut se résoudre avec la règle et le compas. *J. de Mathématiques Pures et Appliquées,* 366-372.