Universitat Autònoma de Barcelona
Treball de Fi de Grau 2019-2020

Àlex Miranda Pascual

Polígons Construïbles més enllà del Regle i Compàs

Tutor: Roberto Rubio Núñez

		3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Resum

Presentem, de manera independent, una generalització de les construccions amb regle i compàs per altres conjunts d'eines, i estudiem quins polígons regulars són construïbles amb aquests conjunts. En el cas clàssic del regle i compàs, desenvolupem i completem els arguments de Gauss per entendre els passos previs de la prova del Teorema de Gauss-Wantzel. Estudiem quins són els polígons construïbles amb regle i compàs de puntes, regle marcat, regle i p-sectors, i regle marcat i compàs. En aquesta darrera construcció, també parlem de quins problemes de construccions encara estan oberts i veiem altres recentment resolts.

Abstract

We present, in an independent way, a generalization of ruler and compass constructions for other sets of tools, and we study which regular polygons are constructible with these sets. In the classic case of ruler and compass, we develop and complete Gauss' arguments to understand the previous steps in the proof of the Gauss-Wantzel theorem. We study which are the constructible polygons with ruler and dividers, marked ruler, ruler and p-sectors, and marked ruler and compass. In the latter one, we also talk about what construction problems are still open and see others recently solved.

Agraïments

Vull expressar al meu agraïment cap a molta gent sense la qual aquest Treball de Fi de Grau no hagués estat possible. En primer lloc, s'agraeix moltíssim l'ajuda del tutor d'aquest treball, Roberto Rubio, gràcies a qui el treball ha pres forma i a qui se l'aprecia l'esforç i l'interès que ha dedicat en aquest en resoldre problemes i donar consells. També vull donar gràcies a la meva família i els meus amics i amigues, a qui se'ls agraeix l'ajuda durant el treball. Finalment, també es vol agrair l'esforç dels professors i professores del departament de matemàtiques, que han influït en el meu pas durant el curs.

Índex

1 Introducció **2**

2 Les construccions de l'antiga Grècia **3**

3 Una generalització dels punts construïbles **5**

4 La divisió de l'angle **10**

5 La construcció de polígons regulars **13**

6 El teorema de Gauss-Wantzel **19**

7 Els teoremes de Mohr-Mascheroni i Poncelet-Steiner **21**

8 Construccions amb regle i compàs de puntes **22**

9 Construccions amb regle marcat **26**

10 Construccions amb regle marcat i compàs **33**

11 Construccions amb regle i p-sectors **34**

12 Taula de polígons construïbles **35**

1 Introducció

La construcció de polígons regulars amb regle i compàs ha captivat les matemàtiques durant segles. Els matemàtics de l'antiga Grècia sabien construir amb aquestes eines el triangle, el quadrat i el pentàgon regular, així com construir un polígon amb el doble de costats que un ja donat. Sorgia aleshores la següent pregunta clàssica: quins polígons regulars són construïbles amb regle i compàs. En l'any 1798 Gauss va donar a *Disquisitiones arithmeticae* una condició de suficiència per garantir quan un polígon és construïble on també va afegir que era la condició de necessitat, malgrat que mai no ho va provar. Quaranta anys després, Wantzel va provar la condició restant, provant l'anomenat teorema de Gauss-Wantzel i posant un punt final al problema de la construcció de polígons regulars amb regle i compàs. No obstant això, la mateixa pregunta es podia fer per construccions amb altres conjunts d'eines de dibuix, com ara el compàs de puntes o el regle marcat.

En aquest treball mirarem quins polígons regulars són construïbles més enllà del regle i compàs, és a dir, amb altres conjunts d'eines. La gran majoria de les construccions de les quals parlarem en el treball estan prèviament descrites en *Geometric Constructions* de Martin, una de les principals referències d'aquest treball. Nosaltres ens centrarem, però, en la part de construccions de polígons regulars.

Tot i que un treball d'aquestes característiques no demana resultats originals, s'ha volgut explicar gran part del treball de manera independent, amb definicions i resultats propis i provant resultats que s'enunciaven sense prova. Part d'aquest treball consisteix en una generalització de construccions geomètriques i del problema de la construcció dels polígons regulars, que s'han creat de manera original a partir d'una col·lecció de referències. Això ha fet que l'avenç sigui més lent, però ha proporcionat un punt de vista molt més interessant en l'àmbit matemàtic que una simple recopilació de teoremes.

Després d'una introducció sobre les construccions amb regle i compàs, donem en la Secció 3 una generalització d'aquestes, que com hem dit, és una part original del treball. Parlarem dels punts construïbles i fixarem hipòtesis sobre aquestes construccions de manera que puguem enfocar el problema des d'un punt algebraic, mitjançant teoria d'extensions algebraiques de cossos i de Galois. Les Seccions 4 i 5 consistiran en una generalització, també original, de la teoria de Gauss, amb la finalitat d'entendre-la i proporcionar demostracions, utilitzant una teoria més moderna, d'aquells resultats que Gauss no provava.

Aquests resultats ens permetran explicitar quines condicions han de complir un conjunt d'eines per tal de garantir quan un polígon regular és construïble o no, i donarem una prova del teorema de Gauss-Wantzel (Secció 6), seguint els passos que explicava Gauss, que serà una demostració alternativa (però equivalent) a la popularment utilitzada. Amb aquesta prova donem importància al valor històric dels resultats de Gauss, i l'incloem en comptes de l'actual, que és més directa, ja que es considera que és un resultat conegut, habitual d'una assignatura de teoria de Galois.

En el treball també parlarem d'algunes construccions que són equivalents a les construccions amb regle i compàs, però que a priori no ho semblen, com ara les construccions amb compàs (Secció 7). Aquesta secció motivarà preguntar-nos si existeix un conjunt d'eines que ens permet construir tot polígon construïble, però que no ens permeti construir tot punt construïble amb regle i compàs. En la

Secció 8 veurem que les construccions amb regle i compàs de puntes compleixen aquestes hipòtesis.

A més parlarem de construccions més potents que les construccions amb regle i compàs, com per exemple, les construccions amb regle marcat (Secció 9), que ens permetrà construir més punts i polígons regulars que amb regle i compàs. Parlarem de les construccions amb regle marcat i compàs (Secció 10), on encara hi ha polígons regulars que no se saben si són o no construïbles amb aquestes eines. Comentarem també la construcció de l'hendecàgon regular, un resultat provat recentment en 2014, i acabarem el treball fent un comentari final de les construccions amb p-sectors (Secció 11).

2 Les construccions de l'antiga Grècia

La recta i la circumferència van ser les primeres línies, en un sentit ample, mai construïdes pels humans. A l'antic Egipte, els experts en geometria utilitzaven cordes per construir aquestes línies sobre el terra: estiraven una corda entre dos punts per construir una recta, i feien girar un punt respecte a un altre que estava fix per construir una circumferència [7]. Aquestes dues corbes, la recta i la circumferència, segueixen definint i estant molt presents en la geometria euclidiana, la geometria definida a partir dels postulats dels *Elements* d'Euclides, basats en rectes i circumferències. Per aquest treball ens interessarà recordar els primers tres postulats d'Euclides [5]:

I. És possible unir dos punts per un segment rectilini.

II. És possible allargar contínuament qualsevol segment rectilini.

III. És possible descriure una circumferència amb qualsevol centre i qualsevol radi.

Malgrat els nombrosos instruments que existeixen per construir una multitud de construccions geomètriques, els geòmetres teòrics segueixen utilitzant dos instruments senzills, el regle i compàs, que els permeten dibuixar rectes i circumferències. Com ja és ben sabut, quan s'utilitzen els mots *regle* i *compàs*, no ens estem referint al regle i al compàs que tots hem tingut, sinó a uns instruments teòrics directament relacionats amb els postulats d'Euclides.

El regle d'Euclides és de longitud infinita i sense marques, que no permet marcar ni mesurar cap distància, però sí dibuixar un segment entre dos punts, i estendre qualsevol segment de manera indefinida. Veiem que els dos primers postulats d'Euclides ens diuen què es pot fer amb aquest regle. D'altra banda, el tercer postulat ens diu quines construccions es poden realitzar amb el compàs: es podran construir circumferències centrades en qualsevol punt i que passen per qualsevol altre, però no es podrà transportar distàncies directament.

Amb aquestes eines es poden realitzar totes les construccions que es realitzen a partir dels primers tres postulats d'Euclides, que inclouen totes les construccions descrites en aquests primers sis llibres dels *Elements* [5, 9]. En només el primer llibre ja tenim construccions geomètriques elementals com la bisecció d'un angle (I.9), la bisecció d'un segment (I.10), la construcció d'una recta perpendicular (I.11 i I.12) i la construcció de rectes paral·leles (I.31).

La construcció de polígons regulars també va interessar a grecs com Euclides. Les construccions amb regle i compàs del triangle equilàter, del quadrat, del

pentàgon i del pentadecàgon regular apareixen al quart llibre dels *Elements*. A més, com sabien bisecar l'angle, també podien construir un polígon amb el doble nombre de costats. En resum, els grecs sabien construir qualsevol polígon regular amb $3 \cdot 2^\alpha$, $4 \cdot 2^\alpha$, $5 \cdot 2^\alpha$ o $15 \cdot 2^\alpha$ nombre de costas (per qualsevol $\alpha \geq 0$), incloent-hi l'hexàgon, l'octàgon i el decàgon regulars, entre altres.

Els grecs no van poder donar construccions amb regle i compàs per la resta de polígons regulars, ni tan sols van poder provar si realment eren o no construïbles. La construcció dels polígons regulars de 7, 9, 11, 13 i 17 costats s'afegien als tres problemes clàssics no resolts pels grecs sobre les construccions amb regle i compàs:

1. La quadratura del cercle: Donat un cercle, es pot construir un quadrat de la mateixa àrea?

2. La trisecció de l'angle: Donat un angle, es pot dividir en tres parts iguals?

3. La duplicació del cub: Donat un cub, es pot construir un altre que tingui el doble d'àrea que el primer?

Tots aquests problemes van romandre sense resposta fins al final del segle XVIII, quan un jove i desconegut Gauss va donar una condició de suficiència per garantir quan un polígon regular és construïble amb regle i compàs. Gauss també va conjecturar que la mateixa condició era necessària, però mai va publicar cap demostració, i no va ser fins quaranta anys després quan Wantzel la va proporcionar.

La demostració d'aquest resultat, conegut actualment com el teorema de Gauss-Wantzel, partia d'una altra reinterpretació de les construccions amb regle i compàs, que era inimaginable pels grecs de l'antiguitat. Gauss i Wantzel van adonar-se que les construccions amb regle i compàs s'associaven a unes certes extensions algebraiques de cossos. Abans de veure el teorema donarem una definició formal de les diverses construccions amb regle i compàs.

Definició 2.1 (Punt construïble amb regle i compàs)**.** En el pla de coordenades cartesianes $\mathbb{R}^2$, diem que un punt P és construïble amb regle i compàs, o simplement, construïble, si és l'últim terme P_n d'una successió finita de punts: $P_{-1}, P_0, P_1, \ldots, P_n$, on $P_{-1} = (0,0)$ i $P_0 = (1,0)$ són els punts base i on P_i per tot $i > 0$ és un dels següents:

i) El punt d'intersecció de dues rectes secants formades per punts previs a P_i en la successió.

ii) Un dels punts d'intersecció d'una recta formada per punts previs a P_i en la successió i d'una circumferència centrada i que passa per punts previs a P_i en la successió.

iii) Un dels punts d'intersecció de dues circumferències diferents centrades i que passen per punts previs a P_i en la successió.

La idea darrere les construccions amb regle i compàs consisteix a estudiar quin és el conjunt de les coordenades dels punts construïbles amb regle i compàs. En la següent secció generalitzarem aquestes construccions, i comentarem més endavant els resultats importants que es dedueixen. No obstant això, presentem ara el teorema de Gauss-Wantzel:

Teorema 2.2 (Teorema de Gauss-Wantzel)**.** *Sigui $n \geq 3$. Aleshores, el polígon regular de n costats és construïble amb regle i compàs si i només si $n = 2^a p_1 \cdots p_k$ amb $a \geq 0$ i $p_1, \ldots, p_k$ primers de Fermat diferents.*

Els primers de Fermat es defineixen com els primers de la forma $F_n = 2^{2^n} + 1$. En realitat la demostració és vàlida per qualsevol primer de la forma $2^m + 1$, però Fermat es va adonar, ja en temps de Gauss [6], que tots els primers senars de la forma $2^m + 1$ havien de ser necessàriament de la forma $2^{2^n} + 1$. Actualment només es coneixen 5 primers de Fermat:

$$F_0 = 3, \quad F_1 = 5, \quad F_2 = 17, \quad F_3 = 257 \ \text{ i } \ F_4 = 65537,$$

i se sap que els nombres F_n per $5 \leq n \leq 30$ no són primers. També es pensa que no n'hi ha cap més, però la pregunta encara segueix oberta. Aquest teorema donava la resposta a la pregunta que es formulaven els grecs, obtenint que l'heptàgon, el nonàgon i l'hendecàgon regulars no són construïbles, però que en canvi l'heptadecàgon sí.

3 Una generalització dels punts construïbles

Generalitzarem les construccions amb regle i compàs de manera que ens serveixin per a qualsevol eina de dibuix (regle, compàs, regle marcat, n-sector d'angles...) suposant unes hipòtesis bàsiques. Donats uns punts del pla cartesià $\mathbb{R}^2$, podrem realitzar certes construccions sobre el pla definides per la natura d'aquestes eines: és a dir, quan parlem de construccions amb regle, podrem construir la recta entre dos punts, mentre que quan parlem de construccions amb bisector, podrem bisecar tot angle donat. Aquesta interpretació està relacionada amb els punts construïbles del pla $\mathbb{R}^2$ per cada eina (o conjunt d'eines). Donat un conjunt de punts base, podem construir més punts mitjançant construccions elementals donades per aquestes eines, per exemple, direm que un punt és construïble amb regle si és el punt d'intersecció de dues rectes formades per punts prèviament construïts, i que un punt és construïble amb compàs si és un dels punts d'intersecció de dues circumferències.

La idea fonamental darrere de tota construcció és d'estudiar els punts que són construïbles amb el conjunt d'eines, i no altres corbes associades, com ara les rectes o circumferències. Donarem una definició formal i abstracta dels punts construïbles amb un conjunt d'eines, però sempre s'haurà de tindre en compte la idea intuïtiva darrere d'aquesta definició.

Definició 3.1 (Punts construïbles)**.** Anomenem conjunt d'eines a un conjunt d'aplicacions $f_1, \ldots, f_n$ tals que $f_j : (\mathbb{R}^2)^{m_j} \longrightarrow \mathcal{P}^*(\mathbb{R}^2)$ on $m_j \in \mathbb{N}$ i $\mathcal{P}^*(\mathbb{R}^2)$ denota el conjunt de parts finites de $\mathbb{R}^2$. A més, associem a cada conjunt d'eines un conjunt finit de punts $\{P_{-l}, P_{-l+1}, \ldots, P_{-1}, P_0\} \subset \mathbb{R}^2$ anomenats punts base a partir dels quals podrem construir la resta de punts. Denotarem al conjunt d'eines com $\mathscr{E}$.

Direm que P és un punt construïble amb $\mathscr{E}$, o simplement un punt de $\mathscr{E}$, si és l'últim punt d'una successió finita $\{P_{-l}, P_{-l+1}, \ldots, P_{-1}, P_0, P_1, \ldots, P_n\}$ de punts de $\mathbb{R}^2$ tal que P_k per tot $k > 0$ és un element de $f_j(Q_1, \ldots, Q_{m_j})$ per un cert j i uns certs $Q_1, \ldots, Q_{m_j}$, que són punts previs a P_k en la successió.

Veiem un exemple d'aquesta definició amb les construccions amb regle, on es construeixen nous punts mitjançant la intersecció de rectes secants. Per tant, podrem definir les construccions amb regle com l'aplicació $f_1 : (\mathbb{R}^2)^4 \longrightarrow \mathcal{P}^*(\mathbb{R}^2)$ de manera que $f_1(A, B, C, D)$ equivalgui al punt d'intersecció de les rectes $\overleftrightarrow{AB}$ i $\overleftrightarrow{CD}$, si aquestes són secants, o al conjunt buit sinó. Fixem-nos que aquesta aplicació no és més que una formalització de la idea intuïtiva de les construccions amb regle.

Definim també les rectes i circumferències construïbles amb $\mathscr{E}$, o, simplement, de $\mathscr{E}$. Direm que una recta del pla cartesià és de $\mathscr{E}$ si la recta passa per dos punts diferents de $\mathscr{E}$, i direm que una circumferència del pla cartesià és de $\mathscr{E}$ si està centrada i que passa per punts diferents de $\mathscr{E}$. S'ha de notar que aquestes nocions són un concepte teòric i que necessàriament no s'han de poder dibuixar o construir físicament amb les eines de $\mathscr{E}$, és a dir, amb aquesta definició tindrà sentit parlar de rectes de compàs malgrat que no es poden dibuixar rectes amb compàs. Per tant, s'ha de tindre en compte que quan diem que construïm una recta o circumferència, generalment estem donant una definició teòrica, i no pas una definició física.

En aquest treball, per garantir bons resultats suposarem unes quantes hipòtesis bàsiques sobre les construccions i els punts de $\mathscr{E}$, i desenvoluparem la teoria a partir d'aquestes hipòtesis, en comptes de la definició precedent. Recordem que els punts construïbles seran punts del pla cartesià $\mathbb{R}^2$ i per tant els escriurem també com (p, q) per $p, q \in \mathbb{R}$. Les construccions amb $\mathscr{E}$ amb les quals treballarem compliran aquestes tres hipòtesis

I. Els punts $(0, 0)$, $(1, 0)$ i $(0, 1)$ són de $\mathscr{E}$.

II. El punt d'intersecció de dues rectes secants de $\mathscr{E}$ és un punt de $\mathscr{E}$.

III. La recta perpendicular a una recta de $\mathscr{E}$ i que passa per un punt de $\mathscr{E}$ és de $\mathscr{E}$.

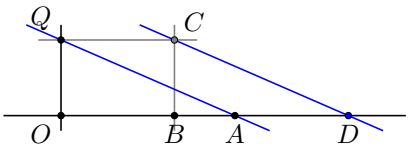
Remarquem que existeixen construccions que no compleixen aquestes hipòtesis, notablement, les construccions amb compàs oxidat, del qual no parlarem en aquest treball, però que es pot trobar a [12, Ch. 7].

Algunes de les conseqüències directes de les hipòtesis són que els eixos d'abscisses i ordenades són rectes de $\mathscr{E}$, i que tota recta paral·lela a una recta de $\mathscr{E}$ i que passa per un punt de $\mathscr{E}$ és de $\mathscr{E}$ (s'obté mitjançant la construcció de dues perpendiculars). A més, construint perpendiculars als eixos obtenim que (p, q) és de $\mathscr{E}$ si i només si $(p, 0)$ i $(0, q)$ ho són; i construint rectes paral·leles a la recta que passa per $(0, 1)$ i $(1, 0)$, obtenim que per tot $p \in \mathbb{R}$, $(p, 0)$ és de $\mathscr{E}$ si i només si $(0, p)$ ho és.

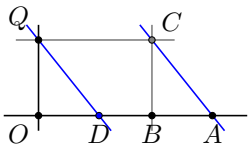
Ens interessarà saber quins valors prendran les coordenades dels punts de $\mathscr{E}$. Direm que un nombre $x \in \mathbb{R}$ és construïble amb $\mathscr{E}$, o simplement de $\mathscr{E}$, si el punt $(x, 0)$ és de $\mathscr{E}$, (on recordem que x, y són de $\mathscr{E}$ si i només si (x, y) és un punt de $\mathscr{E}$). Ens agradarà poder extreure resultats sobre el conjunt de nombres de $\mathscr{E}$, que denotarem E. En el següent teorema veurem que E serà un cos si $\mathscr{E}$ compleix les hipòtesis anteriors, i d'aquesta manera podrem arribar a resultats sobre la construcció de polígons regulars mitjançant la teoria d'extensions de cossos.

Teorema 3.2. *El conjunt de nombres de $\mathscr{E}$, on $\mathscr{E}$ compleix les hipòtesis prèvies, és un cos.*

Demostració. Sabem que $0, 1 \in E$ per la hipòtesi I sobre $\mathscr{E}$. Veurem que E és tancat per la suma, resta, multiplicació i divisió per un nombre diferent de 0. D'aquesta manera obtindrem que E és un cos.

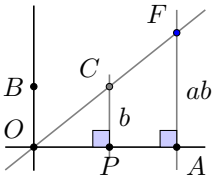


(a) Suma

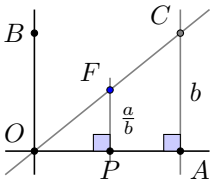


(b) Resta

Siguin $a, b \in E$, veiem que $a + b \in E$. Seguirem la construcció que es mostra en la figura (a). Tenim que $A = (a, 0)$, $B = (b, 0)$ i $Q = (0, 1)$ són punts de $\mathscr{E}$, i per tant $C = (b, 1)$ també ho és. Construïm la recta que passa per Q i A, i construïm la recta paral·lela a aquesta que passa per C. Aleshores, el punt d'intersecció d'aquesta darrera recta amb l'eix d'abscisses és $D = (a + b, 0)$, i per tant $a + b \in E$. Veure que $a - b \in E$ donats $a, b \in E$ resulta anàleg: només haurem de construir la recta que passa per C i A i construir la paral·lela a aquesta que passa per Q, tal com es veu en la figura (b).



(c) Multiplicació



(d) Divisió

Siguin $a, b \in E$, veiem que $ab \in E$. Com abans, seguirem la construcció que es mostra en la figura (c). Com $a, b \in E$, $A = (a, 0)$, $B = (0, b)$, $P = (1, 0)$ i $C = (1, b)$ són punts de $\mathscr{E}$. Construïm la perpendicular a l'eix d'abscisses que passa per A i la recta que passa per l'origen O i C, i veiem que es tallen en el punt $F = (a, ab)$, i per tant, $ab \in E$. El fet que la segona coordenada de F és $|AF| = ab$ és conseqüència del teorema de Tales, ja que

$$\frac{|PC|}{|OP|} = \frac{|AF|}{|OA|} \iff \frac{b}{1} = \frac{|AF|}{a} \iff |AF| = ab.$$

Seguint la construcció de la figura (d) de forma anàloga, obtenim que $\frac{a}{b} \in E$ per $b \neq 0$. $\square$

Deduïm directament del teorema que es pot bisecar tot segment, ja que donats $A = (a, b)$ i $C = (c, d)$, el punt que biseca el segment $\overline{AC}$ és $(\frac{a+c}{2}, \frac{b+d}{2})$. Notem que el Teorema 3.2 no és cert si les hipòtesis sobre $\mathscr{E}$ no es compleixen, com podem comprovar amb el conjunt de nombres construïbles amb compàs oxidat a [12, Ch. 7].

Recordem ara que el cos més petit de característica 0 és $\mathbb{Q}$ i per tant $\mathbb{Q} \subseteq E \subseteq \mathbb{R}$. En conseqüència, tenim que E sempre és un cos real i per tant ordenat.

Tots els cossos amb els quals treballarem en les següents pàgines seran cossos de característica 0, i per tant extensions de $\mathbb{Q}$. La majoria també seran reals ($K \subseteq \mathbb{R}$), i per això, en aquests casos tindrà sentit parlar del subconjunt de nombres positius de K que denotarem com K^+. Donada una extensió de cossos $K \subseteq L$, denotem el grau de l'extensió com $[L : K]$. Quan l'extensió és algebraica i simple, és a dir, quan existeix un nombre algebraic α tal que $L = K(\alpha)$, tenim que el grau de l'extensió correspon al grau del polinomi mònic $p(x)$ irreductible en $K[x]$ (l'anell de polinomis amb coeficients a K) tal que $p(\alpha) = 0$, que denotem $\mathrm{Irr}(\alpha, K)[x]$. Si $K \subseteq K(\alpha)$ és una extensió de grau N, aleshores $\{1, \alpha, \alpha^2, \cdots, \alpha^{N-1}\}$ és una K-base per $K(\alpha)$.

Anomenem torre de cossos sobre K_0 a les extensions iterades sobre K_0, és a dir, a una successió de cossos tals que $K_0 \subseteq K_1 \subseteq \cdots \subseteq K_n$. Recordem que la fórmula de les torres ens donarà una manera d'expressar el grau de $K_0 \subseteq K_n$ en funció de les extensions intermediàries:

$$[K_n : K_0] = [K_n : K_{n-1}][K_{n-1} : K_{n-2}] \cdots [K_1 : K_0].$$

Com les rectes i circumferències de $\mathscr{E}$ són rectes i circumferències del pla cartesià, les podem escriure com $\{(X, Y) \mid aX + bY = c\}$ i $\{(X, Y) \mid (X - d)^2 + (Y - e)^2 = f^2\}$ respectivament, per uns certs coeficients $a, b, c, d, e, f \in \mathbb{R}$. Més específicament,

Proposició 3.3. *Les equacions de tota recta i circumferència de $\mathscr{E}$ es poden expressar de manera que els seus coeficients estiguin en funció de les coordenades dels punts de $\mathscr{E}$ que defineixen la recta i circumferència.*

Demostració. Donat $A = (a, b)$ i $C = (c, d)$ dos punts diferents de $\mathscr{E}$. Aleshores, l'equació de la recta que passa per A i C és $r = \{(X, Y) \mid (b - d)x + (c - a)y = cb - da\}$, i la circumferència centrada a A i que passa per C és $\{(X, Y) \mid (X - a)^2 + (Y - b)^2 = (a - c)^2 + (b - d)^2\}$, d'on es dedueix l'enunciat. $\square$

A més, com E és un cos, obtenim que aquests coeficients sempre són a E.

Com sabem, els grecs no van poder dir quines condicions s'havien de complir per poder construir un polígon regular de n costats. Demostrar-ho geomètricament no és gens fàcil, però si passem al món de l'àlgebra, obtindrem resultats més senzills. La idea darrere la demostració del teorema de Gauss-Wantzel, i per generalització, darrere de les construccions per quasi qualsevol altre conjunt d'eines, s'amaga en la següent observació.

Si $P = (x, y)$ és un punt de $\mathscr{E}$, aleshores, per definició, existeix una successió finita de punts $P_{-l}, P_{-l+1}, \ldots, P_{-1}, P_0, P_1, \ldots, P_n$ tal que $P = P_n$ està definit en funció dels anteriors. En general, si per tot k, K_k és el mínim cos que conté totes les coordenades dels punts $P_{-l}, P_{-l+1}, \ldots, P_{-1}, P_0, P_1, \ldots, P_k$, aleshores podrem dir que

$$[K_{n-1}(x, y) : K_{n-1}] \leq N$$

per un cert $N \in \mathbb{N}$, que no depèn dels punts de la successió. En conseqüència, com la cota no depèn de n ni del punt, si $P_k = (x_k, y_k)$ per $k > 0$ aleshores

$$[K_{k-1}(x_k, y_k) : K_{k-1}] \leq N$$

i recursivament tindrem que $[K_n : K_0]$ serà producte de primers més petits o iguals a N.

Serà important poder calcular N per les diferents construccions de les quals parlem; per exemple tindrem que $N = 1$ per les construccions amb regle, $N = 2$ per les de regle i compàs i $N = 4$ per les de regle marcat. Trobar aquests valors ens permetrà dir quins reals són a E i quins no, en particular, tot nombre de E haurà de ser un element d'un cos $K_n \subset \mathbb{R}$ tal que existeixi una torre de cossos

$$K_0 \subseteq K_1 \subseteq \cdots \subseteq K_n$$

tal que $[K_{i+1} : K_i] \leq N$ per tot i.

Veiem com podem utilitzar aquest fet amb un dels exemples més senzills que tenim: els punts construïbles amb regle, que equival quan $N = 1$. Formalment, la definició de punt de regle no serà massa diferent de la de punt construïble amb regle i compàs (2.1), però només acceptarem punts en la successió sota el punt i) de la definició, i haurem de partir de quatre punts base que no formen un paral·lelogram: $(1, 0)$, $(2, 0)$, $(0, 1)$ i $(0, 2)$.

Teorema 3.4. *El conjunt dels nombres de regle és $\mathbb{Q}$.*

Demostració. Comencem comentant que les construccions amb regle compleixen les hipòtesis I, II i III. Les primeres dues hipòtesis les podem deduir de la definició de punt de regle, però la demostració que es pot construir tota perpendicular només amb regle no és tan senzilla. Martin ens dona una construcció en el seu llibre [12, Th. 4.14], que aquí no inclourem. Per tant, el conjunt de punts E de regle és un cos $\mathbb{Q} \subseteq E$.

Veurem que tot punt de regle té coordenades racionals. Per definició, si $P = (x, y)$ és un punt de $\mathscr{E}$, aleshores existeix una successió finita de punts $P_{-3}, P_{-2}, \ldots, P_n$ tal que $P = P_n$ és el punt d'intersecció de dues rectes formades per punts previs a P en la successió. Siguin $r = \{(X, Y) \mid aX + bY = c\}$ i $s = \{(X, Y) \mid dX + eY = f\}$ aquestes dues rectes, que sabem que tenen coeficients en K_{n-1} per la Proposició 3.3. Aleshores tenim que

$$ax + by = c \qquad \text{i} \qquad dx + ey = f,$$

i aïllant ens dona

$$(x, y) = \left(\frac{bf - ce}{bd - ae}, \frac{cd - af}{bd - ae}\right)$$

que són valors ben definits, ja que $bd - ae = 0$ implicaria que les dues rectes són paral·leles o coincidents. D'aquesta manera obtenim que

$$[K_n : K_{n-1}] = [K_{n-1}(x, y) : K_{n-1}] = 1,$$

i recursivament,

$$[K_n : K_0] = 1^n = 1.$$

Fixem-nos que els coeficients dels punts base són racionals, és a dir, $K_0 = \mathbb{Q}$, i per tant $K_k = \mathbb{Q}$ per tot k. Per tant, el conjunt de punts de regle és $\mathbb{Q}$ i tot punt té coordenades racionals. □

Com a conseqüència, tenim que les hipòtesis I, II i III de $\mathscr{E}$ equivalen a les dues següents

I*. Els punts $(1, 0)$, $(2, 0)$, $(0, 1)$ i $(0, 2)$ són de $\mathscr{E}$.

II*. El punt d'intersecció de dues rectes secants de $\mathscr{E}$ és un punt de $\mathscr{E}$.

Notem que podríem haver substituït les hipòtesis I, II i III per aquestes, però es considera que l'equivalència no és trivial i que les primeres són més intuïtives.

4 La divisió de l'angle

Per entendre la construcció de polígons regulars haurem d'entendre primer la divisió de l'angle amb les eines que tenim.

Donats tres punts A, P, B diferents, podem definir al pla cartesià l'angle $\angle(A, P, B)$ com l'angle entre les semirectes $\overrightarrow{PA}$ i $\overrightarrow{PB}$ (amb P com a vèrtex), mesurat en radians de $\overrightarrow{PA}$ a $\overrightarrow{PB}$ en sentit antihorari. Ens fixem que $\angle(A', P, B) = \angle(A, P, B)$ per qualsevol punt $A' \neq P$ en la semirecta $\overrightarrow{PA}$ i anàlogament el mateix resultat per tot punt de $\overrightarrow{PB}$. Denotarem la mesura d'un angle $\angle(A, P, B)$ com $\theta = |\angle(A, P, B)|$, mesurat en radians. Com els angles de θ i $\theta + 2\pi k$ radians són equivalents per tot $k \in \mathbb{Z}$, donarem sempre a θ el valor corresponent de $(0, 2\pi]$.

Donats dos punts de $\mathscr{E}$ diferents, P i A, direm que l'angle amb vèrtex P i que forma un angle de θ radians (on $\theta \in (0, 2\pi]$) amb la semirecta $\overrightarrow{PA}$ és construïble amb $\mathscr{E}$ si existeix un punt B de $\mathscr{E}$ tal que $|\angle(A, P, B)| = \theta$. Direm que un angle de $\mathscr{E}$ es pot n-secar ($n \geq 2$) si es poden construir $(n-1)$ rectes de $\mathscr{E}$ que divideixin l'angle en n parts iguals.

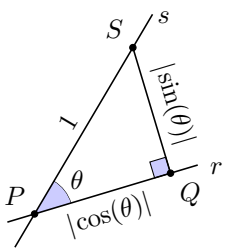
En particular, podrem construir un angle amb vèrtex a l'origen i que forma un angle θ amb el semieix positiu d'abscisses si el punt $(\cos(\theta), \sin(\theta))$ és de $\mathscr{E}$. No obstant això, el recíproc no és cert, ja que per exemple podem construir l'angle de $\frac{\pi}{4}$ amb regle, però el punt $(\cos(\frac{\pi}{4}), \sin(\frac{\pi}{4})) = (\frac{\sqrt{2}}{2}, \frac{\sqrt{2}}{2})$ no és de regle (3.4). Si suposem aquesta quarta hipòtesi sobre $\mathscr{E}$, que ens permetrà traslladar distàncies en el pla cartesià, el recíproc serà cert:

IV. Donada una recta de $\mathscr{E}$ que passa per un punt P de $\mathscr{E}$, aleshores el punt Q sobre la recta és de $\mathscr{E}$ si i només si la distància entre P i Q, $|PQ|$, és a E^+.

Com hem comentat, les construccions amb regle no compleixen aquesta hipòtesi, i es pot veure que amb regle i compàs sí que la compleix (utilitzant el compàs i la translació de segments mitjançant paral·leles). En la Secció 8 introduirem unes construccions equivalents a només complir les hipòtesis I, II, III i IV. Sota la hipòtesi IV tindrem aquest resultat:

Proposició 4.1. *Suposem que $\mathscr{E}$ compleix la hipòtesi IV. Siguin P, A punts diferents de $\mathscr{E}$ i $\theta \in (0, 2\pi]$, aleshores existeix un punt B de $\mathscr{E}$ tal que $|\angle(A, P, B)| = \theta$ si i només si $\cos(\theta), \sin(\theta) \in E$.*

Demostració. Els casos on $\theta = \pi, 2\pi$ són clars. Denotem la recta $r = \overleftrightarrow{PA}$, per la resta de casos. En totes dues implicacions seguirem la figura de sota, que corresponent a quan $\theta \in (0, \frac{\pi}{2}]$.



Suposem primer que $\cos(\theta), \sin(\theta) \in E$, aleshores $|\cos(\theta)|, |\sin(\theta)| \in E^+$, i, per la hipòtesi IV, podem construir el punt Q sobre la recta r a distància $|\cos(\theta)|$

de P (que estarà sobre la semirecta $\overrightarrow{PA}$ si $\cos(\theta) \geq 0$, i sobre l'altra semirecta si $\cos(\theta) \leq 0$). Després construïm la recta perpendicular a r per Q i de la mateixa manera construïm el punt S a distància $|\sin(\theta)|$ de Q sobre la perpendicular (tenint en compte el signe com abans). Així obtenim un punt S de $\mathscr{E}$ tal que $|\angle(A, P, S)| = \theta$.

Veiem ara l'altra implicació. Com θ és un angle de $\mathscr{E}$, existeix una recta s de $\mathscr{E}$ que talla la recta r en el punt P formant un angle θ. Construïm el punt S sobre s a distància 1 de P (utilitzant la hipòtesi IV), i construïm la recta perpendicular a r que passa per S, que talla r en un punt Q. La distància entre P i Q és $|\cos(\theta)|$, mentre que la distància entre Q i S és $|\sin(\theta)|$, per tant $|\cos(\theta)|, |\sin(\theta)| \in E$ per la hipòtesi IV. Finalment, com E és un cos, obtenim que $\cos(\theta), \sin(\theta) \in E$. □

Aquest resultat no és necessàriament cert si la hipòtesi IV no es compleix. Com hem comentat, les construccions amb regle ens proporcionen un contraexemple. Ens fixem llavors que si $\mathscr{E}$ compleix la hipòtesi IV, aleshores

$$\big(\cos(\tfrac{\theta}{n}), \sin(\tfrac{\theta}{n})\big), \big(\cos(2\tfrac{\theta}{n}), \sin(2\tfrac{\theta}{n})\big), \ldots, \big(\cos((n-1)\tfrac{\theta}{n}), \sin((n-1)\tfrac{\theta}{n})\big)$$

són de $\mathscr{E}$ si i només si podem n-secar l'angle θ. Aquesta equivalència serà necessària per a la construcció dels polígons regulars, i per tant, a partir d'ara considerarem que $\mathscr{E}$ sempre compleix la hipòtesi IV, no obstant això, cal remarcar sense aquesta hipòtesi, tindrem l'angle θ de $\mathscr{E}$ del tipus $\angle((1,0),(0,0),B)$ es pot n-secar si els punts anteriors són de $\mathscr{E}$. Comentem també que el cas on $\theta = 2\pi$ consisteix en la divisió de la circumferència unitat en n parts iguals.

A continuació parlarem del càlcul d'aquests punts des d'un punt de vista algebraic.

Lema 4.2. *Siguin K un cos, $n \in \mathbb{N}$ i $\theta \in [0, 2\pi]$. Suposem que $\cos(\frac{\theta}{n}), \sin(\frac{\theta}{n}) \in K$, aleshores $\cos(m\frac{\theta}{n}), \sin(m\frac{\theta}{n}) \in K$ per tot $m \in \mathbb{Z}$.*

Demostració. Està clar que l'enunciat és cert per $m = 0$. Recordem les següents dues expressions sobre suma d'angles,

$$\sin(\alpha \pm \beta) = \sin(\alpha)\cos(\beta) \pm \cos(\alpha)\sin(\beta)$$
$$\cos(\alpha \pm \beta) = \cos(\alpha)\cos(\beta) \mp \sin(\alpha)\sin(\beta).$$

Denotem $\alpha = \frac{\theta}{n}$ i suposem que $\cos(\alpha)$ i $\sin(\alpha)$ són a K, aleshores

$$\sin(2\alpha) = \sin\big((1+1)\alpha\big) = 2\sin(\alpha)\cos(\alpha)$$
$$\cos(2\alpha) = \cos\big((1+1)\alpha\big) = \cos^2(\alpha) - \sin^2(\alpha)$$

i per tant, $\cos(2\alpha)$ i $\sin(2\alpha)$ són a K. Recursivament, obtenim que

$$\sin(m\alpha) = \sin\big((m-1)\alpha\big)\cos(\alpha) + \cos\big((m-1)\alpha\big)\sin(\alpha)$$
$$\cos(m\alpha) = \cos\big((m-1)\alpha\big)\cos(\alpha) - \sin\big((m-1)\alpha\big)\sin(\alpha)$$

i per tant $\cos(m\alpha), \sin(m\alpha) \in K$ per tot $m \in \mathbb{N} \cup \{0\}$, i finalment, com cos i sin són funcions parell i senar, respectivament, obtenim que el resultat és cert per tot $m \in \mathbb{Z}$. □

Per tant, donat un angle θ de $\mathscr{E}$, tenim que $\cos(\frac{\theta}{n}), \sin(\frac{\theta}{n}) \in E$ si i només si l'angle es pot n-secar. Ens agradarà poder simplificar aquest resultat en p-seccions per tot p primer divisor de n, per tant, introduïm aquest resultat

Proposició 4.3. *Siguin K un cos i $n = ab \in \mathbb{N}$ on a i b són coprimers entre ells. Aleshores, $\cos(\frac{\theta}{n}), \sin(\frac{\theta}{n}) \in K$ si i només si $\cos(\frac{\theta}{a}), \sin(\frac{\theta}{a}), \cos(\frac{\theta}{b}), \sin(\frac{\theta}{b}) \in K$.*

Demostració. Suposant que $\cos(\frac{\theta}{n}), \sin(\frac{\theta}{n}) \in K$, aleshores $\cos(\frac{b\theta}{n}) = \cos(\frac{\theta}{a})$ i $\cos(\frac{a\theta}{n}) = \cos(\frac{\theta}{b})$ (i les expressions equivalents pel sin) són a K, pel Lema 4.2.

Veiem l'altra implicació. Com $n = ab$ on a i b són coprimers tenim que

$$\frac{1}{n} = \frac{\alpha}{a} + \frac{\beta}{b}$$

per certs $\alpha, \beta \in \mathbb{Z}$ no nuls. Pel Lema 4.2, com $\cos(\frac{\theta}{a}), \sin(\frac{\theta}{a}), \cos(\frac{\theta}{b}), \sin(\frac{\theta}{b}) \in K$, tenim que $\cos(\frac{\alpha\theta}{a}), \sin(\frac{\alpha\theta}{a}), \cos(\frac{\beta\theta}{b}), \sin(\frac{\beta\theta}{b}) \in K$. Aleshores

$$\begin{aligned} \sin(\tfrac{\theta}{n}) &= \sin(\tfrac{\alpha\theta}{a})\cos(\tfrac{\beta\theta}{b}) + \cos(\tfrac{\alpha\theta}{a})\sin(\tfrac{\beta\theta}{b}) \in K, \\ \cos(\tfrac{\theta}{n}) &= \cos(\tfrac{\alpha\theta}{a})\cos(\tfrac{\beta\theta}{b}) - \sin(\tfrac{\alpha\theta}{a})\sin(\tfrac{\beta\theta}{b}) \in K. \end{aligned}$$

□

Corol·lari 4.4. *Siguin K un cos, $\theta \in [0, 2\pi]$ i $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ la descomposició de n en primers, aleshores $\sin(\frac{\theta}{n}), \cos(\frac{\theta}{n}) \in K$ si i només si $\sin(\frac{\theta}{p_i^{\alpha_i}}), \cos(\frac{\theta}{p_i^{\alpha_i}}) \in K$ per tot i.*

En conseqüència, obtenim que un angle de $\mathscr{E}$ es pot n-secar si i només si es pot p^α-secar per cada primer en multiplicitat màxima p^α que divideix n. A més, resulta evident que si podem p-secar els angles de $\mathscr{E}$, aleshores també els podem p^k-secar, per tot k; però el recíproc no és cert. L'única informació addicional que podem aportar al tema és la Proposició 4.6, que ens diu que per p-secar un angle hem de resoldre com a màxim un polinomi de grau p.

Si recordem que $\mathbb{R}^2 \cong \mathbb{C}$, podrem fer una relació entre els punts del pla cartesià i els nombres complexos. Recordem que tot complex es pot escriure de la forma $z = a + \mathrm{i}b$ amb $a, b \in \mathbb{R}$ o $z = r\mathrm{e}^{\mathrm{i}\theta}$ amb $r \geq 0$ i $\theta \in (0, 2\pi]$, i per tant tenim podem definir la relació coneguda $z \sim (a, b) = (r\cos(\theta), r\sin(\theta))$ entre el pla complex i cartesià. Els següents resultats ens determinen també una relació entre el pla complex i el cartesià en termes d'extensions de cossos. Mencionem que aquests resultats són de construcció pròpia.

Lema 4.5. *Siguin $z, w \in \mathbb{C}$ amb $z = a + \mathrm{i}b$ i $w = c + \mathrm{i}d$, $a, b, c, d \in \mathbb{R}$, tals que $|z|^2, |w|^2 \in \mathbb{Q}$ i tal que $\mathbb{Q}(z) \subseteq \mathbb{Q}(w)$ sigui una extensió finita de cossos. Aleshores $\mathbb{Q}(a, b) \subseteq \mathbb{Q}(c, d)$ és també una extensió finita de cossos que compleix*

$$[\mathbb{Q}(w) : \mathbb{Q}(z)] = \varepsilon[\mathbb{Q}(c, d) : \mathbb{Q}(a, b)],$$

on $\varepsilon = 2$ si $\mathrm{i} \in \mathbb{Q}(w) \backslash \mathbb{Q}(z)$, i $\varepsilon = 1$ altrament.

Demostració. Considerem l'extensió de cossos $\mathbb{Q}(a, b) \subseteq \mathbb{Q}(a, b, \mathrm{i})$ i veiem que $\mathbb{Q}(a, b, \mathrm{i}) = \mathbb{Q}(z, \mathrm{i})$, ja que

$$a = \frac{1}{2}\left(z + \frac{|z|^2}{z}\right) \in \mathbb{Q}(z, \mathrm{i}) \qquad \text{i} \qquad b = \frac{1}{2\mathrm{i}}\left(z - \frac{|z|^2}{z}\right) \in \mathbb{Q}(z, \mathrm{i})$$

i $z = a + \mathrm{i}b \in \mathbb{Q}(a, b, \mathrm{i})$ (la igualtat també és certa quan $z = 0$). Per tant, tenim que $\mathbb{Q}(a, b) \subset \mathbb{Q}(z, \mathrm{i}) = \mathbb{Q}(a, b, \mathrm{i})$ és una extensió de grau 2, perquè $\mathrm{Irr}(\mathrm{i}, \mathbb{Q}(a, b))[x] =$

x^2+1, ja que $\mathbb{Q}(a,b)\subset\mathbb{R}$. De manera anàloga, obtenim que $\mathbb{Q}(c,d)\subset\mathbb{Q}(w,\mathrm{i})$ és una extensió de grau 2. A més, com $\mathbb{Q}(z)\subseteq\mathbb{Q}(w)$ és una extensió finita, existeixen $n\in\mathbb{N}$ i $a_0,\dots,a_n\in\mathbb{Q}$ tals que $z=a_0+a_1w+\cdots+a_nw^n$, i igualant les parts reals i imaginàries de z, obtenim que $\mathbb{Q}(a,b)\subseteq\mathbb{Q}(c,d)$. Aleshores, per la fórmula de les torres,

$$[\mathbb{Q}(w,\mathrm{i}):\mathbb{Q}(c,d)][\mathbb{Q}(c,d):\mathbb{Q}(a,b)]=[\mathbb{Q}(w,\mathrm{i}):\mathbb{Q}(z,\mathrm{i})][\mathbb{Q}(z,\mathrm{i}):\mathbb{Q}(a,b)],$$

d'on obtenim que $[\mathbb{Q}(c,d):\mathbb{Q}(a,b)]=[\mathbb{Q}(w,\mathrm{i}):\mathbb{Q}(z,\mathrm{i})]$. Considerem ara les extensions de cossos $\mathbb{Q}(z)\subseteq\mathbb{Q}(z,\mathrm{i})$ i $\mathbb{Q}(w)\subseteq\mathbb{Q}(w,\mathrm{i})$ que sabem que tenen grau 2 com a màxim. Més específicament, $\mathbb{Q}(z)\subseteq\mathbb{Q}(z,\mathrm{i})$ té grau 1 si i només si $\mathrm{i}\in\mathbb{Q}(z)$ (i anàlogament per $\mathbb{Q}(w)\subseteq\mathbb{Q}(w,\mathrm{i})$). Ens fixem que si $\mathrm{i}\in\mathbb{Q}(z)$ aleshores $\mathrm{i}\in\mathbb{Q}(w)$, i per tant,

$$\varepsilon=\frac{[\mathbb{Q}(z,\mathrm{i}):\mathbb{Q}(z)]}{[\mathbb{Q}(w,\mathrm{i}):\mathbb{Q}(w)]}$$

val 2 si i només si $\mathrm{i}\in\mathbb{Q}(w)\backslash\mathbb{Q}(z)$, i 1 en la resta de casos. En conclusió, per la fórmula de les torres,

$$[\mathbb{Q}(w,\mathrm{i}):\mathbb{Q}(z,\mathrm{i})][\mathbb{Q}(z,\mathrm{i}):\mathbb{Q}(z)]=[\mathbb{Q}(w,\mathrm{i}):\mathbb{Q}(w)][\mathbb{Q}(w):\mathbb{Q}(z)],$$

i aïllant obtenim el resultat que buscàvem:

$$[\mathbb{Q}(w):\mathbb{Q}(z)]=\varepsilon[\mathbb{Q}(c,d):\mathbb{Q}(a,b)].\qquad\square$$

Proposició 4.6. *Siguin p un primer i $\theta\in(0,2\pi]$. Aleshores, $\mathbb{Q}(\mathrm{e}^{\mathrm{i}\theta})\subseteq\mathbb{Q}(\mathrm{e}^{\frac{\mathrm{i}\theta}{p}})$ i $\mathbb{Q}(\cos(\theta),\sin(\theta))\subseteq\mathbb{Q}(\cos(\frac{\theta}{p}),\sin(\frac{\theta}{p}))$ són extensions de cossos tals que*

$$[\mathbb{Q}(\mathrm{e}^{\frac{\mathrm{i}\theta}{p}}):\mathbb{Q}(\mathrm{e}^{\mathrm{i}\theta})]=\varepsilon\big[\mathbb{Q}\big(\cos(\tfrac{\theta}{p}),\sin(\tfrac{\theta}{p})\big):\mathbb{Q}\big(\cos(\theta),\sin(\theta)\big)\big]\leq p$$

on $\varepsilon=2$ si $\mathrm{i}\in\mathbb{Q}(\mathrm{e}^{\frac{\mathrm{i}\theta}{p}})\backslash\mathbb{Q}(\mathrm{e}^{\mathrm{i}\theta})$, i $\varepsilon=1$ altrament. En particular, si $[\mathbb{Q}(\mathrm{e}^{\frac{\mathrm{i}\theta}{p}}):\mathbb{Q}(\mathrm{e}^{\mathrm{i}\theta})]$ és senar, aleshores $\varepsilon=1$.

Demostració. Tenim que $\mathrm{e}^{\frac{\mathrm{i}\theta}{p}}$ és una arrel de $x^p-\mathrm{e}^{\mathrm{i}\theta}\in\mathbb{Q}(\mathrm{e}^{\mathrm{i}\theta})[x]$, per tant, l'extensió $\mathbb{Q}(\mathrm{e}^{\mathrm{i}\theta})\subseteq\mathbb{Q}(\mathrm{e}^{\frac{\mathrm{i}\theta}{p}})$ està ben definida i $[\mathbb{Q}(\mathrm{e}^{\frac{\mathrm{i}\theta}{p}}):\mathbb{Q}(\mathrm{e}^{\mathrm{i}\theta})]\leq p$. Aleshores obtenim la resta de l'enunciat del Lema 4.5, ja que totes les hipòtesis es compleixen. La darrera observació és conseqüència del fet que $\varepsilon\mid[\mathbb{Q}(\mathrm{e}^{\frac{\mathrm{i}\theta}{p}}):\mathbb{Q}(\mathrm{e}^{\mathrm{i}\theta})]$. $\square$

Això ens diu que per p-secar un angle es necessita resoldre un polinomi de grau com a màxim p, i aquest resultat no és millorable en general, és a dir, existeixen casos on el grau del polinomi serà p, com veurem a la Proposició 5.3.

5 La construcció de polígons regulars

Ara comencem a presentar la teoria que hi ha darrere de les construccions dels polígons construïbles amb $\mathscr{E}$. En aquesta secció introduirem i donarem sentit als resultats importants del *Disquisitiones arithmeticae* sobre la construcció de polígons regulars. Definim a continuació els polígons construïbles amb $\mathscr{E}$. Notem que per convenció "ser construïble" implica "ser regular".

Definició 5.1 (Polígon construïble amb $\mathscr{E}$)**.** Sigui $n \geq 3$. Direm que el polígon regular de n costats és construïble amb $\mathscr{E}$, si tots els vèrtexs del polígon regular de n costats inscrit en la circumferència unitat i amb vèrtex $(1, 0)$ són punts de $\mathscr{E}$.

Recordem quins són els vèrtexs del polígon regular de n costats inscrit en la circumferència unitat i amb vèrtex $(1, 0)$. Si pensem en el pla cartesià com el pla complex, només haurem de veure que podem construir les arrels n-èsimes de la unitat, les solucions de $x^n - 1 = 0$, és a dir,

$$1, \mathrm{e}^{\frac{2\pi \mathrm{i}}{n}}, \mathrm{e}^{2\frac{2\pi \mathrm{i}}{n}}, \ldots, \mathrm{e}^{(n-1)\frac{2\pi \mathrm{i}}{n}}$$

Això ens diu que els punts que formen els vèrtexs del polígon regular de n costats són

$$(1, 0), \big(\cos(\tfrac{2\pi}{n}), \sin(\tfrac{2\pi}{n})\big), \ldots, \big(\cos((n-1)\tfrac{2\pi}{n}), \sin((n-1)\tfrac{2\pi}{n})\big)$$

que té sentit per les observacions de la Secció 4, ja que la construcció d'un polígon regular de $\mathscr{E}$ equival a la n-secció de 2π. Per observacions d'aquesta secció, si $\mathscr{E}$ compleix la hipòtesi IV, aleshores ser construïble implica que tot polígon regular inscrit en qualsevol circumferència de $\mathscr{E}$ i amb vèrtex en un punt qualsevol de $\mathscr{E}$, té la resta de vèrtexs en $\mathscr{E}$.

Recordem ara algunes propietats fonamentals de les arrels n-èsimes de la unitat. S'acostuma a denotar $\xi = \mathrm{e}^{\frac{2\pi \mathrm{i}}{n}}$, ja que d'aquesta manera podem escriure totes les arrels del polinomi com $\{1, \xi, \xi^2, \ldots, \xi^{n-1}\}$ (no obstant això, a vegades utilitzarem ξ per referir-nos a qualsevol arrel diferent d'1). Està clar que $\{1, \xi, \xi^2, \ldots, \xi^{n-1}\}$ amb el producte complex usual és un grup isomorf a $\mathbb{Z}_n$, el grup cíclic d'ordre n, i que $\xi^n = 1$ per tota arrel n-èsima de la unitat. Per tant resulta adient anomenar *primitiva* a les arrels n-èsimes tals que n és el menor natural tal que $\xi^n = 1$, ja que d'aquesta manera obtenim que $\{\xi^k \mid k \in \mathbb{N}\} = \{1, \xi, \xi^2, \ldots, \xi^{n-1}\}$ si i només si ξ és una arrel n-èsima primitiva de la unitat, és a dir, una arrel primitiva de la unitat genera la resta. També recordarem que el polinomi $x^n - 1 = 0$ descompon com $(x-1)(x^{n-1} + x^{n-2} + \cdots + x^2 + x + 1)$, i que $x^{p-1} + x^{p-2} + \cdots + x^2 + x + 1$ és irreductible quan p és primer.

Ja hem vist pel Lema 4.2 que només haurem de veure si $\cos(\frac{2\pi}{n}), \sin(\frac{2\pi}{n}) \in E$ per afirmar que el polígon regular de n costat és construïble. A conseqüència del Corol·lari 4.4, tenim que

Corol·lari 5.2. *Sigui $n \geq 3$ tal que $n = p_1^{\alpha_1} \ldots p_k^{\alpha_k}$ sigui la seva descomposició en primers. Aleshores, el polígon regular de n costats és de $\mathscr{E}$ si i només si els polígons regulars de $p_j^{\alpha_j}$ costats, per tot j, són de $\mathscr{E}$.*

Ara ens interessarà poder trobar una manera de calcular $\sin(\frac{2\pi}{p^\alpha}), \cos(\frac{2\pi}{p^\alpha})$ en funció de $\sin(\frac{2\pi}{p}), \cos(\frac{2\pi}{p})$. Gauss a *Disquisitiones arithmeticae* ens explica que donat qualsevol primer p, $\cos(\frac{2\pi}{p^2})$ i $\sin(\frac{2\pi}{p^2})$ es poden obtenir de $\cos(\frac{2\pi}{p})$ i $\sin(\frac{2\pi}{p})$ mitjançant la resolució d'una equació de grau p; i de forma recursiva, $\cos(\frac{2\pi}{p^k})$ i $\sin(\frac{2\pi}{p^k})$ es poden obtenir dels mateixos valors mitjançant la resolució de $k-1$ equacions de grau p. Gauss va més enllà i ens afirma que no hi ha manera d'evitar aquestes resolucions [6, art. 336]. Donem una demostració alternativa i original d'aquest fet:

Proposició 5.3. *Siguin p un primer i $k \geq 1$ un enter. Aleshores,*

$$\left[\mathbb{Q}\left(\cos(\tfrac{2\pi}{p^{k+1}}), \sin(\tfrac{2\pi}{p^{k+1}})\right) : \mathbb{Q}\left(\cos(\tfrac{2\pi}{p^k}), \sin(\tfrac{2\pi}{p^k})\right)\right] = p$$

excepte quan $p^k = 2$, on el grau de l'extensió val 1.

Demostració. Denotem $\xi = \mathrm{e}^{\frac{2\pi \mathrm{i}}{p^{k+1}}}$ obtenint que $\xi^p = \mathrm{e}^{\frac{2\pi \mathrm{i}}{p^k}}$. Calculem primerament el grau de l'extensió $[\mathbb{Q}(\xi) : \mathbb{Q}(\xi^p)]$. Ens fixem que ξ és arrel de $x^p - \xi^p \in \mathbb{Q}(\xi^p)[x]$, i per tant $[\mathbb{Q}(\xi) : \mathbb{Q}(\xi^p)] \leq p$. Tenim que un polinomi del tipus $x^p - a \in K[x]$, on K cos, és irreductible si a no és una potència p-èsima a K [11, Thm 9.1]. En aquest cas, com sabem que ξ^p no és una potència p-èsima de cap element de $\mathbb{Q}(\xi^p)$, el polinomi és irreductible, i concloem que $[\mathbb{Q}(\xi) : \mathbb{Q}(\xi^p)] = p$. Per tant, per la Proposició 4.6 tenim que

$$\left[\mathbb{Q}\left(\cos(\tfrac{2\pi}{p^{k+1}}), \sin(\tfrac{2\pi}{p^{k+1}})\right) : \mathbb{Q}\left(\cos(\tfrac{2\pi}{p^k}), \sin(\tfrac{2\pi}{p^k})\right)\right] = \frac{[\mathbb{Q}(\xi) : \mathbb{Q}(\xi^p)]}{\varepsilon} = \frac{p}{\varepsilon}$$

on $\varepsilon = 1$ quan p és senar. En canvi, quan $p = 2$, tindrem que $\mathrm{i} \in \mathbb{Q}(\xi^p)$ per tot $k > 1$, i per tant $\mathrm{i} \in \mathbb{Q}(\xi) \backslash \mathbb{Q}(\xi^p)$ si i només si $k = 1$. És a dir, $\varepsilon = 1$ per tot valor p^k excepte quan $p^k = 2$, on $\varepsilon = 2$, d'on obtenim l'enunciat. □

Per tant, el problema sobre la construcció dels polígons regulars es redueix al càlcul de $\cos(\frac{2\pi}{p})$ i $\sin(\frac{2\pi}{p})$ per tot p primer divisor de n. Per un argument parell a la proposició anterior tenim que

Proposició 5.4. *Sigui p un primer. Aleshores,*

$$\left[\mathbb{Q}\left(\cos(\tfrac{2\pi}{p}), \sin(\tfrac{2\pi}{p})\right) : \mathbb{Q}\right] = p - 1.$$

Demostració. Obtenim de la Proposició 4.6 que quan $\theta = 2\pi$

$$\left[\mathbb{Q}\left(\cos(\tfrac{2\pi}{p}), \sin(\tfrac{2\pi}{p})\right) : \mathbb{Q}\right] = \left[\mathbb{Q}\left(\mathrm{e}^{\frac{2\pi \mathrm{i}}{p}}\right) : \mathbb{Q}\right],$$

ja que $\mathrm{i} \notin \mathbb{Q}(\mathrm{e}^{\frac{2\pi \mathrm{i}}{p}})$ per tot p, i sabem que $[\mathbb{Q}(\mathrm{e}^{\frac{2\pi \mathrm{i}}{p}}) : \mathbb{Q}] = p - 1$, ja que $\mathrm{Irr}(\mathrm{e}^{\frac{2\pi \mathrm{i}}{p}}, \mathbb{Q})[x] = x^{p-1} + \cdots + x + 1$. □

A continuació parlarem del fet que va permetre a Gauss resoldre el problema de la construcció dels polígons regulars amb regle i compàs. Aquesta part de la teoria de Gauss és llarga i complexa, i intentarem donar sentit a la següent cita que dona cap al final del seu treball.

> La divisió del cercle complet en p parts requereix, 1r, la divisió del cercle complet en $p - 1$ parts; 2n, la divisió d'un altre arc en $p - 1$ parts, que pot ser construït tan bon punt com la primera divisió estigui feta; 3r, l'extracció d'una arrel quadrada i es pot mostrar que sempre és $\sqrt{p}$. [6, art. 360]

Abans de poder donar la demostració d'aquest fet haurem de recordar alguns fets més sobre les arrels n-èsimes de la unitat. Primer de tot, tenim les següents igualtats:

Proposició 5.5. *Sigui $\Sigma_n^{(k)}$ la suma de totes les arrels n-èsimes de la unitat a la k-èsima potència, aleshores*

$$\Sigma_n^{(k)} = \begin{cases} n & \textit{si } k \equiv 0 \pmod{n} \\ 0 & \textit{sinó} \end{cases}$$

Demostració. Sigui $\xi = \mathrm{e}^{\frac{2\pi \mathrm{i}}{n}}$, aleshores tenim que

$$\Sigma_n^{(k)} = 1 + \xi^k + \xi^{2k} + \cdots + \xi^{(n-1)k} = \sum_{i=0}^{n-1} (\xi^k)^i.$$

Si $\xi^k \neq 1$, tenim que

$$\Sigma_n^{(k)} = \sum_{i=0}^{n-1} (\xi^k)^i = \frac{1-(\xi^k)^n}{1-\xi^k} = \frac{1-1}{1-\xi^k} = 0,$$

ja que $(\xi^k)^n = 1$, mentre que $\Sigma_n^{(k)} = n$ quan $\xi^k = 1$, és a dir, si i només si $k \equiv 0 \pmod{n}$. □

Donem uns quants fets més sobre les arrels p-èsimes de la unitat quan p és primer. Aquí tindrem que totes les arrels p-èsimes excepte 1 són primitives. De la Proposició 5.4 obtenim que l'extensió $\mathbb{Q} \subseteq \mathbb{Q}(\xi)$ és de grau $p-1$, d'on es dedueixen fets com que $\{1, \xi, \xi^2, \ldots, \xi^{p-1}\}$ és una $\mathbb{Q}$-base de $\mathbb{Q}(\xi)$.

Recordem també el concepte d'arrel primitiva mòdul p. S'anomena arrel primitiva mòdul p a tot element $a \in \{0, \ldots, p-1\}$ tal que $p-1$ és el mínim exponent que compleix $a^{p-1} \equiv 1 \pmod{p}$. En particular, si a és una arrel primitiva mòdul p, tindrem que $a, a^2, a^3, \ldots, a^{p-1}$ són tots congruents mòdul p a nombres diferents, i per tant podrem establir una correspondència un a un entre els conjunts $\{1, \ldots, p-1\}$ i $\{a, \ldots, a^{p-1}\}$. Recordem que si ξ és una arrel p-èsima primitiva de la unitat, $\xi^\alpha = \xi^\beta$ si i només si $\alpha \equiv \beta \pmod{p}$, i per tant

$$\{\xi, \xi^2, \ldots, \xi^{p-1}\} = \{\xi, \xi^a, \xi^{a^2}, \ldots, \xi^{a^{p-2}}\},$$

on els elements es troben en un ordre diferent en els conjunts, però en bijecció.

Veiem a continuació un lema que ens servirà per entendre la cita de Gauss. La demostració es basa en la suma de nombres de Dirichlet, però donarem una demostració original més directa.

Lema 5.6. *Siguin p un primer, ξ una arrel p-èsima primitiva de la unitat i a una arrel primitiva mòdul p, i denotem totes les arrels $(p-1)$-èsimes de la unitat per $\eta_j = \mathrm{e}^{j\frac{2\pi \mathrm{i}}{p-1}}$. Definim*

$$t_j = \xi + \eta_j \xi^a + \eta_j^2 \xi^{a^2} + \cdots + \eta_j^{p-2} \xi^{a^{p-2}}$$

per tot $j \in \{0, \ldots, p-2\}$. Aleshores $t_0 = -1$ i $|t_j| = \sqrt{p}$ per a tot $j \neq 0$, on $|t_j|$ denota el mòdul de t_j.

Demostració. Quan $j = 0$, $\eta_j = 1$, i per tant

$$t_0 = \sum_{m=0}^{p-2} \xi^{a^m} = \sum_{n=1}^{p-1} \xi^n = \Sigma_p^{(1)} - 1 = -1.$$

Veiem ara l'altra part. Per definició de mòdul tenim que $|t_j|^2 = \overline{t_j} t_j$, i per tant,

$$|t_j|^2 = \sum_{n=0}^{p-2} \eta_j^{-n} \xi^{-a^n} \sum_{m'=0}^{p-2} \eta_j^{m'} \xi^{a^{m'}} = \sum_{n=0}^{p-2} \sum_{m'=0}^{p-2} \eta_j^{m'-n} \xi^{a^{m'}-a^n}$$

i com $a^\alpha = a^\beta$ i $\eta_j^\alpha = \eta_j^\beta$ quan $\alpha \equiv \beta \pmod{p-1}$, això equival a

$$\sum_{n=0}^{p-2}\sum_{m=0}^{p-2} \eta_j^m \xi^{a^{m+n}-a^n} = \sum_{n=0}^{p-2}\sum_{m=0}^{p-2} \eta_j^m \xi^{(a^m-1)a^n} = \sum_{m=0}^{p-2} \eta_j^m \sum_{n=0}^{p-2} \xi^{(a^m-1)a^n}.$$

Ens fixem que $\sum_{n=0}^{p-2} \xi^{(a^m-1)a^n}$ és la suma de totes les arrels n-èsimes menys 1 a la (a^m-1)-èsima potència, i per tant, per la Proposició 5.5, tenim que

$$\sum_{n=0}^{p-2} \xi^{(a^m-1)a^n} + 1 - 1 = \Sigma_p^{(a^m-1)} - 1 = \begin{cases} p-1 & \text{si } a^m \equiv 1 \pmod{p} \\ -1 & \text{sinó} \end{cases}$$

Ens fixem que l'únic valor de $m \in \{0, \dots, p-2\}$ tal que la suma anterior dona $p-1$ és $m = 0$, per tant, substituint aquests valors obtenim que

$$|t_j|^2 = (p-1)\eta_j^0 - \sum_{m=1}^{p-2} \eta_j^m = (p-1) - (\Sigma_{p-1}^{(j)} - 1) = \begin{cases} 1 & \text{si } j = 0 \\ p & \text{sinó} \end{cases}$$

i per tant $|t_j| = \sqrt{p}$ per $j \neq 0$. □

Amb aquest lema podrem demostrar el següent teorema, que està lligat directament amb la cita de Gauss. No seguirem directament la prova de Gauss en *Disquisitiones arithmeticae*, però farem una adaptació bastant fidel a la que Lagrange dona en [10, Nota XIII-XIV].

Teorema 5.7. *Sigui p un primer senar. Aleshores podrem construir les arrels de $x^p - 1 = 0$ si podem $(p-1)$-secar tot angle i $\sqrt{p} \in E$.*

Demostració. Sigui ξ una arrel p-èsima primitiva de la unitat i a una arrel primitiva mòdul p. Recordem que, aleshores, les arrels de $x^p - 1 = 0$ són $1, \xi, \xi^a, \xi^{a^2}, \dots, \xi^{a^{p-2}}$. Si multipliquem cada terme de la successió anterior per ξ^{a^k} (mantenint l'ordre), obtindrem la mateixa successió en el mateix ordre però començant per ξ^{a^k}, és a dir, obtenim

$$(\xi^{a^k}, \xi^{a^k a}, \xi^{a^k a^2}, \dots, \xi^{a^k a^{p-2}}) = (\xi^{a^k}, \xi^{a^{k+1}}, \dots, \xi^{a^{p-2}}, 1, \xi, \dots, \xi^{a^{k+p-2}}).$$

Siguin t_j per tot j tals com els hem definit al Lema 5.6. Aleshores, escollint un valor j i elevant t_j a $p-1$, obtenim que

$$T_j = t_j^{p-1} = f_0(\xi) + \eta_j f_1(\xi) + \eta_j^2 f_2(\xi) + \dots + \eta_j^{p-2} f_{p-2}(\xi)$$

on $f_i(\xi) = A_i + B_i\xi + C_i\xi^a + \dots + P_i\xi^{a^{p-2}}$ per uns certs $A_i, B_i, \dots, P_i$ enters, ja que $\eta_j^{p-1} = 1$ i $\xi^p = 1$. Fixem-nos que donat qualsevol k, tenim que

$$\begin{aligned} \eta_j^k t_j &= \eta_j^k \xi + \eta_j^{k+1}\xi^a + \eta_j^{k+2}\xi^{a^2} + \dots + \eta_j^{k+p-2}\xi^{a^{p-2}} \\ &= \xi^{a^{p-k}} + \eta_j \xi^{a^{p-k+1}} + \dots + \eta_j^{k+p-2}\xi^{a^{p-2}} + \eta_j^k\xi + \dots + \eta_j^{p-2}\xi^{a^{p-k-1}} \end{aligned}$$

i com $(\eta_j^k t_j)^{p-1} = t_j^{p-1} = T_j$, obtenim que $f_i(\xi) = f_i(\xi^a) = \dots = f_i(\xi^{a^{p-2}})$ per tot i, per l'observació anterior. Aleshores, per independència lineal de $\{\xi, \xi^2, \dots, \xi^{p-1}\}$, obtenim $B_i = C_i = \dots = P_i$ i per tant

$$f_i(\xi) = A_i + B_i\xi + C_i\xi^a + \dots + P_i\xi^{a^{p-2}}$$

$$
\begin{aligned}
&= A_i + B_i(\xi^a + \xi^{a^2} + \cdots + \xi^{a^{p-2}}) \\
&= A_i + B_i(\xi + \xi^2 + \cdots + \xi^{p-1}) \\
&= A_i - B_i,
\end{aligned}
$$

ja que $\Sigma_p^{(1)} = 0$. En conclusió, per tot i, $f_i(\xi)$ és un enter que no depèn de ξ, i per tant T_j només depèn de η_j. Fixem-nos que no importa quina arrel η_j de $x^{p-1} - 1 = 0$ agafem, per tant, els mateixos resultats de t_j i T_j són certs per tot j. Sumant tots els termes t_j obtenim

$$\sum_{j=0}^{p-2} t_j = (p-1)\xi + \Sigma_{p-1}^{(1)}\xi^a + \Sigma_{p-1}^{(2)}\xi^{a^2} + \cdots + \Sigma_{p-1}^{(p-2)}\xi^{a^{p-2}} = (p-1)\xi$$

i per tant,

$$\xi = \frac{t_0 + \cdots + t_{p-2}}{p-1} = \frac{-1 + t_1 + \cdots + t_{p-2}}{p-1}.$$

Calculem ara les imatges de T_j per l'arrel $(p-1)$-èsima per $j \in \{1, \ldots, p-2\}$. Fixem-nos que les imatges són

$$\sqrt[p-1]{r_j}\,\mathrm{e}^{\frac{\mathrm{i}(\theta_j + 2\pi k)}{p-1}}$$

per $k \in \{0, \ldots, p-2\}$, i una d'elles sempre és t_j per construcció. Ens fixem pel Lema 5.6 que totes tenen el mateix mòdul, $\sqrt[p-1]{r_j} = |\sqrt[p-1]{T_j}| = |t_j| = \sqrt{p}$. Com podem $(p-1)$-secar tot angle i $\sqrt{p} \in E$, per hipòtesi, tenim que tots els valors anteriors són construïbles, inclosos t_j per tot j, i per tant ξ és construïble. Com ξ és primitiva, obtenim que tota arrel de $x^p - 1 = 0$ és construïble. □

D'aquesta manera, recordant la relació entre el pla $\mathbb{C}$ i $\mathbb{R}^2$ i el fet que per un cert k_j

$$t_j = \sqrt[p-1]{r_j}\,\mathrm{e}^{\frac{\mathrm{i}(\theta_j + 2\pi k_j)}{p-1}} = \sqrt[p-1]{r_j}\cos\left(\frac{\theta_j + 2\pi k_j}{p-1}\right) + \mathrm{i}\sqrt[p-1]{r_j}\sin\left(\frac{\theta_j + 2\pi k_j}{p-1}\right),$$

obtenim aquest resultat:

Teorema 5.8. *Sigui p un primer senar. Aleshores, el polígon regular de p costats és de $\mathscr{E}$ si podem $(p-1)$-secar qualsevol angle amb $\mathscr{E}$ i $\sqrt{p} \in E$.*

Resumint els càlculs realitzats en aquesta secció, quan $\mathscr{E}$ compleix les hipòtesis I, II i III, tenim per definició que el polígon regular de n costats és construïble amb $\mathscr{E}$ si i només si $\cos(\frac{2\pi}{n})$ i $\sin(\frac{2\pi}{n})$ són a E. A més, sabem que el càlcul de $\cos(\frac{2\pi}{n})$ i $\sin(\frac{2\pi}{n})$ consisteix en el càlcul de $\cos(\frac{2\pi}{p^\alpha})$ i $\sin(\frac{2\pi}{p^\alpha})$ per p^α els primers amb màxim exponent que divideixen n. Per les Proposicions 5.3 i 5.4 tenim que per trobar $\cos(\frac{2\pi}{p^\alpha})$ i $\sin(\frac{2\pi}{p^\alpha})$ haurem de resoldre una equació de grau $p-1$ i $\alpha-1$ extensions de grau p (quan p és senar). El Teorema 5.8 ens dona una manera equivalent de calcular $\cos(\frac{2\pi}{p})$ i $\sin(\frac{2\pi}{p})$: només es necessita poder $(p-1)$-secar i construir $\sqrt{p}$.

Acabem la secció comentant quins polígons regulars són de regle

Teorema 5.9. *El quadrat és l'únic polígon construïble amb regle.*

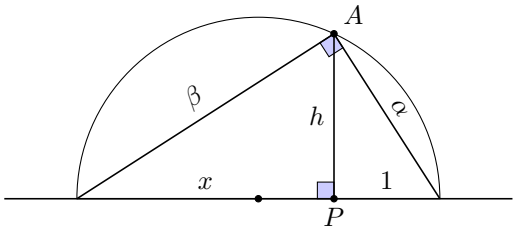
Demostració. Sabem que un polígon regular de n costats és construïble amb regle si i només si $\cos(\frac{2\pi}{n}), \sin(\frac{2\pi}{n}) \in \mathbb{Q}$. L'únic $n \geq 3$ que compleix aquesta propietat és $n = 4$, tal com deduïm de les Proposicions 5.3 i 5.4, i per tant el quadrat és l'únic polígon construïble amb regle. □

6 El teorema de Gauss-Wantzel

Donem en aquesta secció una prova del Teorema de Gauss-Wantzel que utilitza els resultats de la Secció 5 i per tant és una prova basada en els resultats que Gauss va assumir. No obstant això, s'ha de comentar que la prova és equivalent a l'actualment utilitzada.

No és difícil veure que els punts de regle i compàs compleixen les hipòtesis I, II, III i IV que hem mencionat en les Seccions 3 i 4: clarament, per definició de punt construïble amb regle i compàs (2.1) tenim que es compleixen I i II, Euclides mostra III en els *Elements* (I.11 i I.12), i IV es pot provar amb el compàs i la translació de segments mitjançant paral·leles. Per tant, el conjunt de punts de regle i compàs és un cos i el denotarem com $\mathbb{E}$ (en referència a Euclides [12]).

Sabem que $\mathbb{E}$ inclou nombres algebraics no racionals, en particular, $\sqrt{x} \in \mathbb{E}$ per tot $x \in \mathbb{E}^+$. Provem aquest fet: construïm la circumferència centrada en l'origen de radi $\frac{x+1}{2}$, $x \geq 0$, i construïm la perpendicular a l'eix d'abscisses que passa per $P = (\frac{x-1}{2}, 0)$, tal com veiem en la imatge inferior. Sigui $A = (\frac{x-1}{2}, h)$ el punt d'intersecció de la perpendicular i la circumferència que cau en el semiplà positiu ($h > 0$). Calculem el valor de h: seguint el dibuix de sota, obtenim pel teorema de Pitàgores que $1 + h^2 = \alpha^2$, $x^2 + h^2 = \beta^2$ i $\alpha^2 + \beta^2 = (x+1)^2$, d'on es dedueix que $h = \sqrt{x}$. Per tant $\sqrt{x} \in \mathbb{E}$ per tot $x \in \mathbb{E}^+$.



Per definició, si P és un punt de regle i compàs, aleshores existeix una successió finita de punts $P_{-1}, P_0, P_1, \ldots, P_n$ tal que $P = P_n$ és el punt d'intersecció de dues rectes, dues circumferències o una recta i circumferència formades per punts previs a P en la successió. Sabem que aquestes rectes i circumferències tenen coeficients en el mínim cos K_{n-1} que conté les coordenades dels punts previs a P en la successió, per la Proposició 3.3. Ens centrarem a calcular les extensions $K_{n-1} \subseteq K_n$ quan el punt P és la intersecció d'una recta i circumferència, ja que, la intersecció de dues circumferències es pot reduir a la intersecció d'una recta i circumferència, i la intersecció de dues rectes ens dona $K_{n-1} = K_n$, pel Teorema 3.4. Sigui $P = (x, y)$ un punt d'intersecció de la recta $aX + bY = c$ i la circumferència $(X - d)^2 + (Y - e)^2 = f^2$ amb coeficients en K_{n-1}. Igualant les dues equacions obtenim que la coordenada y del punt satisfà

$$(a^{-1}(c - by) - d)^2 + (y - e)^2 = f^2$$

és a dir, compleix una equació de grau 2, i aleshores tenim que

$$[K_{n-1}(x) : K_{n-1}] = [K_{n-1}(y) : K_{n-1}] \leq 2.$$

ja que $x = a^{-1}(c - by)$ (en cas que $a = 0$, aïllarem b en comptes i obtindrem el mateix resultat). Per tant, recursivament, obtenim que $x \in \mathbb{E}$ compleix

$[\mathbb{Q}(x) : \mathbb{Q}] = 2^r$ per un cert r, seguint l'argument que havíem donat en la Secció 3.

Es diu que una extensió de cossos és euclidiana si és del tipus $K \subset K(\sqrt{a})$ on $a \in K^+$ i $\sqrt{a} \notin K$, és a dir si és de grau 2, i per tant, tenim que tot element de $\mathbb{E}$ es troba en una torre de cossos sobre $\mathbb{Q}$ on cada extensió és euclidiana. Podem anomenar 2-torre a aquest tipus de torre. Com $\sqrt{x} \in \mathbb{E}$ per tot $x \in \mathbb{E}^+$, $\mathbb{E}$ és el mínim cos euclidià. Aquest fet ens donarà el següent teorema

Teorema 6.1. *Sigui $x \in \mathbb{R}$. Aleshores, tenim que $x \in \mathbb{E}$ si i només si $[\mathbb{Q}(x) : \mathbb{Q}] = 2^r$ per algun $r \geq 0$.*

Wantzel [14] va ser el primer a donar una prova rigorosa d'aquest resultat, que és clau per afirmar quins polígons no són construïbles amb regle i compàs. Donem ara una prova del teorema de Gauss-Wantzel utilitzant el teorema anterior i els resultats de les Seccions 4 i 5.

Teorema 6.2 (Teorema de Gauss-Wantzel)**.** *Sigui $n \geq 3$. Aleshores, el polígon regular de n costats és construïble amb regle i compàs si i només si $n = 2^a p_1 \cdots p_k$ amb $a \geq 0$ i $p_1, \ldots, p_k$ primers de Fermat diferents.*

Demostració. La Proposició 4.6 i el Teorema 6.1 ens diuen que podem bisecar tot angle amb regle i compàs, però alhora també ens diu que no podrem generalment n-secar angles per $n > 2$ (recordem que ja sabíem que podíem bisecar tot angle donat per Euclides I.9). De les Proposicions 5.3 i 5.4 obtenim

$$\left[\mathbb{Q}\left(\cos\left(\tfrac{2\pi}{p^\alpha}\right), \sin\left(\tfrac{2\pi}{p^\alpha}\right)\right) : \mathbb{Q}\right] = p^{\alpha-1}(p-1)$$

quan p és senar, i pel Teorema 6.1 deduïm que el polígon de p^α costats és construïble si i només si $p^{\alpha-1}(p-1)$ és una potència de dos, que ocorre només quan $\alpha = 1$ i p és un primer de Fermat (és a dir, tot primer tal que $p - 1 = 2^n$).

Per tant, tenim que els únics polígons regulars de p^α costats que són construïbles amb regle i compàs són aquells on p^α és una potència de 2 o un primer de Fermat amb multiplicitat 1. Pel Corol·lari 5.2 obtenim l'enunciat. □

Aquest resultat també es pot obtenir a partir del Teorema 5.8, que deia que tot polígon regular de p costats amb p primer senar és construïble si podem $(p-1)$-secar angles i $\sqrt{p} \in \mathbb{E}$ (que és cert en ser $\mathbb{E}$ euclidià). Amb regle i compàs només podem bisecar angles per tant només poden construir els polígons de p costats quan p és de Fermat.

Acabem la secció amb una nota. Es pot provar la irresolubilitat dels tres problemes clàssics dels grecs (la trisecció de tot angle, la duplicació del cub i la quadratura del cercle) a conseqüència del Teorema 6.1. Aquests problemes estan directament vinculats en el càlcul del grau de les extensions de $\mathbb{Q}(\cos(\theta)) \subseteq \mathbb{Q}(\cos(\frac{\theta}{3}))$ per tot θ, $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2})$ i $\mathbb{Q} \subseteq \mathbb{Q}(\pi)$, i per tant seran resolubles si i només si el grau de l'extensió és una potència de 2. No és difícil veure que la primera extensió té grau 1 o 3 (depenent del valor de θ) i la segona grau 3, provant que els problemes no són resolubles amb regle i compàs. Com en temps de Wantzel no es coneixia si π era algebraic o no, la prova de la irresolubilitat de l'últim problema va romandre oberta fins a l'any 1882, quan Lindemann va provar que π és efectivament transcendent i per tant que $[\mathbb{Q}(\pi) : \mathbb{Q}] = \infty$ [1].

7 Els teoremes de Mohr-Mascheroni i Poncelet-Steiner

En aquesta secció parlarem de dos teoremes importants sobre unes construccions a priori més febles que les construccions amb regle i compàs (en el sentit que el conjunt de punts construïbles és un subconjunt dels punts construïbles amb regle i compàs), però que ens permeten construir el mateix conjunt de punts.

Òbviament, tant el regle com el compàs ens permeten dibuixar formes geomètriques úniques: no podrem pas dibuixar una recta sense el regle, ni una circumferència sense el compàs, i per tant semblaria estrany que una de les dues eines clàssiques no fos necessària per construir tots els punts de regle i compàs, no obstant això, tots els punts de regle i compàs es poden construir només amb compàs. Introduïm el nostre primer teorema, on la definició de punt construïble amb compàs és idèntica a la Definició 2.1, però on tots els punts són construïts sota el punt iii)

Teorema 7.1 (Teorema de Mohr-Mascheroni)**.** *Un punt és de compàs si i només si és de regle i compàs.*

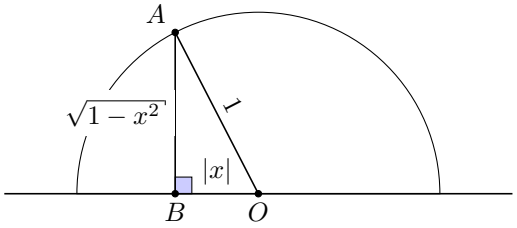
La demostració consisteix a veure que els punts d'intersecció de dues rectes de compàs i d'una recta i circumferència de compàs són de compàs. No demostrarem aquest teorema en aquest treball; la prova no és massa difícil d'entendre, però és llarga i les construccions substitutòries són complexes. Podrem trobar aquesta demostració a [9, Ch. 8] i [12, Ch. 3].

Com hem vist en el Teorema 3.4 no podrem construir tot punt de regle i compàs amb només regle. Ens preguntem, però, quantes vegades com a màxim hem d'utilitzar el compàs per tal que puguem construir tots els punts de regle i compàs. La resposta és igual d'elegant que el teorema de Mohr-Mascheroni: només es necessita utilitzar el compàs un cop per dibuixar una única circumferència. Per comoditat es considera la circumferència de radi 1 centrada a l'origen, però podem escollir qualsevol altra circumferència construïble amb regle. Anomenem *regle i circumferència* a aquest conjunt d'eines, on els punts es construeixen mitjançant intersecció de rectes, i la intersecció de rectes amb la circumferència unitat de radi centrada a l'origen.

Teorema 7.2 (Teorema de Poncelet-Steiner)**.** *Un punt és de regle i circumferència si i només si és de regle i compàs.*

Demostració. Ho farem veient que el conjunt E de nombres de regle i circumferència és $\mathbb{E}$. Com coneixem els cossos de nombres de regle i els de regle i compàs, deduïm que E és un cos tal que $\mathbb{Q} \subseteq E \subseteq \mathbb{E}$.

Veiem que per tot $x \in E$ tal que $|x| \leq 1$ tenim que $\sqrt{1-x^2} \in E$, i ho farem amb ajuda de la imatge inferior, que correspon al cas quan $x < 0$.



Construïm la perpendicular a l'eix d'abscisses que passa per $B = (x, 0)$ i definim A com el punt d'intersecció de la perpendicular i la circumferència unitat que cau en el semiplà positiu (que existeix, ja que $|x| \leq 1$). Pel teorema de Pitàgores, $A = (x, \sqrt{1-x^2})$ i per tant $\sqrt{1-x^2} \in E$. Aleshores tenim per tot $x \in E^+$ que

$$\sqrt{x} = \sqrt{\left(\frac{x+1}{2}\right)^2 - \left(\frac{x-1}{2}\right)^2} = \frac{x+1}{2}\sqrt{1 - \left(\frac{x-1}{x+1}\right)^2} \in E,$$

ja que $|\frac{x-1}{x+1}| \leq 1$. Per tant, E és euclidià i $E = \mathbb{E}$. □

8 Construccions amb regle i compàs de puntes

En aquesta secció parlarem de les construccions amb un conjunt nou d'eines, el regle i compàs de puntes, i ampliarem la teoria que ens dona Martin a *Geometric constructions* per poder dir quins són els polígons construïbles amb regle i compàs. El compàs de puntes ens permetrà transportar distàncies entre dos punts construïbles del pla cartesià. Aquesta és la funció que té el compàs de puntes físic, una eina que serveix per marcar distàncies, utilitzat freqüentment en navegació. Donem la definició formal dels punts construïbles amb regle i compàs de puntes de [12, Def. 5.1], on ens fixem que el conjunt de punts base està format per quatre punts que no formen un paral·lelogram:

Definició 8.1 (Punt construïble amb regle i compàs de puntes)**.** En el pla de coordenades cartesianes $\mathbb{R}^2$, diem que un punt P és construïble amb regle i compàs de puntes si és l'últim terme P_n d'una successió finita de punts: $P_{-3}, P_{-2}, P_{-1}, P_0, P_1, \ldots, P_n$, on $P_{-3} = (1, 0)$, $P_{-2} = (2, 0)$, $P_{-1} = (0, 1)$ i $P_0 = (0, 2)$ són els punts base i on P_i per tot $i > 0$ és un dels següents

i) El punt d'intersecció de dues rectes secants formades per punts previs a P_i en la successió.

ii) Un dels punts P sobre la recta $\overleftrightarrow{AB}$ tal que $|AP| = |CD|$ on A, B, C, D són punts previs a P_i en la successió i $A \neq B$.

I, com sempre, tindrem les definicions de recta, circumferència i de nombre construïble amb regle i compàs de puntes. Denotem el conjunt de nombres construïbles amb regle i compàs de puntes com $\mathbb{P}$, denotat amb una P de Pitàgores, per motius que es faran més clars més endavant.

Ens fixem que el punt i) de la definició correspon a les construccions amb regle, per tant, tot punt de regle és un punt de regle i compàs, i $\mathbb{P}$ és un cos. Per altra banda, el punt ii) de la definició ens diu que podem transportar distàncies. Aquesta propietat és en realitat equivalent a la hipòtesi IV que hem donat a la Secció 4. Aquest fet ens diu que els punts de regle i compàs de puntes són també punts de regle i compàs, ja que el regle i compàs compleixen IV, i més generalment, totes les propietats que veurem sobre les construccions amb regle i compàs de puntes seran certes per tot conjunt d'eines que compleix les hipòtesis I, II, III i IV.

Estudiem el grau de l'extensió de les construccions amb regle i compàs de puntes. Sigui P un punt de regle i compàs de puntes, que per definició és l'últim

punt d'una successió finita de punts $P_{-3}, P_{-2}, \ldots, P_n$. Siguin K_i els mínims cossos que contenen les coordenades dels punts $P_{-3}, P_{-2}, \ldots, P_n$. Pel Teorema 3.4 tenim que la intersecció de dues rectes no ens proporciona nous punts del cos, per tant només haurem de veure les construccions sota el punt ii) de la definició. Utilitzant la notació del punt ii) de la definició, siguin $A = (a, b)$ i $B = (a + a', b + b')$ (on $a, a', b, b' \in K_{n-1}$) els punts col·lineals amb P, tenim que per tant $P = (a + \varepsilon a', b + \varepsilon b')$ per un cert ε. Com la distància $|AP|$ ha de ser igual a $|CD| = \sqrt{c^2 + d^2}$ per certs $c, d \in K_{n-1}$, obtenim que

$$\sqrt{c^2 + d^2} = |AP| = |\varepsilon| \sqrt{a'^2 + b'^2}$$

d'on obtenim dos punts P que compleixen les propietats en funció del signe de ε, que té sentit perquè tenim sempre dos punts a distància $|CD|$ de A sobre cada recta. Tenim que

$$P = \left(a \pm a' \frac{\sqrt{c^2 + d^2}}{\sqrt{a'^2 + b'^2}},\ b \pm b' \frac{\sqrt{c^2 + d^2}}{\sqrt{a'^2 + b'^2}} \right),$$

que està ben definit, ja que $A \neq B$ implica que $\sqrt{a'^2 + b'^2} \neq 0$. Com a, a', b, b', c i d són de K_{n-1}, tenim que $K_n = K_{n-1}(\sqrt{c^2 + d^2}, \sqrt{a'^2 + b'^2})$. Això ens dona un tipus d'extensió molt particular.

Definició 8.2 (Extensió pitagòrica)**.** Diem que una extensió $K \subset L$ és pitagòrica si $L = K(\sqrt{a^2 + b^2})$ on $a, b \in K$ i $\sqrt{a^2 + b^2} \notin K$, i que una $K_0 \subset K_n$ és una extensió pitagòrica iterada sobre K_0 si existeix una torre de cossos $K_0 \subset K_1 \subset \cdots \subset K_n$ pitagòrica, és a dir, una torre on cada extensió intermèdia és pitagòrica.

Per definició, tenim que l'extensió $K_{n-1} \subseteq K_{n-1}(\sqrt{c^2 + d^2}, \sqrt{a'^2 + b'^2})$ és o bé una igualtat (quan $\sqrt{c^2 + d^2}, \sqrt{a'^2 + b'^2} \in K_{n-1}$) o bé és una extensió pitagòrica iterada, i per tant podem concloure que tot nombre de $\mathbb{P}$ està en una extensió pitagòrica iterada sobre $\mathbb{Q}$. El recíproc també és cert, ja que construint el punt P sobre l'eix d'abscisses tal que $|OP| = |OA|$ on O és l'origen i $A = (a, b)$, obtenim que $P = (\sqrt{a^2 + b^2}, 0)$ i per tant $\sqrt{a^2 + b^2} \in \mathbb{P}$; que ens diu que la suma de dos quadrats de $\mathbb{P}$ és un quadrat de $\mathbb{P}$. A més tenim que la suma de m quadrats de $\mathbb{P}$ és sempre un quadrat, ja que $a^2 + b^2 + c^2 = a^2 + (\sqrt{b^2 + c^2})^2$ és la suma de dos quadrats de $\mathbb{P}$, i de forma recursiva obtenim el resultat. Diem que un cos que compleix aquesta propietat és pitagòric, i per tant tenim que $\mathbb{P}$ és el mínim cos pitagòric sobre $\mathbb{Q}$.

Com tota extensió pitagòrica és euclidiana tenim que $\mathbb{Q} \subset \mathbb{P} \subseteq \mathbb{E}$. Veurem a continuació que $\mathbb{P} \neq \mathbb{E}$, que és un resultat no trivial que ens requerirà demostrar uns quants resultats previs. Comencem veient alguns exemples de nombres irracionals de $\mathbb{P}$:

Proposició 8.3. *Sigui $x \in \mathbb{Q}^+$, aleshores $\sqrt{x} \in \mathbb{P}$.*

Demostració. Provem-ho primer per tot $n \in \mathbb{N}$ per inducció sobre n. Quan $n = 1$, tenim que $\sqrt{1} = 1 \in \mathbb{Q} \subset \mathbb{P}$. Suposem que és cert per $n - 1$ i ho demostrem per n. Per la hipòtesi d'inducció tenim que $\sqrt{n-1} \in \mathbb{P}$, i com el cos és pitagòric, tenim

$$\sqrt{1^2 + \left(\sqrt{n-1}\right)^2} = \sqrt{1 + n - 1} = \sqrt{n} \in \mathbb{P}.$$

En conclusió, com $\mathbb{P}$ és un cos, per tot racional $x > 0$ existeixen $p, q \in \mathbb{N}$ tals que

$$\sqrt{x} = \sqrt{\frac{p}{q}} = \frac{\sqrt{p}}{\sqrt{q}} \in \mathbb{P}. \qquad \square$$

Els següents lemes ens permetran arribar a un $x \in \mathbb{E}$ que no és a $\mathbb{P}$. Com hem comentat abans, els cossos que introduïm seran de característica 0 i per tant extensions de $\mathbb{Q}$.

Lema 8.4. *Siguin x, y, a elements d'un cos K tals que $\sqrt{a} \notin K$, aleshores tenim que $x + y\sqrt{a}$ és suma de quadrats de $K(\sqrt{a})$ si i només si $x - y\sqrt{a}$ és suma de quadrats de $K(\sqrt{a})$.*

Demostració. Si $x + y\sqrt{a}$ és suma de quadrats de $K(\sqrt{a})$, aleshores existeixen $x_1, y_1 \ldots, x_n, y_n \in K$ tals que

$$\begin{aligned} x + y\sqrt{a} &= \sum_{i=1}^{n} (x_i + y_i\sqrt{a})^2 = \sum_{i=1}^{n} (x_i^2 + ay_i^2 + 2x_iy_i\sqrt{a}) \\ &= \sum_{i=1}^{n} (x_i^2 + ay_i^2) + \sum_{i=1}^{n} 2x_iy_i\sqrt{a}. \end{aligned}$$

Com $\sqrt{a} \notin K$, $\{1, \sqrt{a}\}$ és una K-base de $K(\sqrt{a})$, d'on deduïm que

$$x = \sum_{i=1}^{n} (x_i^2 + ay_i^2) \qquad \text{i} \qquad y = \sum_{i=1}^{n} 2x_iy_i.$$

En conclusió veiem que

$$x - y\sqrt{a} = \sum_{i=1}^{n} (x_i^2 + ay_i^2) - \sum_{i=1}^{n} 2x_iy_i\sqrt{a} = \sum_{i=1}^{n} (x_i - y_i\sqrt{a})^2$$

és una suma de quadrats. La implicació cap a l'esquerra es fa de manera anàloga canviant el signe de y. $\square$

Lema 8.5. *Sigui $K \subset K(\alpha)$ una extensió de cossos pitagòrica, aleshores si $x \in K$ és una suma de quadrats de $K(\alpha)$, x és suma de quadrats de K.*

Demostració. Per definició d'extensió pitagòrica, tenim que $\alpha = \sqrt{a^2 + b^2}$ amb $a, b \in K$ i $\alpha \notin K$. Com $\alpha \notin K$, $\{1, \alpha\}$ és una K-base de $K(\alpha)$, i com x és suma de quadrats de $K(\alpha)$, tenim que

$$x = \sum_{i=1}^{n} (x_i + y_i\alpha)^2$$

amb $x_1, y_1 \ldots, x_n, y_n \in K$. Desenvolupant els quadrats obtenim que

$$\sum_{i=1}^{n} (x_i + y_i\alpha)^2 = \sum_{i=1}^{n} (x_i^2 + \alpha^2 y_i^2 + 2x_iy_i\alpha) = \sum_{i=1}^{n} (x_i^2 + \alpha^2 y_i^2) + \sum_{i=1}^{n} 2x_iy_i\alpha,$$

mentre que per independència lineal tenim

$$x = \sum_{i=1}^{n} (x_i^2 + \alpha^2 y_i^2) = \sum_{i=1}^{n} (x_i^2 + (a^2 + b^2)y_i^2)$$

i com $x_1, y_1 \ldots, x_n, y_n, a, b \in K$, x és suma de quadrats en K. $\square$

Aplicant successivament aquest lema arribem a què

Corol·lari 8.6. *Sigui $K \subset L$ una extensió pitagòrica iterada, aleshores si $x \in K$ és una suma de quadrats de L, x és suma de quadrats en K.*

En conseqüència, tot element x d'una extensió pitagòrica iterada és suma de quadrats en el primer cos de la torre en què apareix o és impossible que sigui una suma de quadrats en cossos superiors. Per tant, com tot $x \in \mathbb{P}$ viu en una extensió pitagòrica iterada sobre $\mathbb{Q}$, x és o bé una suma de quadrats dins l'extensió en què primer apareix o no ho és en cap, ni tan sols a $\mathbb{P}$. Això ens permet provar la següent proposició

Proposició 8.7. *Siguin $x, y, a \in \mathbb{Q}$ amb a positiu tal que $\sqrt{a} \notin \mathbb{Q}$. Aleshores, $\sqrt{x + y\sqrt{a}} \in \mathbb{P}$ si i només si $\sqrt{x - y\sqrt{a}} \in \mathbb{P}$.*

Demostració. Suposem que $\sqrt{x + y\sqrt{a}} \in \mathbb{P}$, per tant, per l'observació anterior, com $x+y\sqrt{a}$ és un quadrat, s'ha de poder escriure com a suma de quadrats d'una extensió pitagòrica iterada $\mathbb{Q}(\alpha_1, \ldots, \alpha_n)$ (on $\alpha_{i+1} = \sqrt{a_i^2 + b_i^2} \notin \mathbb{Q}(\alpha_1, \ldots, \alpha_i)$ amb $a_i, b_i \in \mathbb{Q}(\alpha_1, \ldots, \alpha_i)$ per tot i). Definim la següent torre de cossos

$$\mathbb{Q}(\sqrt{a}) = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_n \subset \mathbb{R}$$

de manera que, per tot i, $K_{i+1} = K_i$ si $\alpha_i \in K_i$ i $K_{i+1} = K_i(\alpha_i)$ si no. Fixem-nos que en aquest darrer cas $K_i \subset K_{i+1}$ és una extensió pitagòrica, i aleshores $K_0 \subseteq K_n$ és una extensió pitagòrica iterada (o $K_0 = K_n$). Com $\mathbb{Q}(\alpha_1, \ldots, \alpha_n) \subseteq K_n$, $x + y\sqrt{a}$ s'escriu com a suma de quadrats de K_n, per tant, el Corol·lari 8.6, $x + y\sqrt{a}$ s'escriu com suma de quadrats de $K_0 = \mathbb{Q}(\sqrt{a})$. En conseqüència, pel Lema 8.4, $x - y\sqrt{a}$ és també suma de quadrats de $\mathbb{Q}(\sqrt{a})$.

Com $\sqrt{a} \in \mathbb{P}$ per la Proposició 8.3, $\mathbb{Q}(\sqrt{a}) \subset \mathbb{P}$, i en conclusió, $x - y\sqrt{a}$ és suma de quadrats de $\mathbb{P}$ i per tant $\sqrt{x - y\sqrt{a}} \in \mathbb{P}$. El recíproc és immediat canviant el signe de y. □

Aquest resultat ens permetrà construir elements de $\mathbb{E}$ que no són a $\mathbb{P}$, com veiem en la següent proposició:

Proposició 8.8. *Sigui $n > 1$ un natural no quadrat, aleshores tenim que $\sqrt{1 + \sqrt{n}}$ i que $\sqrt[4]{n}$ no són de $\mathbb{P}$.*

Demostració. Com n no és un quadrat, tenim que $\sqrt{n} \notin \mathbb{Q}$, per tant, per la Proposició 8.7, tenim que $\sqrt{1 + \sqrt{n}} \in \mathbb{P}$ si i només si $\sqrt{1 - \sqrt{n}} \in \mathbb{P}$, però clarament $\sqrt{1 - \sqrt{n}} \notin \mathbb{P}$, ja que no és real ($\sqrt{n} > 1$).

Per altra banda, deduïm que $\sqrt[4]{n} \notin \mathbb{P}$. Si $\sqrt[4]{n} \in \mathbb{P}$, aleshores

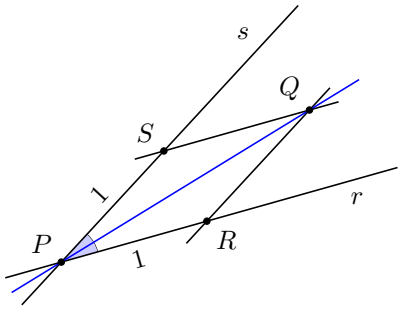
$$\sqrt{1^2 + (\sqrt[4]{n})^2} = \sqrt{1 + \sqrt{n}} \in \mathbb{P},$$

ja que $\mathbb{P}$ és un cos pitagòric, arribant a contradicció. □

Per tant, tenim que $\mathbb{P} \neq \mathbb{E}$, ja que $\sqrt{1 + \sqrt{n}}$ i $\sqrt[4]{n}$ són a $\mathbb{E}$ per tot $n \in \mathbb{Q}$. Això ens diu que hi ha punts de regle i compàs que no són de regle i compàs de puntes, no obstant això, tot polígon construïble amb regle i compàs serà construïble amb regle i compàs de puntes. Per provar aquest resultat només ens falta veure que podem bisecar amb regle i compàs de puntes:

Proposició 8.9. *Podem bisecar tot angle donat amb regle i compàs de puntes.*

Demostració. Sigui $\angle(A, P, B)$, amb A, P, B punts de regle i compàs de puntes, l'angle que ens demanen bisecar. Està clar que podem bisecar l'angle si $|\angle(A, P, B)| = \theta = \pi, 2\pi$, ja que podem construir la perpendicular a una recta i estendre una semirecta. Fixem-nos també que podem bisecar l'angle θ si i només si podem bisecar $2\pi - \theta$, per tant només ens cal provar el resultat per $\theta \in (0, \pi)$.



En la resta de casos, seguim la figura de sobre, sigui r la semirecta $\overrightarrow{PA}$ i s la semirecta $\overrightarrow{PB}$ i construïm els punts R i S a una distància 1 de P sobre r i s, respectivament. A continuació, construïm la recta r' paral·lela a r que passa per R i la recta s' paral·lela a s que passa per S. Les rectes es tallen en el punt Q, i per tant obtenim que la recta que passa per P i Q biseca l'angle $\angle(A, P, B)$. □

Teorema 8.10. *Sigui $n \geq 3$. Aleshores, el polígon regular de n costats és construïble amb regle i compàs de puntes si i només si és construïble amb regle i compàs.*

Demostració. Clarament, com $\mathbb{P} \subset \mathbb{E}$, tenim que els únics candidats a polígons construïbles amb regle i compàs de puntes són els polígons construïbles amb regle i compàs. Per conseqüència del Teorema 5.8, tenim que tots aquests són construïbles amb regle i compàs de puntes, ja que $\sqrt{p} \in \mathbb{P}$ per tot primer (8.3) i podem bisecar tot angle amb regle i compàs de puntes (8.9). □

Cal comentar, més enllà d'aquest resultat, que Martin ens demostra que les construccions amb regle i compàs de puntes són les mateixes que les construccions amb regle i bisector d'angles (l'eina que ens permet bisecar tot angle) [12, Thm. 5.4]. Per tant, tindre un bisector o un compàs de puntes, a més del regle, és equivalent a que es compleixi la hipòtesi IV.

9 Construccions amb regle marcat

En aquesta secció parlarem de les construccions amb regle marcat, unes construccions que ens permetran construir més punts que amb regle i compàs [13]. Obtindrem el teorema de Pierpont, un resultat anàleg al teorema de Gauss-Wantzel però per construccions amb regle marcat.

Introduïm el regle marcat, que, a més de permetre'ns fer totes les construccions amb regle, ens permetrà construir els punts R i S a distància 1 si són col·lineals amb un punt P de regle marcat i estan sobre dues rectes l i m de regle marcat. Aquesta nova construcció és una classe de construccions anomenades *neusis*, que consisteixen a col·locar un segment de longitud a, anomenada el diastema, entre dues corbes donades (l i m), de manera que el segment (o la seva extensió) passa a través d'un punt donat P, tal com es veu en la figura 1. Aquesta distància a, que equival a 1 en el nostre cas, és la distància entre les "marques" del regle marcat. Fixem-nos en la figura que la neusis està lligada amb fer girar el regle (amb P com centre de rotació) fins a trobar la distància entre les dues corbes tal que estiguin a la distància a. Aquesta és la definició precisa que es dona a [12, Ch. 9]. Definim formalment els punts construïbles amb regle marcat com

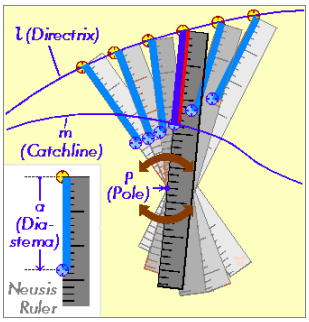


Figura 1: Construcció amb neusis [4]

Definició 9.1 (Punt construïble amb regle marcat)**.** En el pla de coordenades cartesianes $\mathbb{R}^2$, diem que un punt P és construïble amb regle marcat si és l'últim terme d'una successió finita $P_{-2}, P_{-1}, P_0, P_1, \ldots, P_n$, on $P_{-2} = (0,0)$, $P_{-1} = (1,0)$ i $P_0 = (0,1)$ són els punts base i on P_i per tot $i > 0$ és un dels següents punts:

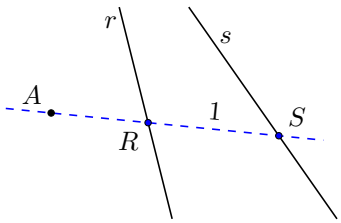
i) El punt d'intersecció de dues rectes secants formades per punts previs a P_i en la successió.

ii) Els punts R o S a una unitat de distància i col·lineals amb un punt previ a P_i en la successió, tals que R i S estan sobre rectes diferents formades per punts previs a P_i en la successió.

A més, assumirem les mateixes definicions per regle, circumferència i nombre de regle marcat que hem donat al llarg del treball.

Comencem veient que tots els punts de regle són de regle marcat, i per tant, tenim que el conjunt de nombres de regle marcat és un cos, que denotarem $\mathbb{V}$, per motius que veurem més endavant.

Interpretem el punt ii) de la definició, que correspon a la neusis entre dues rectes. Seguint la figura de sota, siguin R i S els punts que s'obtenen (a distància 1), r i s les rectes que passen sobre cada respectiu punt i A el punt col·lineal als anteriors.



Per definició, donat P un punt de regle marcat, existeix una successió finita de punts $P_{-2}, P_{-1}, P_0, P_1, \ldots, P_n$ tal que $P = P_n$ s'obté per un dels casos de

la Definició 9.1. Per la Proposició 3.3, sabem que els coeficients de les rectes estan en el mínim cos K que conté les coordenades dels punts previs a P en la successió. Sabem que la intersecció de dues rectes no ens proporciona nous punts del cos (3.4), per tant haurem de centrar-nos en la segona construcció de la definició.

Siguin $R = (x, y)$ i $S = (z, w)$, com la figura d'abans, els dos punts que estan a una unitat de distància, $A = (a, b)$ amb $a, b \in K$ el punt col·lineal amb els anteriors, i r i s les rectes amb coeficients a K que passen, respectivament, per R i S. Sabem que l'equació de la recta r és o bé de la forma $\{(X, Y) \mid Y = m'X + n'\}$ o bé $\{(X, Y) \mid X = m'\}$, i similarment de la de s és $\{(X, Y) \mid Y = mX + n\}$ o $\{(X, Y) \mid X = m\}$, amb $m', m, n', n \in K$.

Estudiarem el grau de l'extensió $K \subseteq K(x, y)$, és a dir, de les coordenades de R. Com A, R i S són col·lineals, es compleix

$$(x - z)(b - y) = (y - w)(a - x),$$

i com R i S estan a una unitat de distància:

$$(x - z)^2 + (y - w)^2 = 1,$$

aleshores, multiplicant la segona per $(b - y)^2$ i substituint-hi la primera obtenim

$$(y - w)^2(a - x)^2 + (y - w)^2(b - y)^2 = (b - y)^2.$$

Separarem casos en funció dels pendents de les rectes r i s. Centrem-nos en el cas quan s és horitzontal, és a dir, quan $s = \{(X, Y) \mid Y = n\}$ amb $n \in K$ i $S = (z, w) = (z, n)$ on $n \in K$. Substituint l'equació de la recta $r = \{(X, Y) \mid Y = m'X + n'\}$, obtenim

$$(m'x + n' - n)^2(a - x)^2 + (m'x + n' - n)^2(b - m'x - n')^2 = (b - m'x - n')^2$$

i per tant x és solució d'un polinomi de grau com a molt 4 amb coeficients a K, per tant $[K(x, y) : K] \leq 4$. Anàlogament, quan la recta r és vertical, tenim que y és també solució d'un polinomi de grau com a màxim 4. El cas quan s és vertical és parell a aquest.

Parlem ara del cas quan $s = \{(X, Y) \mid Y = mX + n\}$. La transformació lineal sobre el pla cartesià $(X, Y) \longmapsto (X - mY, mX + Y)$ transforma la recta s en una recta horitzontal, és a dir, en la recta

$$s' = \{(X, Y) \mid mX + Y = m(X - mY) + n\} = \left\{(X, Y) \;\middle|\; Y = \frac{n}{1 + m^2}\right\},$$

i anomenant x', y', z', w' les imatges respectives de x, y, z, w sota aquesta transformació lineal, obtenim que

$$(x' - z')(b' - y') = (y' - w')(a' - x'),$$

i que

$$\begin{aligned}(x' - z')^2 + (y' - w')^2 &= \big((x - my) - (z - mw)\big)^2 + \big((mx + y) - (mz + w)\big)^2 \\ &= (x - z)^2 + m^2(y - w)^2 - 2m(x - y)(z - w) + \\ &\quad + m^2(x - z)^2 + (y - w)^2 + 2m(x - y)(z - w)\end{aligned}$$

$$= (1+m^2)\big((x-z)^2+(y-w)^2\big) = 1+m^2$$

i per tant estem en les mateixes condicions que quan s és horitzontal, ja que $1+m^2 \in K$, i per tant, obtenim que el grau de l'extensió $K \subseteq K(x,y)$ per tot punt és com a molt 4.

Ara que hem trobat una cota pels graus de les extensions, ens preguntem quines construccions addicionals podem fer. Comencem veient que amb regle marcat podem construir tot punt de regle i circumferència que hem introduït a la Secció 7. Si P és un punt de regle i circumferència, aleshores existeix una successió finita de punts tal que P és construïble a partir dels altres. Suposem que P s'ha obtingut per la intersecció d'una recta r i la circumferència unitat. Veiem que P i $O = (0,0)$ compleixen les hipòtesis del punt ii) de la definició de punt construïble amb regle marcat (9.1): P i O estan a distància 1, són col·lineals amb O (és un punt base i res ens impedeix considerar el mateix punt), i cada punt passa per una recta construïda per punts previs a la successió: P passa per la recta r, que està formada per punts previs a la successió, i O passa per un eix (que sempre podem escollir que no sigui la recta r). En conclusió, tot punt de regle i circumferència és de regle marcat, i pel Teorema de Poncelet-Steiner (7.2), obtenim que $\mathbb{E} \subseteq \mathbb{V} \subset \mathbb{R}$.

Diem que un cos K és vietà, anomenat així per François Viète (conegut també com a Vieta), si és tancat per l'arrel cúbica i per trisecció, és a dir, si per tot $x \in K$, $\sqrt[3]{x} \in K$, i si per tot $\cos(\theta) \in K$, $\cos(\frac{\theta}{3}) \in K$. Es pot demostrar que $\mathbb{V}$ és un cos vietà, però no ho veurem en aquest treball ([12, Th. 9.3-9.6] i [8] proporcionen demostracions). És més, en realitat $\mathbb{V}$ és el mínim cos vietà, i per tant, denotem aquest cos amb una V de Vieta, com es deduirà de la següent proposició:

Proposició 9.2. *Sigui $x \in \mathbb{R}$. Aleshores, $x \in \mathbb{V}$ si i només si existeix una torre de cossos*

$$\mathbb{Q} = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_n$$

tal que $x \in K_n \subset \mathbb{R}$ i $[K_{i+1} : K_i] \leq 4$ per tot i. En aquest cas direm que K_n és una 2-3-4-torre real sobre $\mathbb{Q}$.

Demostració. Comencem veient la implicació cap a la dreta ($\Longrightarrow$). Per definició, tenim que $x \in \mathbb{V}$ si i només si $(x,0)$ és construïble amb regle marcat. Si $P_{-2}, P_{-1}, P_0, P_1, \ldots, P_n$ és la successió de punts tals que $P_n = (x,0)$ i K_k el mínim cos que conté les coordenades de P_k i els punts anteriors, aleshores per raonament anterior trobem una torre de cossos $K_0 \subseteq K_1 \subseteq \cdots \subseteq K_n$ tals que $[K_{i+1} : K_i] \leq 4$ per tot i. Finalment, per construcció dels cossos de la torre, tenim que $K_0 = \mathbb{Q}$ i $x \in K_n \subset \mathbb{R}$.

Veiem ara la implicació cap a l'esquerra ($\Longleftarrow$). Si $x \in \mathbb{Q}$, tenim directament que $x \in \mathbb{V}$, i per tant podem assumir que $1 < [K_{i+1} : K_i] \leq 4$ per tot i. Veurem que $K_i \subset \mathbb{V}$ per tot i per inducció. En el cas $i = 0$ tenim que $K_0 = \mathbb{Q} \subset \mathbb{V}$. Suposem $K_i \subset \mathbb{V}$ i vegem que $K_{i+1} \subset \mathbb{V}$. Com $1 < [K_{i+1} : K_i] \leq 4$, existeix un element $\alpha \in K_{i+1}$ tal que $K_{i+1} = K_i(\alpha)$ i tal que $\mathrm{Irr}(\alpha, K_i)[x]$ és de grau $[K_{i+1} : K_i]$. Per tant, α és l'arrel d'un polinomi de grau 2, 3 o 4 amb coeficients en $K_i \subset \mathbb{V}$.

Per entendre el final de la resolució s'han de recordar les equacions de Cardano per la resolució de polinomis de grau 3, i la resolució de polinomis de grau 4, que sempre es pot reduir al càlcul de polinomis de grau menor. Sabem que

podem resoldre polinomis de grau 2, ja que en particular, $\mathbb{V}$ és euclidià i α és real, mentre que la resolució de grau polinomis de grau 3 requerirà només poder construir arrels cúbiques i trisecar l'angle, que es poden realitzar, ja que $\mathbb{V}$ és vietà [12, Th. 9.3]. $\square$

D'aquesta prova obtenim que $\mathbb{V}$ és el mínim cos tal que conté tota arrel real d'un polinomi de grau 2, 3 o 4 amb coeficients racionals. El resultat també es pot millorar només demanant que $[K_{i+1} : K_i] \leq 3$, és a dir, que K_n sigui una 2-3-torre real sobre $\mathbb{Q}$. En efecte, si $[K_{i+1} : K_i] = 4$, aleshores $K_{i+1} = K_i(\beta)$ on β és arrel d'un polinomi de grau 4, i per tant podem substituir K_{i+1} pel cos de real descomposició de $\mathrm{Irr}(\beta, K_i)[x]$, que es pot escriure com una 2-3-torre real sobre K_i, ja que β es pot expressar mitjançant arrels quadrades i cúbiques [2, p. 161-162]. Com a conseqüència obtenim el següent resultat:

Corol·lari 9.3. *Si $x \in \mathbb{V}$, aleshores $[\mathbb{Q}(x) : \mathbb{Q}] = 2^r 3^s$ per alguns $r, s \geq 0$.*

Demostració. Per la Proposició 9.2, tenim una extensió de cossos

$$\mathbb{Q} \subseteq K_1 \subseteq \cdots \subseteq K_n \subset \mathbb{R}$$

on $x \in K_n$ i $[K_{i+1} : K_i] \leq 4$ per tot i. Per la fórmula de les torres tenim que

$$[K_n : \mathbb{Q}] = [K_n : K_{n-1}] \cdots [K_2 : K_1][K_1 : \mathbb{Q}]$$

i com cada extensió és de grau 1, 2, 3 o $4 = 2^2$, tenim que $[K_n : \mathbb{Q}] = 2^{r'} 3^{s'}$ per uns certs $r', s' \geq 0$. Com $\mathbb{Q} \subseteq \mathbb{Q}(x) \subseteq K_n$, aleshores $[\mathbb{Q}(x) : \mathbb{Q}]$ divideix $[K_n : \mathbb{Q}]$ i per tant $[\mathbb{Q}(x) : \mathbb{Q}] = 2^r 3^s$ per $r \leq r'$ i $s \leq s'$. $\square$

Amb el resultat anterior ja podríem demostrar el Teorema de Pierpont amb una prova similar a la que donem a la Secció 6.

Els resultats que introduirem a continuació consistiran a trobar per quins n el grau de l'extensió $\mathbb{Q} \subseteq \mathbb{Q}(\cos(\frac{2\pi}{n}))$ és un múltiple de 2 i 3. Recordem que havíem reduït la pregunta sobre la construcció de polígons regulars a veure que $\cos(\frac{2\pi}{n})$ i $\sin(\frac{2\pi}{n})$ són elements del cos de nombres construïbles, però en aquest cas, tenim que $\cos(\frac{2\pi}{n}) \in \mathbb{V}$ si i només si $\sin(\frac{2\pi}{n}) \in \mathbb{V}$, ja que $\mathbb{V}$ és un cos euclidià i $\cos^2(\theta) + \sin^2(\theta) = 1$ per tot $\theta \in [0, 2\pi]$.

Serà necessari recordar també alguns resultats de la teoria de Galois. Definim el grup de Galois d'una extensió de cossos algebraica $K \subseteq L$ com

$$\mathrm{Gal}(L/K) = \{f \in \mathrm{Aut}(L) \mid f|_K = \mathrm{id}\},$$

i sabem que $|\mathrm{Gal}(L/K)| \leq [L : K]$. Diem que una extensió de cossos algebraica $K \subseteq L$ és de Galois si és una extensió separable (si $\alpha \in L$, aleshores $\mathrm{Irr}(\alpha, K)[x]$ no té arrels múltiples a L) i normal (si $\alpha \in L$, aleshores totes les arrels de $\mathrm{Irr}(\alpha, K)[x]$ són a L). Si l'extensió $K \subseteq L$ és de Galois, aleshores $|\mathrm{Gal}(L/K)| = [L : K]$ i podrem aplicar el teorema fonamental de la teoria de Galois finita, que ens dona una correspondència un a un entre el reticle de cossos intermedis de l'extensió $K \subseteq L$ i el reticle de subgrups de $\mathrm{Gal}(L/K)$. Més precisament, F és un cos intermedi de l'extensió, $K \subseteq F \subseteq L$, tal que $[F : K] = n$, si i només si existeix un subgrup $H = \mathrm{Gal}(L/F)$ de $\mathrm{Gal}(L/K)$ d'índex n, i a més tenim que l'extensió $K \subseteq F$ és normal si i només si H és un subgrup normal.

En el nostre cas, com treballem amb extensions sobre cossos de característica 0, tenim que tota extensió algebraica és separable, i per tant serà de Galois si i

només si és normal. Donada ξ una arrel n-èsima primitiva de la unitat, tenim que l'extensió $\mathbb{Q} \subseteq \mathbb{Q}(\xi)$ és de Galois, ja que les arrels del polinomi $\mathrm{Irr}(\xi, \mathbb{Q})[x]$ són potències de ξ, i per tant a $\mathbb{Q}(\xi)$. El grup de Galois d'aquesta extensió és isomorf a $\mathbb{Z}_n^*$, el grup d'elements invertibles de $\mathbb{Z}_n$, que és un grup abelià d'ordre $\phi(n)$, on ϕ és la funció ϕ d'Euler. Coneixent aquests fets podem demostrar els següents resultats.

Lema 9.4. *Siguin $n \geq 3$. Aleshores,*

$$\phi(n) = 2\big[\mathbb{Q}\big(\cos(\tfrac{2\pi}{n})\big) : \mathbb{Q}\big].$$

Demostració. Sigui $\xi = \mathrm{e}^{\frac{2\pi \mathrm{i}}{n}}$, aleshores

$$2\cos(\tfrac{2\pi}{n}) = \xi + \bar{\xi} = \mathrm{e}^{\frac{2\pi \mathrm{i}}{n}} + \mathrm{e}^{-\frac{2\pi \mathrm{i}}{n}}$$

i per tant $[\mathbb{Q}(\cos(\frac{2\pi}{n})) : \mathbb{Q}] = [\mathbb{Q}(\xi + \bar{\xi}) : \mathbb{Q}]$. Considerem l'extensió de cossos $\mathbb{Q} \subseteq \mathbb{Q}(\xi + \bar{\xi}) \subseteq \mathbb{Q}(\xi)$. Pels fets anteriors, com ξ és una arrel n-èsima de la unitat, tenim que

$$[\mathbb{Q}(\xi) : \mathbb{Q}] = \big|\mathrm{Gal}\big({}^{\mathbb{Q}(\xi)}/_{\mathbb{Q}}\big)\big| = |\mathbb{Z}_n^*| = \phi(n).$$

Calculem ara $[\mathbb{Q}(\xi) : \mathbb{Q}(\xi + \bar{\xi})]$, que equival al grau de $\mathrm{Irr}(\xi, \mathbb{Q}(\xi + \bar{\xi}))[x]$. Tenim que $p(x) = x^2 - (\xi + \bar{\xi})x + 1 \in \mathbb{Q}(\xi)[x]$ és un polinomi amb arrels ξ i $\bar{\xi}$, que són complexes no reals per tot $n \geq 3$. Aleshores, com $\mathrm{Irr}(\xi, \mathbb{Q}(\xi + \bar{\xi}))[x] \mid p(x)$ i $\mathbb{Q}(\xi + \bar{\xi}) \subset \mathbb{R}$, tenim que $\mathrm{Irr}(\xi, \mathbb{Q}(\xi + \bar{\xi}))[x] = p(x)$ de grau 2. Per tant, $[\mathbb{Q}(\xi) : \mathbb{Q}(\xi + \bar{\xi})] = 2$ i substituint aquestes igualtats en la fórmula de les torres per l'extensió obtenim que

$$[\mathbb{Q}(\xi) : \mathbb{Q}] = [\mathbb{Q}(\xi) : \mathbb{Q}(\xi + \bar{\xi})][\mathbb{Q}(\xi + \bar{\xi}) : \mathbb{Q}] \Longleftrightarrow \phi(n) = 2[\mathbb{Q}(\xi + \bar{\xi}) : \mathbb{Q}]. \quad \square$$

Proposició 9.5. *Sigui $n \geq 3$. Un polígon regular de n costats és construïble amb regle marcat si i només si $\phi(n) = 2^{r+1}3^s$ per certs $r, s \geq 0$.*

Demostració. Sabem que un polígon regular de n costats és construïble amb regle marcat si i només si $2\cos(\frac{2\pi}{n}) = \xi + \bar{\xi} \in \mathbb{V}$ on $\xi = \mathrm{e}^{\frac{2\pi \mathrm{i}}{n}}$. Pel Lema 9.4 tenim que

$$\phi(n) = 2[\mathbb{Q}(\xi + \bar{\xi}) : \mathbb{Q}].$$

Si el polígon de n costats és construïble amb regle marcat, tenim que $\xi + \bar{\xi} \in \mathbb{V}$, i per tant, pel Corol·lari 9.3, $[\mathbb{Q}(\xi + \bar{\xi}) : \mathbb{Q}] = 2^r 3^s$ per $r, s \geq 0$, i en conclusió

$$\phi(n) = 2[\mathbb{Q}(\xi + \bar{\xi}) : \mathbb{Q}] = 2 \cdot 2^r 3^s = 2^{r+1}3^s.$$

Veiem ara l'altra implicació. Com el grup $\mathbb{Z}_n^* \cong \mathrm{Gal}({}^{\mathbb{Q}(\xi)}/_{\mathbb{Q}})$ és abelià, tenim que tot subgrup és normal, i en particular, pel teorema fonamental de la teoria de Galois finita, l'extensió $\mathbb{Q} \subseteq \mathbb{Q}(\xi + \bar{\xi})$ és normal i per tant de Galois. Aleshores, per hipòtesi

$$\big|\mathrm{Gal}\big({}^{\mathbb{Q}(\xi+\bar{\xi})}/_{\mathbb{Q}}\big)\big| = [\mathbb{Q}(\xi + \bar{\xi}) : \mathbb{Q}] = \frac{\phi(n)}{2} = 2^r 3^s$$

Per tant, tenim que $G = \mathrm{Gal}({}^{\mathbb{Q}(\xi+\bar{\xi})}/_{\mathbb{Q}})$ és un grup abelià d'ordre $2^r 3^s$. Pel teorema de classificació de grups abelians finits tenim que

$$G \cong \mathbb{Z}_{2^{r_1}} \times \cdots \times \mathbb{Z}_{2^{r_k}} \times \mathbb{Z}_{3^{s_1}} \times \cdots \times \mathbb{Z}_{3^{s_l}}$$

on $r_i, s_j \in \mathbb{N}$ són tals que $r_1 + \cdots + r_k = r$ i $s_1 + \cdots + s_l = s$. Per tant, G és resoluble de la forma

$$\{\mathrm{id}\} = G_0 \lhd G_1 \lhd \cdots \lhd G_{r+s} = G$$

tal que G_{i+1}/G_i és d'ordre 2 si $i < r$ i d'ordre 3 sinó, i per tant, pel teorema fonamental de la teoria de Galois finita, tenim que existeix una torre de cossos

$$\mathbb{Q} = K_{r+s} \subset K_{r+s-1} \subset \cdots \subset K_0 = \mathbb{Q}(\xi + \bar{\xi}) \qquad (*)$$

on $[K_i : K_{i+1}] = 3$ si $i \geq r$ i $[K_i : K_{i+1}] = 2$ sinó, (ja que el teorema inverteix l'ordre de les inclusions). Aleshores, per la Proposició 9.2, tenim que $\xi + \bar{\xi} \in \mathbb{V}$ i per tant el polígon de n costats és construïble amb regle marcat. □

Ara només ens faltarà estudiar quins naturals n compleixen que $\phi(n) = 2^{r+1}3^s$ per certs $r, s \geq 0$. També es dedueix d'aquesta prova que un polígon és construïble amb regle i compàs si i només si $\phi(n) = 2^{r+1}$ per un cert $r \geq 0$. De la mateixa forma que tenim una classe de primers (els primers de Fermat) associats als polígons construïbles amb regle i compàs, tenim uns altres associats als polígons construïbles amb regle marcat, anomenats primers de Pierpont.

Definició 9.6 (Primer de Pierpont)**.** Direm que un primer és de Pierpont si és de la forma $2^r3^s + 1$ amb $r, s \geq 0$.

A diferència dels primers de Fermat dels quals només se'n coneixen cinc, tenim que existeixen milers de primers de Pierpont (es creu que n'hi ha infinit, però el resultat encara no s'ha provat). Els primers de Pierpont que són més petits de 100 són 2, 3, 5, 7, 13, 17, 19, 37, 73 i 97. Fixem-nos també que tot primer de Fermat és també un primer de Pierpont.

Proposició 9.7. *Sigui $n \geq 3$. Aleshores $\phi(n) = 2^{r+1}3^s$ per $r, s \geq 0$ si i només si n és de la forma*

$$n = 2^a 3^b p_1 \cdots p_k$$

on $a, b \geq 0$ i $3 < p_1 < \cdots < p_k$ són primers de Pierpont diferents.

Demostració. Sabem que tot nombre $n \geq 3$ es pot escriure de manera única com

$$n = q_1^{r_{q_1}} \cdots q_l^{r_{q_l}}$$

on $q_1 < \cdots < q_l$ són primers i $r_{q_i} > 0$ per tot i. Usant propietats de la funció ϕ d'Euler, obtenim que $\phi(n)$ sota aquesta expressió és

$$\begin{aligned}\phi(n) &= \phi(q_1^{r_{q_1}}) \cdots \phi(q_l^{r_{q_l}}) \\ &= q_1^{r_{q_1}-1}(q_1 - 1) \cdots q_l^{r_{q_l}-1}(q_l - 1) \\ &= q_1^{r_{q_1}-1} \cdots q_l^{r_{q_l}-1}(q_1 - 1) \cdots (q_l - 1).\end{aligned}$$

Veiem en particular que $\phi(n) = 2^{r+1}3^s$ per certs $r, s \geq 0$ si i només si les potències dels primers diferents de 2 i 3 són 1 i si $(q_i - 1)$ són productes de potències de 2 i 3 (o són 1). És a dir, si i només si n és de la forma

$$n = 2^a 3^b p_1 \cdots p_k$$

on p_i són primers diferents dos a dos tals que $p_i - 1 = 2^{r'}3^{s'}$ per certs $r', s' \geq 0$, és a dir, primers de Pierpont diferents, arribant d'aquesta manera al resultat que volíem veure. □

Obtenim a conseqüència de les Proposicions 9.5 i 9.7 el teorema de Pierpont:

Teorema 9.8 (Teorema de Pierpont)**.** *Sigui $n \geq 3$. Aleshores els següents enunciats són equivalents:*

1. *El polígon regular de n costats és construïble amb regle marcat.*
2. *$\phi(n) = 2^{r+1}3^s$ per certs $r, s \geq 0$.*
3. *$n = 2^a 3^b p_1 \cdots p_k$ amb $a, b \geq 0$ i $p_1, \ldots, p_k$ primers de Pierpont diferents.*

Amb aquest teorema podem provar que polígons regulars com l'heptàgon i nonàgon són construïbles amb regle marcat. Tenim que el polígon amb menys nombre de costats que no és construïble amb regle marcat és l'hendecàgon, ja que $\phi(11) = 2 \cdot 5$.

Per acabar la secció fem uns comentaris sobre la trisecció de l'angle. Hem deduït que el regle marcat ens permet trisecar tot angle, és a dir, tot punt construïble amb regle, compàs i trisector d'angles és un punt construïble amb regle marcat; però el recíproc no és cert. Gleason [8] estudia directament les construccions amb regle, compàs i trisector d'angles i dedueix que x és un nombre de regle, compàs i trisector si i només si existeix una torre de cossos

$$\mathbb{Q} = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_n$$

tal que $x \in K_n \subset \mathbb{R}$ i $K_i \subseteq K_{i+1}$ és una extensió normal de grau 3 o menor per tot i. Veiem que es tracta d'una extensió de cossos quasi idèntica a la que hem vist, però on imposem que les extensions són sempre normals. El cos de punts de regle, compàs i trisector, que podem denotar $\mathbb{T}$, és euclidià, ja que tota extensió real de grau 2 és normal, però no és vietà perquè no és tancat per arrel cúbica: per exemple, l'extensió $\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{2})$ no és una extensió normal, ja que el cos de descomposició de $\mathrm{Irr}(\sqrt[3]{2}, \mathbb{Q})[x]$ no és real. No obstant això, tenim el teorema de Gleason (on destaquem la similitud amb el Teorema 8.10).

Teorema 9.9 (Teorema de Gleason)**.** *Un polígon és construïble amb regle marcat si i només si és construïble amb regle, compàs i trisector d'angles.*

No resulta difícil provar aquest teorema a partir dels resultats que hem vist, és més, la prova és idèntica on l'únic detall que caldria comentar és que tota extensió en la torre de cossos $(*)$ dins la prova de la Proposició 9.5 és normal, que és una conseqüència immediata de l'aplicació que hem fet del teorema fonamental de la teoria de Galois finita en la demostració.

10 Construccions amb regle marcat i compàs

A continuació fem un comentari sobre les construccions amb regle marcat i compàs. Com el nom indica, aquestes construccions ens permetran fer totes les construccions permeses amb regle i compàs, i regle marcat, a més de fer neusis entre dues circumferències i una recta i circumferència. No entrarem massa en estudiar quins són els polinomis corresponents a aquestes construccions amb neusis, però donarem els resultats finals. Seguint les notacions de les pàgines prèvies i de *Geometric Constructions*, denotem $\mathbb{M}$ al cos de nombres construïbles amb regle marcat i compàs. Baragar [2] ens demostra el següent resultat

Teorema 10.1. *Sigui $x \in \mathbb{M}$. Aleshores existeix una torre de cossos*

$$\mathbb{Q} = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_n$$

tal que $x \in K_n \subset \mathbb{R}$ i $[K_{i+1} : K_i] \leq 6$ per tot i. A més es dedueix directament que $[\mathbb{Q}(x) : \mathbb{Q}] = 2^r 3^s 5^t$ per alguns $r, s, t \geq 0$.

La complexitat dels polinomis que s'obtenen a partir de les construccions i el fet que els polinomis de grau 5 i 6 no són necessàriament resolubles per radicals ens porten moltes dificultats per estudiar quins són els punts de regle marcat i compàs. No obstant això, el teorema ens dona molts resultats sobre quins nombres algebraics no són de regle marcat i compàs: per exemple, tenim que $\sqrt[7]{2} \notin \mathbb{M}$, ja que requereix la resolució d'un polinomi de grau 7.

Recordem que dèiem que un polígon regular de n costats és construïble amb regle marcat i compàs si i només si $\cos(\frac{2\pi}{n}) \in \mathbb{M}$, (ja que $\cos(\frac{2\pi}{n}) \in \mathbb{M}$ si i només si $\sin(\frac{2\pi}{n}) \in \mathbb{M}$). Per tant, pel Lema 9.4 i Teorema 10.1, deduïm que si el polígon regular de n costats és construïble amb regle marcat i compàs, aleshores necessàriament 2, 3 i 5 són els únics divisors primers de $\phi(n)$. A més, com podem garantir que tots els polígons construïbles amb regle marcat també són construïbles amb regle marcat i compàs, tenim que

Proposició 10.2. *Sigui $n \geq 3$. Aleshores*

1. *Si 2 i 3 són els únics primers divisors de $\phi(n)$, aleshores el polígon regular de n costats és construïble amb regle marcat i compàs.*

2. *Si $\phi(n)$ és divisible per un primer diferent de 2, 3 i 5, aleshores el polígon regular de n costats no és construïble amb regle marcat i compàs.*

Obtenim que el polígon regular de 23 costats és el polígon regular amb menys costats que sabem que no és construïble amb regle marcat i compàs ($\phi(23) = 2 \cdot 11$). En canvi, si 5 divideix $\phi(n)$ i no té més divisors primers a part de 2 i 3, no tindrem prou informació per garantir si és possible construir el polígon regular de n costats. El nombre més petit que compleix aquesta propietat és 11 ($\phi(11) = 2 \cdot 5$), és a dir, l'hendecàgon és el polígon més petit que no podem garantir si és construïble amb la proposició que hem donat.

Molt recentment, en l'any 2014, Benjamin i Snyder van aconseguir provar que l'hendecàgon regular és construïble amb regle marcat i compàs. La seva demostració es basa a estudiar un conjunt de construccions més senzilles que les de regle marcat i compàs, que s'anomenen *construccions amb regle marcat i compàs restringides*, que consistia a considerar només les construccions pròpies del regle i compàs i del regle marcat, juntament amb la neusis entre una recta i circumferència. Van poder provar que l'hendecàgon era construïble donant forma als polinomis sota aquestes construccions [3].

11 Construccions amb regle i p-sectors

Fem un comentari final sobre la funció ϕ d'Euler, que ens pot donar una idea més general de quins polígons són construïbles amb un cert conjunt d'eines. El valor $\phi(n)$ està directament relacionat amb el grau de les extensions $\mathbb{Q} \subseteq$

$\mathbb{Q}(\cos(\frac{2\pi}{n}), \sin(\frac{2\pi}{n}))$ i per tant també amb la construcció del polígon regular de n costats. En efecte, de la Proposició 5.3 obtenim que

$$\left[\mathbb{Q}\left(\cos(\tfrac{2\pi}{p^\alpha}), \sin(\tfrac{2\pi}{p^\alpha})\right) : \mathbb{Q}\right] = p^{\alpha-1}(p-1) = \phi(p^\alpha)$$

quan $p \neq 2$, i a més per la proposició 4.3, quan $n = ab$ i a, b són coprimers tenim que

$$\mathbb{Q}\left(\cos(\tfrac{2\pi}{n}), \sin(\tfrac{2\pi}{n})\right) = \mathbb{Q}\left(\cos(\tfrac{2\pi}{a}), \sin(\tfrac{2\pi}{a}), \cos(\tfrac{2\pi}{b}), \sin(\tfrac{2\pi}{b})\right)$$

i de la mateixa manera, $\phi(n) = \phi(a)\phi(b)$.

En conseqüència, deduïm del Teorema 5.7 que podem construir el polígon regular de n costats si el nostre conjunt d'eines, a més de contenir el regle i compàs, permet p-secar i construir $\sqrt{p}$ per tot primer p divisor de $\phi(n)$ [8, 12]. Recordem que si el conjunt d'eines conté el regle, aleshores les hipòtesis I, II i III es compleixen, i si conté el compàs de puntes, aleshores compleix la hipòtesi IV, i $\sqrt{p}$ sempre serà construïble (8.3). Obtenim d'aquesta manera aquest teorema:

Teorema 11.1. *Siguin $n \geq 3$ i $\mathscr{E}$ un conjunt d'eines que compleix les hipòtesis I, II, III i IV. Aleshores, el polígon regular de n costats és construïble amb $\mathscr{E}$ si podem p-secar angles per tot primer p divisor de $\phi(n)$.*

Per tant, per tot polígon regular existeix un conjunt d'eines que ens permeten construir el polígon. Per exemple, podrem construir el polígon de 23 costats amb regle, compàs i 11-sector d'angles, ja que $\phi(23) = 2 \cdot 11$; i és cert que també és construïble amb regle, compàs i 23-sector d'angles, però aquest resultat permet treballar amb p-sectors més petits, un resultat gens trivial, ja que no podem descompondre totes les 23-seccions en funció de p-seccions més petites. Més precisament, com $\phi(n)$ sempre és parell per $n \geq 3$, i les construccions amb regle i bisector compleixen la hipòtesi IV, obtenim del teorema que el polígon regular de n costats és construïble amb regle i tot p-sectors per cada p divisor de $\phi(n)$.

12 Taula de polígons construïbles

Acabem el treball donant una taula dels polígons construïbles de menys de 100 costats

		3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

- Construïbles amb regle i compàs coneguts pels grecs
- Construïbles amb regle i compàs provats per Gauss
- Construïbles amb regle marcat
- Construïbles amb regle marcat i compàs
- Desconeguts si són construïbles amb regle marcat i compàs
- No construïbles amb regle marcat i compàs

Referències

[1] W.S. Anglin. *Mathematics: A Concise History and Philosophy*. Undergraduate Texts in Mathematics. Springer New York, 2012.

[2] A. Baragar. "Constructions Using a Compass and Twice-Notched Straightedge". A: *The Mathematical Association of America* 109 (febr. de 2002), pàg. 151 - 164.

[3] E. Benjamin i C. Snyder. "On the construction of the regular hendecagon by marked ruler and compass". A: *Mathematical Proceddings of the Cambridge Philosophical Society* 156 (maig de 2014), pàg. 409 - 424.

[4] H. van Deukeren. *Neusis*. 2006. URL: https://commons.wikimedia.org/w/index.php?curid=644884.

[5] Euclides. *Elements*. Versió online per D.E. Joyce a https://mathcs.clarku.edu/~djoyce/java/elements/elements.html.

[6] C.F. Gauss. *Disquisitiones Arithmeticae*. Trad. de M. Villarino, M. Josephy i A. Ruiz. Vol. 14. 1987.

[7] E. Giusti. "The Geometry of the curve". A: *Beyond the compasses*. Polistampa, Firenze, 2000.

[8] A.M. Gleason. "Angle Trisection, the Heptagon, and the Triskaidecagon". A: *The American Mathematical Monthly* 14 (abr. de 1988), pàg. 185 - 194.

[9] H.P. Hudson. *Ruler & Compasses*. Longman, Green i co. London, 1916.

[10] J.-L. Lagrange. *Traité de la résolution des équations numériques de tous les degrés. Avec des notes sur plusieurs points de la théorie des équations algébriques*. Paris, Bachelier, 1826.

[11] S. Lang. *Algebra*. Graduate texts in mathematics. Springer-Verlag New York, 2002.

[12] G.E. Martin. *Geometric Constructions*. Undergraduate texts in mathematics. Springer-Verlag New York, 1998.

[13] J. Pierpont. "On an undemonstrated theorem of the Disquisitiones Arithmeticæ". A: *Bulletin of the American Mathematical Society* 2.3 (des. de 1895), pàg. 77 - 83.

[14] P.L. Wantzel. "Recherches sur les moyens de reconnaître si un problème de Géométrie peut se résoudre avec la règle et le compas". A: *Journal de mathématiques pures et appliquées* 2 (1837), pàg. 366 - 372.