



UNIVERSITAT DE
BARCELONA

Facultat de Matemàtiques
i Informàtica

GRAU DE MATEMÀTIQUES

Treball final de grau

NOMBRES CONSTRUÏBLES AMB PAPIROFLÈXIA

Autora: Alba Mur Vázquez

Director: Carlos D'Andrea

Realitzat a: Departament de Matemàtiques i Informàtica

Barcelona, 10 de juny de 2024

Abstract

In this work, we will study geometric constructions using paper folding or origami, demonstrating that this technique allows us to reproduce all the straightedge and compass constructions, and even surpass the limitations of this classical method. To conduct this study, we will rely on the algebraic content learnt during the degree, such as algebraic structures and Galois theory.

Resum

En aquest treball estudiarem les construccions geomètriques utilitzant la papiroflèxia, demostrant que aquesta tècnica permet reproduir totes les possibles construccions amb regla i compàs i, a més a més, superar les limitacions d'aquest mètode clàssic. Per dur a terme aquest estudi, ens basarem en continguts algebraics adquirits durant el grau, com les estructures algebraiques i la teoria de Galois.

Agraïments

M'agradaria començar donant les gràcies al tutor d'aquest TFG, en Carlos D'Andrea, per apostar per la idea d'aquest treball que era nova pels dos, per motivar-me a cada reunió i per fer-me creure que sóc vàlida com a matemàtica.

En segon lloc, vull agrair a la meva família, per haver-me fet costat en tot moment. En especial, mencionar a la meva mare per recordar-me sempre que fer cinc mils no és fàcil.

No em voldria oblidar dels amics i amigues, tant els que he fet en aquesta etapa com els que m'acompanyen des de fa més temps. Vull fer una menció especial a la Cris, per ser la més forta de totes i haver-nos fet costat des del primer dia. I no puc acabar sense dedicar unes últimes paraules al Lluís, per haver-me transmès la seva passió per les matemàtiques i estar sempre disposat a ajudar-me.

Moltes gràcies a tothom.

Índex

1	Introducció	1
1.1	El projecte	1
1.2	Estructura de la Memòria	2
2	Construccions amb regla i compàs	3
2.1	Els nombres construïbles amb regla i compàs	3
2.2	Construccions bàsiques amb regla i compàs	4
2.3	El conjunt dels nombres construïbles amb regla i compàs	6
2.4	Polígons regulars construïbles amb regla i compàs	14
2.5	Construccions impossibles amb regla i compàs	14
3	Primeres construccions amb papiroflèxia	16
3.1	Axiomes de la papiroflèxia	16
3.2	Trisecció de l'angle	19
3.3	Recta tangent a dues paràboles	21
3.4	Translació de distàncies	25
4	La papiroflèxia equivalent al regla i compàs	27
4.1	Suma	27
4.2	Multiplicació	28
4.3	Arrel quadrada	30
5	El conjunt dels nombres construïbles amb papiroflèxia	34
5.1	Polígons regulars construïbles amb papiroflèxia	39
5.2	Construccions impossibles	41
6	Requisits matemàtics	42
6.1	Requisits geomètrics	42
6.2	Requisits algebraics	43
7	Conclusions	49

1 Introducció

Les construccions amb regle i compàs són una part fonamental de la geometria clàssica, amb una història que es remunta a l'antiga Grècia. Els grecs van establir les bases d'aquestes tècniques a través d'obres magistrals com “*Els Elements*” d'Euclides. Utilitzant només un regle no graduat i un compàs, els matemàtics grecs van aconseguir resoldre problemes importants, com la construcció d'alguns polígons regulars o la divisió d'un segment en parts iguals. No obstant això, també van descobrir les seves limitacions amb problemes com la duplicació del cub, la trisecció de l'angle i la quadratura del cercle, resultant ser impossibles de resoldre només amb aquestes eines. Amb el pas del temps s'han anat desenvolupant altres eines per a fer construccions geomètriques planes que permeten creuar els límits de les construccions amb regle i compàs. La papiroflèxia és l'eina que estudiarem en aquest treball.

La papiroflèxia, també coneguda com a origami, és l'art japonès de crear figures i formes a partir d'un full de paper, sense tallar ni enganxar. Aquest art mil·lenari té els seus orígens a la Xina al voltant del segle II, però va ser al Japó on va evolucionar i es va convertir en una forma d'expressió cultural significativa. Es poden construir una gran varietat de figures, des de senzilles formes geomètriques fins a complexos models tridimensionals. Com ja hem esmentat, també podem utilitzar la papiroflèxia com a eina per a fer construccions geomètriques planes. Aquest ús de la papiroflèxia va ser introduït per primera vegada l'any 1893 per T. Sundara Row en el seu llibre “*Geometric Exercises in Paper Folding*”, [9].

En les construccions amb papiroflèxia, en comptes d'un regle i un compàs, només disposem d'un full de paper que podem doblegar, sense superposar plecs i on cada plec construeix una recta. D'entrada podem pensar que, com només podem construir rectes, la papiroflèxia és una eina menys potent que el regle i compàs, però ens sorprendrà veure que és just el contrari. Així doncs, en aquest treball veurem que la papiroflèxia no és només un art, sinó també una eina poderosa per a l'exploració matemàtica.

1.1 El projecte

En aquest treball estudiarem les construccions amb papiroflèxia tot comparant-les amb les construccions amb regle i compàs. El que ens proposem és veure que amb papiroflèxia podem construir tot el que és construïble amb regle i compàs i molt més.

Descriurem en detall els sis axiomes de la papiroflèxia tot definint els plecs bàsics d'un paper a partir dels quals podrem fer construccions. Direm que un punt és construïble amb papiroflèxia si és intersecció de dues rectes construïdes a partir d'aquests plecs bàsics. Utilitzant els axiomes farem algunes construccions bàsiques, com la d'una recta paral·lela a una altra, i altres construccions més sorprenents, com la trisecció d'un angle qualsevol, que ens farà començar a veure el potencial de la papiroflèxia.

Aleshores, estudiarem en detall els axiomes per tal de veure exactament què s'hi amaga al darrere i ens adonarem que el sisè axioma és el que ho canvia tot, ja que permet construir una recta tangent a dues paràboles a la vegada. Aquesta construcció fa que puguem resoldre qualsevol equació de tercer grau i també construir l'arrel cúbica de qualsevol nombre construït prèviament.

Utilitzant els coneixements adquirits en l'assignatura d’“*Estructures algebraïques*” estudiarem quina estructura té el conjunt de nombres construïbles amb papiroflèxia tant

si contemplem els sis axiomes com si només considerem els cinc primers. Veurem que si deixem de banda el sisè axioma el conjunt de nombres construïbles és exactament el mateix conjunt que es genera utilitzant regle i compàs.

En afegit, ens ajudarem de la Teoria de Galois apresada en l'assignatura d'“*Equacions algebraïques*” per a demostrar teoremes i proposicions claus que marcaran la diferència entre la papiroflèxia i el regle i compàs. Amb l'ajuda d'aquests resultats estudiarem els polígons construïbles i analitzarem quines de les construccions impossibles amb regle i compàs deixen de ser impossibles amb la papiroflèxia.

1.2 Estructura de la Memòria

Abans d'endinsar-nos al món de la papiroflèxia, començarem estudiant les construccions amb regle i compàs (Capítol 2). Veurem alguns resultats importants que utilitzarem més endavant en l'estudi de la papiroflèxia i ens permetran comparar aquestes dues eines de construcció geomètrica.

Dedicarem el Capítol 3 a definir les bases de les construccions amb papiroflèxia, tot detallant els axiomes a partir dels quals podrem construir. En aquest mateix capítol ens familiaritzarem amb aquesta nova eina de construcció i descriurem algunes construccions rellevants que ens permetran intuir el potencial que amaga.

Tot seguit, durant el Capítol 4, entrarem a demostrar que els cinc primers axiomes de la papiroflèxia construeixen el mateix conjunt de nombres que el generat pel regle i compàs. Per fer-ho, ens caldrà descriure com fer les operacions suma, multiplicació i arrel quadrada utilitzant papiroflèxia.

En el capítol 5 estudiarem el conjunt de nombres construïbles a partir dels sis axiomes de la papiroflèxia. Per fer-ho utilitzarem el resultat obtingut en el capítol anterior que ens permetrà fer ús dels teoremes i proposicions vistes en el capítol 2 per a demostrar resultats anàlegs per a la papiroflèxia.

Finalment, en el capítol 6 adjuntem tots els continguts matemàtics necessaris per a demostrar els resultats vistos al llarg del treball. De tota manera, se suposa que el lector té coneixements matemàtics previs sobre geometria bàsica, nombres complexos, teoria de grups, anells i cossos i teoria de Galois.

2 Construccions amb regla i compàs

Dediquem aquest capítol a descriure les construccions amb regla i compàs. Veurem alguns resultats importants, estudiarem els polígons construïbles i analitzarem algunes construccions impossibles. Aquest capítol segueix les seccions 10.1 i 10.2 del llibre [2].

2.1 Els nombres construïbles amb regla i compàs

Les construccions amb regla i compàs consisteixen en, donats una sèrie de punts del pla complex $\mathbb{C}$, determinar nous punts, rectes i circumferències a partir d'un regla (infinít, sense mesures i amb només una vora) i un compàs.

Més concretament, fer construccions amb regla i compàs consisteix en, donats una sèrie de punts, traçar rectes i circumferències de la següent manera:

(RC1) Donats $\alpha, \beta \in \mathbb{C}$ amb $\alpha \neq \beta$ podem construir (mitjançant el regla) la recta l que passa per α i β .

(RC2) Donats $\alpha, \beta, \gamma \in \mathbb{C}$ amb $\alpha \neq \beta$ podem construir (mitjançant el compàs) la circumferència C amb centre γ i radi la distància d' α a β .

A partir d'aquestes rectes i circumferències construïbles obtenim nous punts construïbles:

(RC3) A partir de dues rectes construïbles (no paral·leles, ni coincidents), construïm el seu punt d'intersecció.

(RC4) A partir d'una circumferència i una recta construïbles, construïm els seus punts d'intersecció (poden ser dos, un o cap punt).

(RC5) A partir de dues circumferències construïbles, construïm els seus punts d'intersecció (de nou, poden ser dos, un o cap punt).

Definició 2.1.1. Diem que $\alpha \in \mathbb{C}$ és un *nombre construïble amb regla i compàs* si existeix una seqüència finita de construccions RC1, RC2, RC3, RC4 i RC5 que comença amb els punts donats 0 i 1 i acaba amb α .

Observació 2.1.2. Tots els nombres naturals són construïbles amb regla i compàs. Donats 0 i 1, per una banda, tracem l'eix d'abscisses i, per l'altra banda, utilitzant RC2 obtenim la circumferència amb centre 1 i radi la distància de 0 a 1. Per RC4 aconseguim el punt de tall de l'eix i la circumferència que és exactament el punt 2. Repetint el procediment utilitzant 1 i 2 obtindrem el 3 i, successivament, van apareixent tots els naturals. De forma anàloga aconseguirem també tots els nombres enters negatius.

2.2 Construccions bàsiques amb regla i compàs

Dediquem aquesta secció a detallar com fer algunes construccions bàsiques amb regla i compàs, per així també familiaritzar-nos amb aquest tipus de construccions.

- Mediatriu d'un segment.

Donat un segment AB , construïm dues circumferències utilitzant $RC2$: la primera amb centre A i radi la distància d' A a B i la segona amb centre B i radi la distància d' A a B . Amb $RC5$ construïm els seus dos punts de tall i que anomenarem C i D . Amb $RC1$ construïm la recta que passa per C i D que és exactament la mediatriu del segment AB .

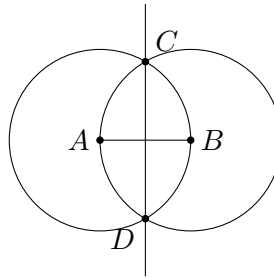


Figura 2.1. Construcció de la mediatriu amb regla i compàs.

- Bisectriu d'un angle donat.

Donat un angle $\angle ABC$, on A, B i C són 3 punts construïbles, amb $RC2$ construïm una circumferència amb centre B i radi qualsevol. Per $RC4$ construïm dos punts: el punt D com la intersecció de la circumferència amb el segment AB i el punt E com la intersecció de la circumferència amb el segment BC . Ara, utilitzant $RC2$ construïm dues circumferències més: una amb centre D i radi la distància de D a E i l'altra amb centre E i radi la distància de D a E . A continuació, per $RC5$ obtenim el punt F com a intersecció d'aquestes dues circumferències que acabem de construir. Finalment, per $RC1$ tracem la recta que passa per F i B . Aquesta recta bisecta l'angle $\angle ABC$ donat inicialment.

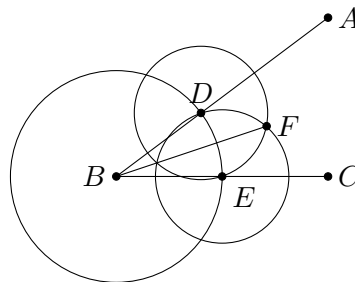


Figura 2.2. Construcció de la bisectriu amb regla i compàs.

- La recta perpendicular a una recta donada que passa per un punt donat.

Donada una recta r i un punt A , per $RC2$ construïm una circumferència amb centre A i radi tal que es talli amb la recta r en dos punts diferents. Per $RC4$ construïm aquests dos punts d'intersecció, els anomenem B i C . Ara, per $RC2$ construïm

dues circumferències: la primera amb centre B i radi la distància de B a C i la segona amb centre C i radi la distància de B a C . Per $RC5$ construïm els punts d'intersecció entre aquestes dues circumferències i els anomenem D i E . Per $RC1$ construïm la recta que passa per D i E que és exactament la recta perpendicular a r que passa per A .

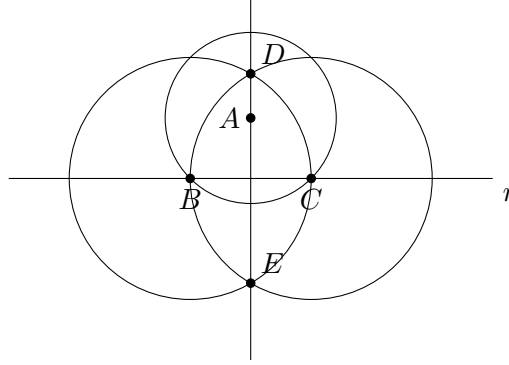


Figura 2.3. Construcció d'una recta perpendicular amb regla i compàs.

- La recta paral·lela a una recta donada que passa per un punt donat.

Donada una recta r i un punt A , per $RC2$ construïm una circumferència amb centre B , sent B un punt qualsevol de la recta r , i radi la distància d' A a B , l'anomenarem s . El següent pas és construir la recta perpendicular a r que passa per B . Per fer-ho, per $RC4$ comencem construint els punts d'intersecció de la circumferència amb la recta r , els anomenem C i D . Tot seguit, per $RC2$ construïm dues circumferències: una amb centre C i radi la distància de C a D i l'altra amb centre D i radi la distància de C a D . Per $RC5$ obtenim el seu punt d'intersecció que anomenem E . Per $RC1$ tenim la recta que passa per E i B que és exactament la recta perpendicular a r que passa per B , l'anomenem t .

Ara, per $RC4$ obtenim el punt d'intersecció de la recta t amb la circumferència s , l'anomenem F . A continuació, per $RC2$ tracem la circumferència amb centre F i radi la distància de F a A . Per $RC5$ trobem el punt de tall entre aquesta circumferència i s , a aquest punt l'anomenem G . Per acabar, per $RC1$ tracem la recta que passa per A i G que és exactament la recta paral·lela a r que passa per A .

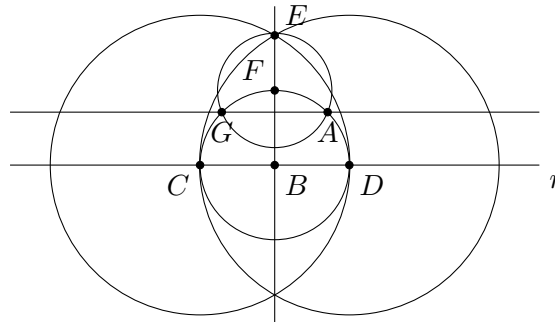


Figura 2.4. Construcció d'una recta paral·lela amb regla i compàs.

Observació 2.2.1. A partir dels punts 0 i 1 podem traçar l'eix d'abscisses utilitzant $RC1$ i l'eix d'ordenades construint la recta perpendicular a l'eix d'abscisses que passa pel 0.

2.3 El conjunt dels nombres construïbles amb regla i compàs

Definició 2.3.1. Definim $\mathcal{C}$ com el següent conjunt:

$$\mathcal{C} := \{\alpha \in \mathbb{C} \mid \alpha \text{ és construïble amb regla i compàs}\}$$

i l'anomenem *conjunt dels nombres construïbles amb regla i compàs*.

Teorema 2.3.2. *El conjunt $\mathcal{C}$ és subcòs de $\mathbb{C}$. A més a més,*

- (a) *Si $\alpha = a + ib \in \mathbb{C}$, amb $a, b \in \mathbb{R}$. Aleshores, $\alpha \in \mathcal{C}$ si, i només si, $a, b \in \mathcal{C}$.*
- (b) *Si $\alpha \in \mathcal{C}$, aleshores $\sqrt{\alpha} \in \mathcal{C}$.*

Demostració. Comencem demostrant que $\mathcal{C}$ és subcòs de $\mathbb{C}$. Les operacions suma i producte que considerem són la suma i el producte en els complexos tal com les coneixem. Així doncs, cal veure que compleix:

(i) $\mathcal{C}$ és subanell de $\mathbb{C}$. Per veure que és subanell cal provar dos punts:

- $(\mathcal{C}, +)$ és subgrup de $(\mathbb{C}, +)$. Vegem-ho:
 - $\mathcal{C}$ és un subconjunt no buit de $\mathbb{C}$. Per definició de $\mathcal{C}$, tenim $\mathcal{C} \subset \mathbb{C}$. Com $0, 1 \in \mathcal{C}$, tenim que $\mathcal{C} \neq \emptyset$. Per tant, $\mathcal{C}$ és un subconjunt no buit de $\mathbb{C}$.
 - Si $\alpha, \beta \in \mathcal{C}$, aleshores $\alpha + \beta \in \mathcal{C}$. Utilitzant que 0 és construïble, per *RC2* podem construir dues circumferències: una amb centre α i radi la distància de 0 a β i l'altra amb centre β i radi la distància de 0 a α . Una de les interseccions d'aquestes dues circumferències és $\alpha + \beta$. La següent figura mostra un exemple d'aquesta construcció:

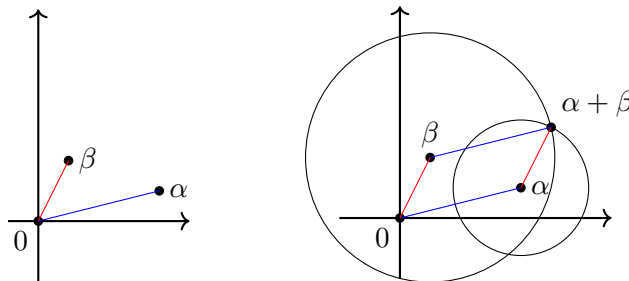


Figura 2.5. Construcció de la suma amb regla i compàs.

- $\mathcal{C}$ té estructura de grup amb la suma. Compleix les següents propietats:
 - * Compleix la propietat associativa per ser la suma de complexos una operació associativa.
 - * L'element neutre és el 0 i $0 \in \mathcal{C}$.
 - * L'element oposat de $\alpha \in \mathcal{C}$ és $-\alpha$. Per *RC1* tracem la recta que passa per 0 i α . Per *RC2* construïm la circumferència centrada en el 0 i amb radi la distància de 0 a α . Per *RC4* obtenim els dos punts de tall de la recta amb la circumferència: un és α i l'altre $-\alpha$. Per tant, $-\alpha \in \mathcal{C}$.
- $\mathcal{C}$ és tancat respecte al producte de $\mathbb{C}$.

(ii) $\alpha^{-1} \in \mathcal{C}, \forall \alpha \in \mathcal{C} \setminus \{0\}$.

Deixem pendents aquests dos últims apartats, ja que per a provar-los ens cal primer demostrar l'apartat (a) del teorema.

(a) Sigui $\alpha = a + ib \in \mathbb{C}$, amb $a, b \in \mathbb{R}$. Volem veure que $\alpha \in \mathcal{C}$ si, i només si, $a, b \in \mathcal{C}$.
Veiem les dues implicacions per separat:

$\Leftarrow$ Suposem que $a, b \in \mathcal{C}$. Com tenim que $a, b \in \mathbb{R}$ tindrem que a i b es troben sobre l'eix d'abscisses. El primer pas que hem de fer és transportar b a l'eix d'ordenades. Amb *RC2* tracem la circumferència amb centre 0 i radi la distància de 0 a b . Per *RC4* obtenim els dos punts d'intersecció de la circumferència amb l'eix d'ordenades, ens quedem amb el punt que tingui el mateix signe que b , aquest punt serà ib . Tot seguit, tracem la recta paral·lela a l'eix d'ordenades que passa per a i la recta paral·lela a l'eix d'abscisses que passi per ib . El punt de tall d'aquestes dues rectes és α . Per tant, $\alpha \in \mathcal{C}$.

$\Rightarrow$ Suposem que $\alpha \in \mathcal{C}$. Podem traçar la recta paral·lela a l'eix d'ordenades que passa per α , la intersecció d'aquesta recta amb l'eix d'abscisses és el punt $a \in \mathbb{R}$. També podem traçar la recta paral·lela a l'eix d'abscisses que passa per α , la intersecció d'aquesta recta amb l'eix d'ordenades ens dona el punt ib . De la mateixa manera que abans, construïm la circumferència amb centre 0 i radi la distància de 0 a ib i l'intersequem amb l'eix d'abscisses. Ens quedem amb el punt d'intersecció que tingui el mateix signe que ib , aquest punt serà $b \in \mathbb{R}$. Per tant, $a, b \in \mathcal{C}$.

Seguim, ara, amb la demostració que $\mathcal{C}$ és subcòs de $\mathbb{C}$:

- $\mathcal{C}$ és tancat respecte al producte de $\mathbb{C}$. Cal veure que si $\alpha, \beta \in \mathcal{C}$, aleshores $\alpha\beta \in \mathcal{C}$. Farem primer, el cas que $\alpha, \beta \in \mathcal{C} \cap \mathbb{R}$.

Si α o β valen 0, aleshores $\alpha\beta = 0 \in \mathcal{C}$. Així doncs, suposem que $\alpha, \beta > 0$, per ser reals positius els trobem sobre l'eix d'abscisses positiu. Tal com hem fet abans, a partir de β podem construir $i\beta$. També, a partir d'1 podem obtenir i . Per *RC1* tracem la recta que passa per i i per α . Tot seguit, contruïm la recta paral·lela a aquesta que passa per $i\beta$. Anomenem x al punt d'intersecció d'aquesta segona recta amb l'eix d'abscisses. La següent figura mostra aquestes construccions que acabem de descriure en el cas en què $\beta > 1$ i quan $\beta < 1$:

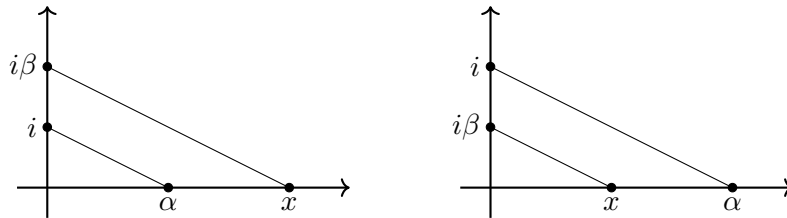


Figura 2.6. Construcció del producte amb regla i compàs amb $\alpha, \beta > 0$.

En ambdós casos, pel primer teorema de Tales (Teorema 6.1.3) obtenim que:

$$\frac{x}{\alpha} = \frac{i\beta}{i} \quad \Rightarrow \quad x = \alpha\beta$$

I, per tant, $\alpha\beta \in \mathcal{C} \cap \mathbb{R}, \forall \alpha, \beta \in \mathcal{C} \cap \mathbb{R}$ amb $\alpha, \beta > 0$.

Fem amb detall, també, el cas en què $\alpha > 0$ i $\beta < 0$. Fent les mateixes construccions que abans obtenim la situació que mostra la següent figura, pel cas $\beta > 1$ i quan $\beta < 1$:

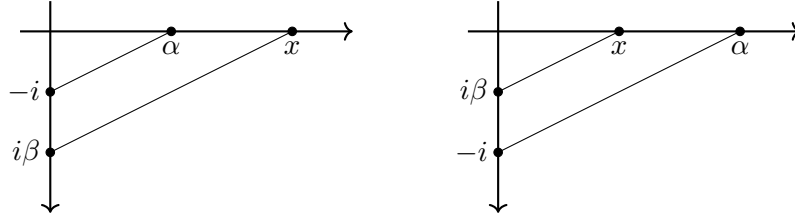


Figura 2.7. Construcció del producte amb regla i compàs amb $\alpha > 0$ i $\beta < 0$.

De nou, pel primer teorema de Tales, obtenim que:

$$\frac{x}{\alpha} = \frac{i\beta}{-i} \Rightarrow x = -\alpha\beta$$

Per RC2 construïm la circumferència de centre 0 i radi la distància d' α a β . La intersecció de l'eix d'abscisses negatiu amb la circumferència és exactament $\alpha\beta$. Per tant, $\alpha\beta \in \mathcal{C} \cap \mathbb{R}, \forall \alpha, \beta \in \mathcal{C} \cap \mathbb{R}$ amb $\alpha > 0$ i $\beta < 0$.

Anàlogament, obtenim que pels casos $\alpha, \beta < 0$ i $\alpha < 0, \beta > 0$ també es compleix que $\alpha\beta \in \mathcal{C} \cap \mathbb{R}$. Per tant, acabem de veure que $\alpha\beta \in \mathcal{C} \cap \mathbb{R}, \forall \alpha, \beta \in \mathcal{C} \cap \mathbb{R}$.

Ara, considerem $\alpha, \beta \in \mathcal{C} \subset \mathbb{C}$. Escrivim $\alpha = a + ib$ i $\beta = c + id$, per $a, b, c, d \in \mathbb{R}$. Per l'apartat (a) d'aquest teorema, com $\alpha, \beta \in \mathcal{C}$, aleshores $a, b, c, d \in \mathcal{C} \cap \mathbb{R}$. Per la definició del producte en els complexos tenim:

$$\alpha\beta = (a + ib)(c + id) = ac - bd + i(ad + bc)$$

Com $a, b, c, d \in \mathcal{C} \cap \mathbb{R}$, pel que acabem de veure tenim que $ac, bd, ad, bc \in \mathcal{C} \cap \mathbb{R}$. Ara, per ser $(\mathcal{C}, +)$ subgrup de $(\mathbb{C}, +)$ tenim que $ac - bd, ad + bc \in \mathcal{C} \cap \mathbb{R}$. I, en últim lloc, per l'apartat (a) d'aquest teorema, com $ac - bd, ad + bc \in \mathcal{C}$, aleshores $ac - bd + i(ad + bc) = \alpha\beta \in \mathcal{C}$.

Acabem de provar que $\mathcal{C}$ és tancat respecte al producte de $\mathbb{C}$.

Per tant, podem concloure que $\mathcal{C}$ és subanell de $\mathbb{C}$.

(ii) $\alpha^{-1} \in \mathcal{C}, \forall \alpha \in \mathcal{C} \setminus \{0\}$. Fem primer el cas en què $\alpha \in (\mathcal{C} \setminus \{0\}) \cap \mathbb{R}$. Suposem que $\alpha > 0$, per tant, es troba a l'eix d'abscisses positiu. Com ja hem fet abans, construïm $i\alpha$ que està sobre l'eix d'ordenades positiu. Per RC1 tracem la recta que passa per $i\alpha$ i 1. Tot seguit, construïm una recta paral·lela que passi per i . El punt de tall d'aquesta segona recta amb l'eix d'abscisses l'anomenem x . Les següents figures mostren aquestes construccions que acabem de descriure en el cas en què $\alpha > 1$ i quan $\alpha < 1$:

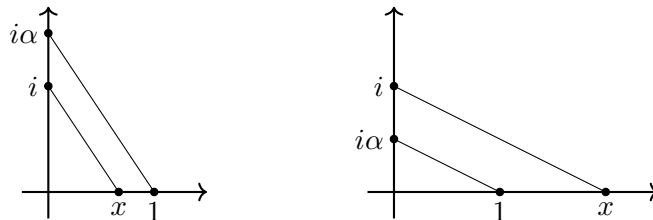


Figura 2.8. Construcció de l'element invers amb regla i compàs amb $\alpha > 0$.

En ambdós casos, pel primer teorema de Tales tenim:

$$\frac{x}{1} = \frac{i}{i\alpha} \Rightarrow x = \frac{1}{\alpha} = \alpha^{-1}$$

Per tant, $\alpha^{-1} \in (\mathcal{C} \setminus \{0\}) \cap \mathbb{R}$ per $\alpha \in (\mathcal{C} \setminus \{0\}) \cap \mathbb{R}$ amb $\alpha > 0$. Anàlogament, obtenim el mateix resultat per a $\alpha < 0$.

Per tant, acabem de veure que $\alpha^{-1} \in (\mathcal{C} \setminus \{0\}) \cap \mathbb{R}, \forall \alpha \in (\mathcal{C} \setminus \{0\}) \cap \mathbb{R}$.

Ara, considerem $\alpha \in \mathcal{C} \setminus \{0\} \subset \mathbb{C}$. Escrivim $\alpha = a + ib$ amb $a, b \in \mathbb{R}$ tals que a i b no són els dos 0. Per l'apartat (a) d'aquest teorema, com $\alpha \in \mathcal{C}$ aleshores, $a, b \in \mathcal{C} \cap \mathbb{R}$. Per la definició d'element invers en els complexos tenim:

$$\frac{1}{\alpha} = \frac{1}{a + ib} \cdot \frac{a - ib}{a - ib} = \frac{a - ib}{a^2 + b^2} = a \cdot (a^2 + b^2)^{-1} - i(b \cdot (a^2 + b^2)^{-1})$$

Com $a, b \in \mathcal{C} \cap \mathbb{R}$ tenim que $a^2 = a \cdot a \in \mathcal{C} \cap \mathbb{R}$ i $b^2 = b \cdot b \in \mathcal{C} \cap \mathbb{R}$. Ara, per ser $(\mathcal{C}, +)$ subgrup de $(\mathbb{C}, +)$ tenim que $a^2 + b^2 \in \mathcal{C} \cap \mathbb{R}$. Com a i b no són els dos 0, tenim que $a^2 + b^2 \in (\mathcal{C} \setminus \{0\}) \cap \mathbb{R}$. Així doncs, pel que acabem de veure $(a^2 + b^2)^{-1} \in (\mathcal{C} \setminus \{0\}) \cap \mathbb{R}$. Per tant, $a \cdot (a^2 + b^2)^{-1}, b \cdot (a^2 + b^2)^{-1} \in \mathcal{C} \cap \mathbb{R}$. I, finalment, per l'apartat (a) d'aquest teorema tenim que $\alpha^{-1} \in \mathcal{C}$.

Aquí acaba la demostració que $\mathcal{C}$ és subcòs de $\mathbb{C}$. Ara falta demostrar l'apartat (b) del teorema:

(b) Sigui $\alpha \in \mathcal{C}$, volem veure que $\sqrt{\alpha} \in \mathcal{C}$. Si $\alpha = 0$, aleshores $\sqrt{\alpha} = \sqrt{0} = 0 \in \mathcal{C}$. Suposem que $\alpha \neq 0$.

Escrivim α en forma polar: $\alpha = r \cdot e^{i\theta}$, amb $r \in \mathbb{R}$ tal que $r = |\alpha| > 0$ i $\theta \in [0, 2\pi)$.

Per tant:

$$\sqrt{\alpha} = \sqrt{r \cdot e^{i\theta}} = \sqrt{r} \cdot e^{i\frac{\theta}{2}}$$

Així doncs, per veure que $\sqrt{\alpha} \in \mathcal{C}$ veurem que $\sqrt{r} \in \mathcal{C}$ i $e^{i\frac{\theta}{2}} \in \mathcal{C}$.

- $e^{i\frac{\theta}{2}} \in \mathcal{C}$: Per *RC1* podem traçar la recta que passa per 0 i α . Aquesta recta amb l'eix d'abscisses generen l'angle θ . Com hem esmentat en la secció 2.2, podem bisecar un angle amb regla i compàs. Així doncs, obtenim que $\frac{\theta}{2} \in \mathcal{C}$. Ara, per *RC2* construïm la circumferència amb centre 0 i radi la distància de 0 a 1. Per *RC4*, en intersecar aquesta circumferència amb la recta que bisecta θ obtenim el punt $e^{i\frac{\theta}{2}}$.
- $\sqrt{r} \in \mathcal{C}$: Per *RC2* podem construir la circumferència de centre 0 i radi la distància de 0 a α , que és exactament r . Per tant, si intersequem aquesta circumferència amb l'eix d'abscisses obtenim r . Acabem de veure que $r \in \mathcal{C} \cap \mathbb{R}$. Per ser r construïble també podem construir $1+r$ i, en conseqüència $\frac{1+r}{2}$ (fent la mediatriu entre 0 i $1+r$ i intersecant-la amb l'eix d'abscisses). Així doncs, per *RC2* obtenim la circumferència de centre $\frac{1+r}{2}$ i radi la distància de 0 a $\frac{1+r}{2}$. Ara, podem traçar la recta perpendicular a l'eix d'abscisses que passi per 1. El punt de tall entre aquesta recta i la circumferència que hem construït l'anomenem x . Pel segon teorema de Tales (Teorema 6.1.4) tenim que el triangle amb vèrtexs 0, x i $1+r$ és un triangle rectangle.

La següent figura mostra la construcció que acabem de descriure:

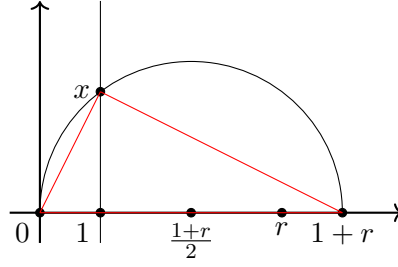


Figura 2.9. Construcció de l'arrel quadrada de r amb regla i compàs.

Pel teorema de l'altura (Teorema 6.1.5) obtenim que: $x^2 = 1 \cdot r$, per tant, $x = \sqrt{r}$. Així doncs, $\sqrt{r} \in \mathcal{C}$.

Ara, com $\sqrt{r} \in \mathcal{C}$, $e^{i\frac{\theta}{2}} \in \mathcal{C}$ i $\mathcal{C}$ és subcòs de $\mathbb{C}$ obtenim que $\sqrt{\alpha} = \sqrt{r} \cdot e^{i\frac{\theta}{2}} \in \mathcal{C}$, tal com volíem veure. $\square$

Teorema 2.3.3. *Sigui $\alpha \in \mathbb{C}$. Aleshores $\alpha \in \mathcal{C}$ si, i només si, existeix una torre de subcossos:*

$$\mathbb{Q} = F_0 \subset F_1 \subset \cdots \subset F_{n-1} \subset F_n \subset \mathbb{C}$$

tal que $\alpha \in F_n$ i $[F_i : F_{i-1}] = 2, \forall i \in \{1, \dots, n\}$.

Demostració. Sigui $\alpha \in \mathbb{C}$. Provem les dues implicacions per separat:

$\Leftarrow$ Suposem que existeixen subcossos:

$$\mathbb{Q} = F_0 \subset F_1 \subset \cdots \subset F_{n-1} \subset F_n \subset \mathbb{C}$$

tals que $\alpha \in F_n$ i $[F_i : F_{i-1}] = 2$, per a $1 \leq i \leq n$. Volem provar que $\alpha \in \mathcal{C}$. Per fer-ho, veurem que $F_n \subset \mathcal{C}$ per inducció.

Comencem veient el cas inicial $F_0 = \mathbb{Q}$. Per ser $\mathcal{C}$ subcòs de $\mathbb{C}$ tenim, directament, que $\mathbb{Q} \subset \mathcal{C}$. Ara, per a $n > 0$, suposem que $F_{n-1} \subset \mathcal{C}$ i volem veure que $F_n \subset \mathcal{C}$. Sabem que $\alpha \in F_n$ i com per hipòtesi $[F_n : F_{n-1}] = 2$ tenim que α és arrel d'un polinomi $f \in \mathcal{C}[X]$ de grau com a màxim 2. Si $\text{gr}(f) = 1$ immediatament tenim que $\alpha \in \mathcal{C}$. Si $\text{gr}(f) = 2$, aleshores, per la fórmula de resolució d'equacions de segon grau podem expressar α en funció d'elements de $\mathcal{C}$ i arrels quadrades d'elements de $\mathcal{C}$. Per tant, pel Teorema 2.3.2 tenim que $\alpha \in \mathcal{C}$, tal com volíem veure.

$\Rightarrow$ Sigui $\alpha = a + ib \in \mathcal{C}$, amb $a, b \in \mathbb{R}$. Veurem que existeix una torre de subcossos:

$$\mathbb{Q} = F_0 \subset \cdots \subset F_{n-1} \subset \mathbb{C} \quad (2.3.1)$$

tal que $[F_i : F_{i-1}] = 2$, per a $1 \leq i \leq n-1$, i F_{n-1} conté la part real i la part imaginària de tots els nombres que cal construir per acabar construint α . Veurem que, aleshores, a, b pertanyen a F_{n-1} o a una extensió quadràtica de F_{n-1} .

A partir d'aquí el teorema quedarà demostrat, ja que si $a, b \in F_{n-1}$ podem agafar $F_n := F_{n-1}(i)$, com $[F_n : F_{n-1}] = [F_{n-1}(i) : F_{n-1}] = \text{gr}(\text{Irr}(i, F_{n-1})) = \text{gr}(X^2 + 1) = 2$ tindrem que existeix una torre de subcossos:

$$\mathbb{Q} = F_0 \subset F_1 \subset \cdots \subset F_{n-1} \subset F_n \subset \mathbb{C}$$

tals que $\alpha = a + ib \in F_n$ i $[F_i : F_{i-1}] = 2$, per a $1 \leq i \leq n$, tal com volem.

També si a i b pertanyen a una extensió quadràtica de F_{n-1} anomenarem F_n a

aquesta extensió i definirem $F_{n+1} := F_n(i)$ i aconseguirem la torre de subcossos desitjada de la mateixa manera.

Farem aquesta demostració aplicant inducció sobre el nombre N de vegades que utilitzem $RC3$, $RC4$ o $RC5$ per a construir α . Si $N = 0$ tenim que $\alpha = 0$ o 1 i, en aquest cas, $F_n = F_0 = \mathbb{Q}$.

Ara, suposem que tenim una torre com (2.3.1) per a $N \leq k-1$, amb $k > 0$, i volem demostrar el cas $N = k$. Per a passar del pas $k-1$ al pas k només podem haver aplicat una de les tres construccions $RC3$, $RC4$ o $RC5$. Estudiarem cada un dels casos per separat:

- Cas $RC3$: Suposem que l'últim pas per a construir α ha estat interseccar dues rectes l_1 i l_2 diferents i no paral·leles. Anomenem α_j i β_j , amb $\alpha_j \neq \beta_j$, als punts a partir dels quals s'ha construït l_j utilitzant $RC1$, per a $j = 1, 2$. Per hipòtesi d'inducció tenim una torre de subcossos com (2.3.1) tal que F_{n-1} conté la part real i imaginària d' α_1 , β_1 , α_2 i β_2 . Veurem que aleshores, en aquest cas, $a, b \in F_{n-1}$.

Suposem que cap de les dues rectes és vertical. Aleshores, per a $j = 1, 2$ definim $y = m_j x + n_j$ com l'equació de la recta l_j . Volem veure que $m_j, n_j \in F_{n-1}$. Posem $\alpha_j = a_j + ib_j$, $\beta_j = c_j + id_j$ on, per hipòtesi, $a_j, b_j, c_j, d_j \in F_{n-1}$. Aleshores, tenim que:

$$m_j = \frac{d_j - b_j}{c_j - a_j}, \text{ per ser el pendent de la recta } l_j.$$

Observem que $a_j \neq c_j$, ja que estem suposant que no tenim rectes verticals. Per tant, $m_j \in F_{n-1}$. Aleshores, ens queda que $n_j = b_j - m_j \cdot a_j \in F_{n-1}$. Per tant, ara podem dir que a i b és solució del sistema:

$$\begin{cases} y = m_1 x + n_1 \\ y = m_2 x + n_2 \end{cases}$$

De fet, com l_1 i l_2 són diferents i no paral·leles, podem assegurar que $m_1 \neq m_2$. Per tant, es tracta d'un sistema amb solució única $x = a$ i $y = b$. Per tant, tenim que:

$$\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} -m_1 & 1 \\ -m_2 & 1 \end{pmatrix}^{-1} \cdot \begin{pmatrix} n_1 \\ n_2 \end{pmatrix} = \frac{1}{m_1 - m_2} \begin{pmatrix} -n_1 + n_2 \\ -m_2 n_1 + m_1 n_2 \end{pmatrix}$$

Per tant, acabem de veure que $a, b \in F_{n-1}$ quan no tenim cap recta vertical.

Ara, sense pèrdua de generalitat, suposem que l_1 és una recta vertical, per tant, $a_1 = c_1$ i l'equació de la recta és $x = a_1$. Com l_1 i l_2 no són paral·leles posem $y = m_2 x + n_2$ l'equació de la recta l_2 , on ja hem vist que $m_2, n_2 \in F_{n-1}$. Aleshores, en aquest cas tenim que a i b és solució del sistema:

$$\begin{cases} x = a_1 \\ y = m_2 x + n_2 \end{cases}$$

Per tant, $a = a_1 \in F_{n-1}$ i $b = m_2 a_1 + n_2 \in F_{n-1}$. I aquest cas queda demostrat.

- Cas $RC4$: Suposem que l'últim pas per a construir α ha estat interseccar una recta l amb una circumferència C . Per una banda, anomenem α_1, β_1 als punts a partir dels quals s'ha construït l . Per altra banda, anomenem $\alpha_2, \beta_2, \gamma_2$ als

punts a partir dels quals, utilitzant $RC2$, s'ha construït C amb centre γ_2 i radi la distància d' α_2 a β_2 .

Per hipòtesi d'inducció tenim una torre de subcossos com (2.3.1) tal que F_{n-1} conté la part real i imaginària d' $\alpha_1, \beta_1, \alpha_2, \beta_2$ i γ_2 . Veurem que, aleshores, $a, b \in F_{n-1}$ o en una extensió quadràtica de F_{n-1} .

Suposem que l no és vertical. Aleshores, com abans, definim $y = m_1x + n_1$ com l'equació de la recta l on, pel que hem vist abans, $m_1, n_1 \in F_{n-1}$. Ara, definim $x^2 + y^2 + m_2x + n_2y + p_2 = 0$ com l'equació de la circumferència C . Volem veure que $m_2, n_2, p_2 \in F_{n-1}$. Posem $\alpha_2 = a_2 + ib_2$, $\beta_2 = c_2 + id_2$ i $\gamma_2 = e_2 + if_2$ on, per hipòtesi, $a_2, b_2, c_2, d_2, e_2, f_2 \in F_{n-1}$. Com C està centrada en γ_2 i té per radi la distància d' α_2 a β_2 , podem escriure l'equació de C com:

$$(x - e_2)^2 + (y - f_2)^2 = \sqrt{(c_2 - a_2)^2 + (d_2 - b_2)^2}^2$$

I manipulant-la obtenim que:

$$x^2 + y^2 - 2e_2x - 2f_2y + e_2^2 + f_2^2 = (c_2 - a_2)^2 + (d_2 - b_2)^2$$

Per tant,

$$m_2 = -2e_2 \in F_{n-1}$$

$$n_2 = -2f_2 \in F_{n-1}$$

$$p_2 = e_2^2 + f_2^2 - (c_2 - a_2)^2 - (d_2 - b_2)^2 \in F_{n-1}$$

Aleshores a i b són solució del següent sistema (tindrà una o dues solucions, ja que l i C s'intersequen):

$$\begin{cases} y = m_1x + n_1 \\ x^2 + y^2 + m_2x + n_2y + p_2 = 0 \end{cases}$$

Que per a solucionar-lo cal resoldre la següent equació de segon grau:

$$x^2 + (m_1x + n_1)^2 + m_2x + n_2 \cdot (m_1x + n_1) + p_2 = 0$$

Per la fórmula de resolució d'equacions quadràtiques, podem expressar x en termes de suma, producte i arrel quadrada de nombres de F_{n-1} . Aleshores, si l'arrel quadrada del discriminant està inclosa en F_{n-1} tindrem que $x \in F_{n-1}$ i, en conseqüència, $y = m_1x + n_1 \in F_{n-1}$. En cas contrari, tindrem que l'arrel quadrada del discriminant, $\sqrt{\Delta}$, estarà inclosa en $F_{n-1}(\sqrt{\Delta})$, que és una extensió quadràtica de F_{n-1} . Per tant, $x \in F_{n-1}(\sqrt{\Delta})$ i, en conseqüència, $y \in F_{n-1}(\sqrt{\Delta})$ també. Així doncs, acabem de veure que, si l no és una recta vertical, $a, b \in F_{n-1}$ o $a, b \in F_{n-1}(\sqrt{\Delta})$.

Ara, suposem que l és una recta vertical, per tant, té equació $x = a_1$. Aleshores, aquesta vegada a i b són solució del sistema:

$$\begin{cases} x = a_1 \\ x^2 + y^2 + m_2x + n_2y + p_2 = 0 \end{cases}$$

Que per a solucionar-lo cal resoldre la següent equació de segon grau:

$$a_1^2 + y^2 + m_2a_1 + n_2y + p_2 = 0$$

I seguint els mateixos arguments que abans tenim que $a, b \in F_{n-1}$ o en una extensió quadràtica de F_{n-1} . I aquest cas queda demostrat.

- Cas RC5: Suposem que l'últim pas per a construir α ha estat intersecar dues circumferències diferents C_1 i C_2 . Anomenem $\alpha_j, \beta_j, \gamma_j$ als punts a partir dels quals s'ha construït C_j amb centre γ_j i radi la distància d' α_j a β_j , per a $j = 1, 2$. Per hipòtesi d'inducció tenim una torre de subcossos com (2.3.1) tal que F_{n-1} conté la part real i imaginària d' $\alpha_1, \beta_1, \gamma_1, \alpha_2, \beta_2$ i γ_2 . Veurem que, aleshores, $a, b \in F_{n-1}$ o en una extensió quadràtica de F_{n-1} . Per a $j = 1, 2$, definim $x^2 + y^2 + m_j x + n_j y + p_j = 0$ l'equació de la circumferència C_j on, pel que hem vist en el cas anterior, $m_j, n_j, p_j \in F_{n-1}$. Aleshores a i b són solució del següent sistema:

$$\begin{cases} x^2 + y^2 + m_1 x + n_1 y + p_1 = 0 \\ x^2 + y^2 + m_2 x + n_2 y + p_2 = 0 \end{cases} \quad (2.3.2)$$

Si restem la segona equació a la primera obtenim:

$$(m_1 - m_2)x + (n_1 - n_2)y + p_1 - p_2 = 0 \quad (2.3.3)$$

Observem que C_1 i C_2 són circumferències diferents i que s'intersequen. Per tant, no poden tenir el mateix centre les dues, és a dir, $\gamma_1 \neq \gamma_2$. Per a $j = 1, 2$, posem $\gamma_j = e_j + if_j$. En el cas anterior hem vist que $m_j = -2e_j$ i $n_j = -2f_j$. Com acabem de dir que $\gamma_1 \neq \gamma_2$ tenim que $(m_1 - m_2)$ i $(n_1 - n_2)$ no es poden anul·lar a la vegada. Per tant, l'equació (2.3.3) ens dona una recta. Aleshores, resoldre el sistema (2.3.2) equival a resoldre:

$$\begin{cases} x^2 + y^2 + m_1 x + n_1 y + p_1 = 0 \\ (m_1 - m_2)x + (n_1 - n_2)y + p_1 - p_2 = 0 \end{cases}$$

Aquest sistema és un sistema com els que hem considerat en el cas anterior. Per tant, podem concloure que $a, b \in F_{n-1}$ o en una extensió quadràtica de F_{n-1} . I aquest cas també queda demostrat. $\square$

Corol·lari 2.3.4. $\mathcal{C}$ és el subcòs més petit de $\mathbb{C}$ tancat respecte a l'operació arrel quadrada.

Demostració. Pel Teorema 2.3.2 sabem que $\mathcal{C}$ és tancat respecte a l'operació arrel quadrada, per tant, només ens queda provar que és el subcòs més petit de $\mathbb{C}$ amb aquesta propietat.

Sigui F un subcòs de $\mathbb{C}$ tancat respecte a l'operació arrel quadrada. Volem veure que $\mathcal{C} \subset F$. Agafem $\alpha \in \mathcal{C}$ qualsevol. Pel Teorema 2.3.3 tenim que existeix una torre de subcossos $\mathbb{Q} = F_0 \subset \dots \subset F_n \subset \mathbb{C}$ tal que $\alpha \in F_n$ i $[F_i : F_{i-1}] = 2$, $\forall i \in \{1, \dots, n\}$. Demostrarem que $F_i \subset F$ per inducció sobre $i \in \{0, \dots, n\}$. Si $i = 0$ tenim que $F_0 = \mathbb{Q} \subset F$ per ser F subcòs de $\mathbb{C}$. Ara, per a $n > 0$, suposem que $F_{n-1} \subset F$ i volem veure que $F_n \subset F$. Com $[F_n : F_{n-1}] = 2$, existeix un element $\beta \in F_{n-1}$ tal que $F_n = F_{n-1}(\sqrt{\beta})$. Aleshores, com $\beta \in F_{n-1} \subset F$ i F és tancat respecte a l'operació arrel quadrada tenim que $\sqrt{\beta} \in F$. Aleshores $F_n = F_{n-1}(\sqrt{\beta}) \subset F$. Per tant, tenim que $\alpha \in F_n \subset F$, és a dir, que $\alpha \in F$. $\square$

Teorema 2.3.5. Sigui $\alpha \in \mathbb{C}$ algebraic sobre $\mathbb{Q}$ i sigui $\mathbb{Q} \subset L$ el cos de descomposició del polinomi irreductible d' α sobre $\mathbb{Q}$. Aleshores, $\alpha \in \mathcal{C}$ si, i només si, $[L : \mathbb{Q}] = 2^a$, per un enter $a \geq 0$.

Demostració. La demostració d'aquest teorema es fa seguint les mateixes idees que utilitzem en la demostració d'un resultat anàleg per a la papiroflèxia (Teorema 5.0.4). També es pot consultar aquesta demostració en les pàgines 263-264 del llibre [2]. $\square$

2.4 Polígons regulars construïbles amb regla i compàs

A partir de la teoria que acabem de desenvolupar, estudiem quins polígons regulars són construïbles amb regla i compàs.

Definició 2.4.1. Considerem un polígon regular de n costats, amb $n > 2$ enter. Sense pèrdua de generalitat el situem amb centre en el 0 i un dels vèrtexs en l'1. Direm que un *polígon regular de n costats és construïble amb regla i compàs* si els seus vèrtexs són punts construïbles amb regla i compàs.

Observació 2.4.2. Observem que els vèrtexs d'un polígon regular de n costats es corresponen amb les potències de l'arrel n -èsima primitiva de la unitat, ζ_n . Per tant, un polígon regular de n costats és construïble amb regla i compàs si, i només si, $\zeta_n \in \mathcal{C}$.

Definició 2.4.3. Un *nombre de Fermat* és un natural de la forma $\mathcal{F}_k := 2^{2^k} + 1$, per un enter $k \geq 0$.

Un *nombre primer de Fermat* és un nombre primer que és de Fermat.

Observació 2.4.4. Els cinc nombres de Fermat més petits són nombres primers de Fermat:

$$\mathcal{F}_0 = 3 \quad \mathcal{F}_1 = 5 \quad \mathcal{F}_2 = 17 \quad \mathcal{F}_3 = 257 \quad \mathcal{F}_4 = 65537$$

De fet, per ara, són els únics nombres primers de Fermat que es coneixen.

Teorema 2.4.5. *Sigui un enter $n > 2$. Un polígon regular de n costats es pot construir amb regla i compàs si, i només si, $n = 2^a p_1 \cdots p_s$, on $a \geq 0$ enter i $p_1, \dots, p_s$ són $s \geq 0$ nombres primers de Fermat diferents.*

Demostració. La demostració d'aquest teorema es fa seguint les mateixes idees que utilitzem en la demostració d'un resultat anàleg per a la papiroflèxia (Teorema 5.1.5). També es pot consultar aquesta demostració en les pàgines 270-271 del llibre [2]. $\square$

Amb aquest teorema queden determinats quins són els polígons regulars construïbles amb regla i compàs. Per tant, podem assegurar que es poden construir triangles equilàters, quadrats, pentàgons, hexàgons, octàgons, decàgons i dodecàgons regulars, entre d'altres. Però, mai podrem construir alguns polígons regulars com l'heptàgon, l'enneàgon, l'hendecàgon o el tridecàgon regular amb regla i compàs.

2.5 Construccions impossibles amb regla i compàs

És sabut que els geòmetres grecs no van saber resoldre alguns problemes com la duplicació del cub, la trisecció de l'angle i la quadratura del cercle. Anem a veure que realment són problemes impossibles de solucionar amb regla i compàs:

- Duplicació del cub: Aquest problema tracta de construir l'aresta d'un cub que tingui volum igual al doble del d'un cub donat.
Considerem que les arestes del cub donat mesuren $x \in \mathbb{R}$, per tant, té volum x^3 . Sense pèrdua de generalitat, considerem que una de les arestes del cub és el segment que va de 0 a x . Per tal de construir un cub amb volum igual al doble del cub

donat, cal construir un cub de volum $2x^3$ que implica construir una aresta que vagi de 0 a $\sqrt[3]{2}x$. Així doncs, aquest cub serà construïble si $\sqrt[3]{2}x$ és construïble. Com x és construïble, només cal veure si $\sqrt[3]{2}$ també ho és.

Definim $\alpha := \sqrt[3]{2}$. Observem que $X^3 - 2$ és el polinomi irreductible de α sobre $\mathbb{Q}$. Al ser irreductible, el cos de descomposició d'aquest polinomi és $\mathbb{Q}(\alpha)$. Per tant, obtenim que

$$[\mathbb{Q}(\alpha) : \mathbb{Q}] = \text{gr}(X^3 - 2) = 3.$$

Per tant, pel Teorema 2.3.5 veiem que α no és construïble amb regla i compàs. Podem concloure que la duplicació del cub és un problema impossible de resoldre amb regla i compàs.

- Trisecció de l'angle: Aquest problema tracta de construir un angle d'amplitud igual a un terç de la d'un angle donat.

Suposem que ens donen l'angle $\frac{2\pi}{3}$ rad. Comencem veient que, efectivament, aquest angle és construïble. Pel Teorema 2.4.5 tenim que un triangle regular és construïble amb regla i compàs, ja que $3 = 2^0 \cdot \mathcal{F}_0 = 1 \cdot 3$, per tant, els seus vèrtexs són construïbles. Així doncs, obtenim que el punt $\zeta_3 = e^{\frac{2\pi}{3}i}$ és construïble. La recta que passa pel 0 i ζ_3 amb l'eix d'abscisses formen exactament un angle de $\frac{2\pi}{3}$ rad.

Trisecar un angle de $\frac{2\pi}{3}$ rad és equivalent a construir un angle de $\frac{2\pi}{9}$ rad. Ara, per l'apartat (a) del Teorema 2.3.2, $\frac{2\pi}{9} \in \mathcal{C}$ si, i només si, $\cos(\frac{2\pi}{9}), \sin(\frac{2\pi}{9}) \in \mathcal{C}$. Anem a veure que $\cos(\frac{2\pi}{9}) \notin \mathcal{C}$.

Tenim la fórmula trigonomètrica $\cos(3\alpha) = 4\cos^3(\alpha) - 3\cos(\alpha)$ (es dedueix a partir de la fórmula de De Moivre). Aplicant-la a $\alpha = \frac{2\pi}{9}$, obtenim:

$$\cos(\frac{2\pi}{3}) = 4\cos^3(\frac{2\pi}{9}) - 3\cos(\frac{2\pi}{9}).$$

Per tant, com $\cos(\frac{2\pi}{3}) = -\frac{1}{2}$, $\cos(\frac{2\pi}{9})$ és arrel del polinomi $8X^3 - 6X + 1$. Però, pel Criteri de Gauss (Teorema 6.2.52) sabem que les úniques possibles arrels racionals d'aquest polinomi són: $\pm 1, \pm \frac{1}{2}, \pm \frac{1}{4}, \pm \frac{1}{8}$. Fàcilment, es pot comprovar que cap d'aquests nombres és arrel de $8X^3 - 6X + 1$, per tant, és un polinomi irreductible sobre $\mathbb{Q}$. Aleshores, obtenim que:

$$[\mathbb{Q}(\cos(\frac{2\pi}{9})) : \mathbb{Q}] = \text{gr}(8X^3 - 6X + 1) = 3.$$

Per tant, pel Teorema 2.3.5, $\cos(\frac{2\pi}{9}) \notin \mathcal{C}$. Acabem de veure que l'angle $\frac{2\pi}{9}$ rad $\notin \mathcal{C}$ i, per tant, amb regla i compàs és impossible trisecar l'angle $\frac{2\pi}{3}$ rad donat inicialment.

- Quadratura del cercle: Aquest problema tracta de construir el costat d'un quadrat amb àrea igual a la d'un cercle donat.

Considerem el cercle amb origen 0 i radi la distància de 0 a 1. L'àrea d'aquest cercle és π . Si volem construir un quadrat amb àrea π cal que els seus costats mesurin $\sqrt{\pi}$, és a dir, cal que $\sqrt{\pi} \in \mathcal{C}$. Pel Teorema 2.3.5, $\sqrt{\pi} \in \mathcal{C}$ si, i només si, $[L : \mathbb{Q}]$ és una potència de 2, on L és el cos de descomposició del polinomi irreductible de $\sqrt{\pi}$ en $\mathbb{Q}$. Però, l'any 1882 Lindemann va demostrar que π és transcendent sobre $\mathbb{Q}$ (Lindemann va publicar la demostració en [6], però per a una demostració més accessible consultar [10]). Per tant, no existeix cap polinomi que tingui $\sqrt{\pi}$ com a arrel. Aleshores, $\sqrt{\pi} \notin \mathcal{C}$. Queda demostrat que la quadratura del cercle és una construcció impossible amb regla i compàs.

3 Primeres construccions amb papiroflèxia

Deixem de banda les construccions amb regle i compàs i dediquem aquest capítol a definir les construccions amb papiroflèxia a la vegada que comencem a explorar el seu potencial. Aquest capítol segueix principalment [1] i la secció 10.3.A del llibre [2].

3.1 Axiomes de la papiroflèxia

De manera similar a les construccions amb regle i compàs, les construccions amb papiroflèxia consisteixen en, donats una sèrie de punts del pla complex $\mathbb{C}$, determinar nous punts a partir de fer plecs amb un full de paper. Un cop fet un plec determinat sempre el desfarem immediatament, és a dir, mai sobreposarem plecs.

Més concretament, fer construccions amb papiroflèxia consisteix en, donats una sèrie de punts, fer plecs i construir nous punts de la següent manera:

- (O1) Donats $\alpha, \beta \in \mathbb{C}$ amb $\alpha \neq \beta$ podem construir la recta l que passa per α i β . Aquesta construcció l'aconseguim fent un plec del paper que passi exactament pels punts α i β .



Figura 3.1. Axioma O1.

- (O2) A partir de dues rectes construïbles (no paral·leles), construïm el seu punt d'intersecció.
- (O3) Donats $\alpha, \beta \in \mathbb{C}$ amb $\alpha \neq \beta$ construïm la mediatriu del segment que connecta α i β . Aquesta construcció l'aconseguim fent un plec que porti el punt α just a sobre del punt β .

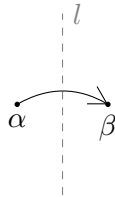


Figura 3.2. Axioma O3.

- (O4) Donat un angle entre dues rectes construïbles r i s (no paral·leles) podem construir la recta l que bisecta aquest angle. Aquesta construcció l'aconseguim fent un plec que faci coincidir les dues rectes.

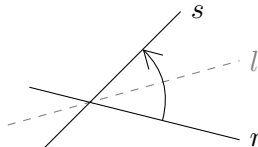


Figura 3.3. Axioma O4.

(O5) Donats $\alpha, \beta \in \mathbb{C}$ amb $\alpha \neq \beta$ i una recta construïble r , sempre que sigui possible, podem construir una recta l que passi per β i faci que el punt simètric d' α respecte l (anomenat α') pertanyi a r . Aquesta construcció l'aconseguim fent un plec que passi per β i porti α sobre algun punt de la recta donada r .

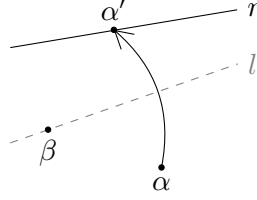


Figura 3.4. Axioma O5.

(O6) Donats $\alpha_1, \alpha_2 \in \mathbb{C}$ amb $\alpha_1 \neq \alpha_2$ i les rectes construïbles r_1 i r_2 , sempre que sigui possible, si tenim un nombre finit de rectes l que fan que el punt simètric d' α_1 respecte l (anomenat α'_1) pertanyi a r_1 a la vegada que el punt simètric d' α_2 respecte l (anomenat α'_2) pertanyi a r_2 , aleshores aquestes rectes l són construïbles. Aquesta construcció l'aconseguim fent un plec que porti α_1 sobre algun punt de r_1 a la vegada que porti α_2 sobre algun punt de r_2 .

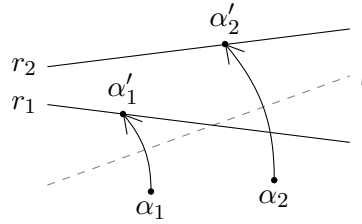


Figura 3.5. Axioma O6.

A aquestes sis construccions les anomenem els *axiomes de la papiroflèxia*. Per a designar aquests axiomes utilitzem la lletra O provinent de la paraula *Origami*.

Definició 3.1.1. Diem que $\alpha \in \mathbb{C}$ és un *nombre construïble amb papiroflèxia* si existeix una seqüència finita de construccions $O1, O2, O3, O4, O5$ i $O6$ que comença amb els punts donats 0 i 1 i acaba amb α .

Definició 3.1.2. Definim $\mathcal{P}$ com el següent conjunt:

$$\mathcal{P} := \{\alpha \in \mathbb{C} \mid \alpha \text{ és construïble amb papiroflèxia}\}$$

i l'anomenem *conjunt dels nombres construïbles amb papiroflèxia*.

Observació 3.1.3. Les construccions dels axiomes $O5$ i $O6$ no són sempre possibles. Veiem un cas on no existeix cap recta l de l'axioma $O6$:

Siguin $\alpha_1 \neq \alpha_2$ punts que no pertanyen a les rectes $r_1 \neq r_2$. Suposem r_1 i r_2 paral·leles. Suposem també que existeix una recta l satisfent $O6$. Anomenem α'_1 i α'_2 , respectivament, als punts simètrics d' α_1 i α_2 respecte l . Per construcció, la distància entre α'_1 i α'_2 és igual a la distància entre α_1 i α_2 . Al ser r_1 i r_2 paral·leles, la mínima distància entre α'_1 i α'_2 és la distància entre r_1 i r_2 . Per tant, si la distància entre α_1 i α_2 és menor que la distància entre r_1 i r_2 , la construcció no és possible.

Per tant, els axiomes $O5$ i $O6$ només els podrem utilitzar en casos on les respectives rectes existeixin.

Observació 3.1.4. L'axioma *O6* especifica que, per tal de construir rectes l cal que n'existixin un nombre finit. Anem a veure la importància d'aquesta condició.

Suposem que $\alpha_1 \in r_1$, $\alpha_2 \in r_2$ i r_1 i r_2 paral·leles. Aleshores qualsevol recta perpendicular a r_1 (que també serà perpendicular a r_2) és una possible recta l , però com hi ha infinites rectes perpendiculars a r_1 aquesta construcció no és possible fer-la utilitzant *O6*. Així doncs, descartem el cas de tenir infinites rectes l , ja que si no, a partir d'aquest exemple que hem donat podríem construir tots els nombres complexos.

Observació 3.1.5. Anem a veure que totes les construccions amb regle i compàs fetes en la secció 2.2 són també possibles amb papiroflèxia:

1. Mediatriu d'un segment: És directament construïble a partir de l'axioma *O3*.
2. Bisectriu d'un angle donat: És directament construïble a partir de l'axioma *O4*.
3. Perpendicular a una recta donada que passa per un punt donat: Anomenem r a la recta donada i β al punt donat. Aquesta construcció és possible aplicant l'axioma *O5* donant com a α un punt qualsevol de la recta r .

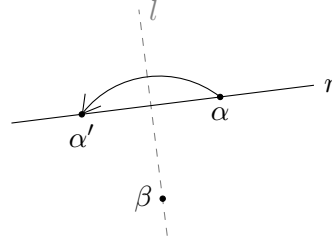


Figura 3.6. Construcció d'una recta perpendicular amb papiroflèxia.

4. La paral·lela a una recta donada que passa per un punt donat: Anomenem r a la recta donada i β al punt donat. Primer de tot construïrem la recta perpendicular a r que passa per β com hem fet en l'exemple anterior, l'anomenarem l . Ara, construïm la recta perpendicular a l que passa per β , de nou utilitzant l'exemple anterior.

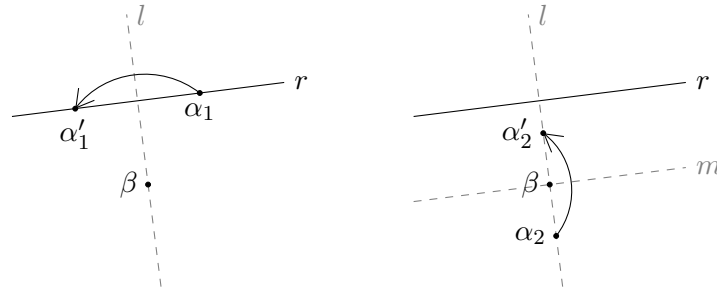


Figura 3.7. Construcció d'una recta paral·lela amb papiroflèxia.

Observació 3.1.6. Seguint l'axioma *O2* un punt és construïble si és intersecció de dues rectes construïbles. Sent rigoroses, en els axiomes *O5* i *O6* els punts α' , α'_1 i α'_2 no els hem construït. Veiem, però que és fàcil construir-los utilitzant la construcció de rectes perpendiculars que hem vist en l'observació anterior. Per exemple, en el cas de l'axioma *O5*, α' és el punt d'intersecció entre la recta donada r i la recta perpendicular a l que passa per α . Anàlogament, podem construir α'_1 i α'_2 de l'axioma *O6*.

3.2 Trisecció de l'angle

Acabem de veure que algunes de les construccions amb regle i compàs també són possibles de construir utilitzant els axiomes de la papiroflèxia. En aquesta secció veurem que una de les construccions impossibles amb regle i compàs sí que és possible construir-la amb papiroflèxia.

Considerem que ens donen un angle $\theta \in [\frac{\pi}{4}, \frac{\pi}{2}]$. Suposarem que és l'angle format per la vora inferior del nostre paper i la recta r_2 tal com indica el dibuix de més a l'esquerra de la Figura 3.8. Anomenem P_1 al punt de tall entre la vora esquerra i la vora inferior del full.

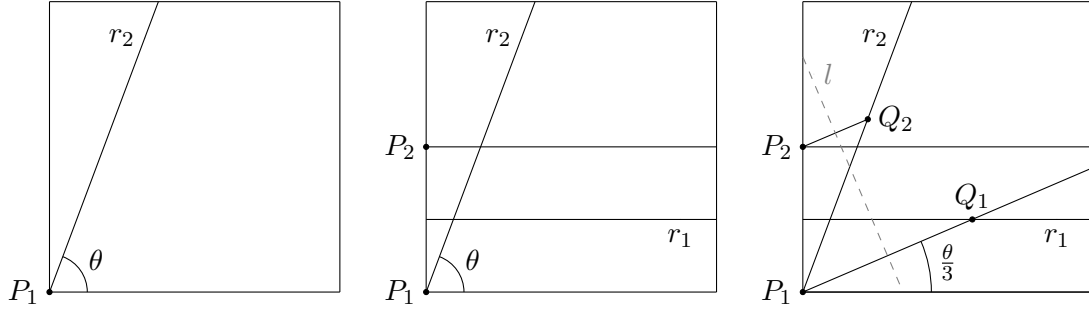


Figura 3.8. Trisecció d'un angle amb papiroflèxia.

Seguint el dibuix del mig construïm dues rectes paral·leles a la vora inferior del paper de tal manera que la recta r_1 sigui equidistant a les altres dues rectes, la que passa per P_1 i la que passa per P_2 .

En darrer lloc, construïm la recta l aplicant l'axioma O6: fent que el punt P_1 vagi a parar sobre la recta r_1 i el punt P_2 sobre la recta r_2 . A partir de l'Observació 3.1.6 construïm els punts simètrics de P_1 i P_2 respecte l i els anomenem Q_1 i Q_2 , respectivament.

Finalment, la recta que passa per P_1 i Q_1 triseca θ .

Proposició 3.2.1. *Donat un angle $\theta \in [\frac{\pi}{4}, \frac{\pi}{2}]$, la construcció que acabem de descriure triseca θ .*

Demostració. Sigui $\theta \in [\frac{\pi}{4}, \frac{\pi}{2}]$ i siguin $P_1, P_2, Q_1, Q_2, r_1, r_2$ i l els descrits en la construcció anterior. Anem a veure que aquesta construcció realment triseca θ .

Primer de tot, anem a veure que si anomenem Q al punt d'intersecció de r_2 amb la recta P_2Q_1 , aleshores també tenim que $Q \in l$.

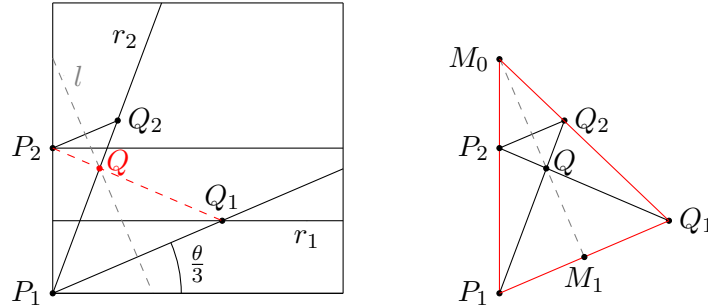


Figura 3.9. Punt Q i triangle $P_1M_0Q_1$.

Per tal de veure que $Q \in l$, primer observem que tenim el triangle $P_1M_0Q_1$, marcat en vermell en la imatge esquerra de la Figura 3.9. Sabem que el punt M_0 (que és el punt de tall de les rectes P_1P_2 , Q_1Q_2 i l) existeix per com hem construït la recta l utilitzant O6. De fet, per aquesta mateixa construcció sabem que la recta l està formada pels punts mitjans entre les rectes P_1P_2 i Q_1Q_2 . Per tant, podem assegurar que el triangle $P_1M_0Q_1$ és isòsceles sent $\overline{P_1M_0} = \overline{Q_1M_0}$. Per tant, tenim les següents igualtats:

$$\overline{P_1P_2} = \overline{Q_1Q_2} \quad \text{i} \quad \overline{P_2M_0} = \overline{Q_2M_0}$$

Hem anomenat M_1 al punt mitjà entre P_1 i Q_1 , per tant, $M_1 \in l$ i $\overline{P_1M_1} = \overline{M_1Q_1}$. Per tant, obtenim que:

$$\frac{\overline{P_1M_1}}{\overline{M_1Q_1}} \cdot \frac{\overline{Q_1Q_2}}{\overline{Q_2M_0}} \cdot \frac{\overline{M_0P_2}}{\overline{P_2P_1}} = \frac{\overline{P_1M_1}}{\overline{P_1M_1}} \cdot \frac{\overline{P_1P_2}}{\overline{P_2M_0}} \cdot \frac{\overline{M_0P_2}}{\overline{P_2P_1}} = 1$$

Aleshores, aplicant el Teorema de Ceva (Teorema 6.1.2) obtenim que qualssevol tres cevianes del nostre triangle $P_1M_0Q_1$ són concurrents. Com P_1Q_2 , P_2Q_1 i el segment de l que va de M_0 a M_1 són cevianes, obtenim que totes tres es tallen en el punt Q . Per tant, queda vist que $Q \in l$.

Passem ara a analitzar diferents angles que apareixen en el nostre full de paper plegat. Anomenem els angles tal com indica la següent figura:

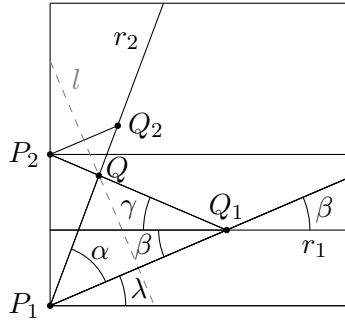


Figura 3.10. Nom dels angles utilitzats durant la trisecció de l'angle amb papiroflèxia.

Clarament, els dos angles que hem anomenat β són congruents. A més a més, com r_1 és paral·lela a la vora inferior del paper, β és congruent a λ . Per tant, obtenim que θ és congruent a $\alpha + \beta$.

Observem que, per una banda, com r_1 és equidistant a les rectes paral·leles a ella que passen per P_1 i P_2 , el triangle $P_1Q_1P_2$ és isòsceles i, per tant, β és congruent a γ . Per altra banda, com $Q \in l$ tenim que el triangle P_1QQ_1 és també isòsceles i, per tant, α és congruent a $\gamma + \beta = 2\beta$. Aleshores, com hem dit que θ és congruent a $\alpha + \beta$ amb el que acabem de veure ens queda que:

$$\theta = \alpha + \beta = 2\beta + \beta = 3\beta. \quad \implies \quad \beta = \frac{\theta}{3}$$

I queda demostrat que la construcció descrita triseca l'angle θ donat inicialment. $\square$

Observació 3.2.2. Per a fer aquesta construcció hem considerat que θ era l'angle format entre la vora inferior del full i la recta r_2 . Agafem la vora inferior del full com una de les rectes que forma aquest angle per a facilitar l'explicació. Però la mateixa construcció es pot fer donat un angle entre dues rectes qualssevol, sempre que l'angle estigui en $[\frac{\pi}{4}, \frac{\pi}{2}]$.

Observació 3.2.3. Acabem d'explicar com trisecar un angle $\theta \in [\frac{\pi}{4}, \frac{\pi}{2}]$. A partir d'aquesta construcció podem trisecar qualsevol angle utilitzant que podem bisecar i doblar angles amb papiroflèxia.

És a dir, sigui $\alpha > \frac{\pi}{4}$, començant per α podem anar bisecant angles tantes vegades com calgui perquè $\frac{\alpha}{2^n} \in [\frac{\pi}{4}, \frac{\pi}{2}]$, sent n el nombre de vegades que bisequem α . Utilitzant les construccions anteriors podem trisecar l'angle $\frac{\alpha}{2^n}$ i, per tant, construir $\frac{\alpha}{3 \cdot 2^n}$. Fent l'angle doble n vegades a partir de $\frac{\alpha}{3 \cdot 2^n}$ obtenim $\frac{\alpha}{3}$.

Anàlogament, donat un angle $\alpha \in (0, \frac{\pi}{4})$ podem fer el mateix procediment, però fent primer angles dobles i després bisecant angles.

En aquesta observació que acabem de fer hem donat per suposat que utilitzant papiroflèxia podem construir l'angle doble d'un angle donat. Però, fins ara, no hem explicat si és o no possible aquesta construcció. Afirmem que sí que és possible construir un angle doble amb papiroflèxia, però veurem la construcció amb detall una mica més endavant.

3.3 Recta tangent a dues paràboles

Passem ara a analitzar amb més detall la geometria que s'amaga darrere dels axiomes O5 i O6. Primer de tot recordem la següent definició:

Definició 3.3.1. Una *paràbola* és el conjunt de punts que equidisten d'una recta r (anomenada *directriu*) i d'un punt fix $F \notin r$ (anomenat *focus*).

Aquesta definició ens dona la següent situació, on P és un punt de la paràbola i $Q \in r$ tal que $\overline{FP} = \overline{QP}$.

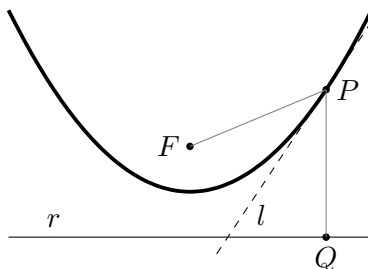


Figura 3.11. Definició d'una paràbola a partir del focus i la directriu.

Ara, volem demostrar el següent resultat:

Lema 3.3.2. *Sigui r una recta i $F \in \mathbb{C}$ un punt tal que $F \notin r$. Sigui l una altra recta donada. Anomenem F' al punt simètric de F respecte l . Aleshores, $F' \in r$ si, i només si, l és tangent a la paràbola amb focus F i directriu r .*

Demostració. Sense pèrdua de generalitat considerem que $F = (0, a)$ i r és la recta $y = -a$, per $a > 0$. Comencem veient quina és l'equació de la paràbola amb focus F i directriu r . Sigui $P = (x_0, y_0)$ un punt de la paràbola. Per tant, P és equidistant de F i d'un punt de la recta r que anomenem $Q = (x_0, -a)$. Aleshores es compleix que:

$$\begin{aligned} \overline{FP} = \overline{PQ} &\implies \sqrt{x_0^2 + (y_0 - a)^2} = \sqrt{0^2 + (y_0 + a)^2} \implies x_0^2 + (y_0 - a)^2 = (y_0 + a)^2 \\ &\implies x_0^2 + y_0^2 - 2ay_0 + a^2 = y_0^2 + 2ay_0 + a^2 \implies x_0^2 = 4ay_0 \end{aligned}$$

Com aquest resultat és cert per a tot punt P de la paràbola, obtenim que l'equació de la paràbola és $y = \frac{1}{4a}x^2$.

Provem, ara, cada una de les implicacions:

⇐ Suposem que l és una recta tangent a la paràbola $y = \frac{1}{4a}x^2$. Volem veure que el $F' \in r$. Primer de tot, observem que l'equació d'aquesta recta tangent a un punt $P = (x_0, y_0)$ de la paràbola és:

$$y = \frac{x_0}{2a}(x - x_0) + \frac{x_0^2}{4a} \implies y = \frac{x_0}{2a}x - \frac{x_0^2}{4a} \quad (3.3.1)$$

Veiem ara que la recta l és perpendicular al segment FQ . El vector director de l és $(2a, x_0)$ i $\vec{FQ} = (x_0 - 0, -a - a) = (x_0, -2a)$. Fem el producte escalar d'aquests dos vectors: $(2a, x_0) \cdot (x_0, -2a) = 2ax_0 - 2ax_0 = 0$. Per tant, queda vist que l és perpendicular a FQ .

Ara, anomenem M al punt mitjà entre F i Q . Tenim que $M = (\frac{x_0}{2}, 0)$. Volem veure que $M \in l$:

$$y = \frac{x_0}{2a} \cdot \frac{x_0}{2} - \frac{x_0^2}{4a} = \frac{x_0^2}{4a} - \frac{x_0^2}{4a} = 0$$

Així doncs, queda vist que $M \in l$ i podem assegurar que Q és el punt simètric de F respecte l , és a dir, $Q = F'$. Per tant, $F' \in r$.

⇒ Suposem ara que $F' \in r$, per tant, $F' = (x_0, -a)$, per a $x_0 \in \mathbb{R}$. Volem veure que l ha de ser tangent a la paràbola $y = \frac{1}{4a}x^2$. Per tal de trobar l'equació de la recta l utilitzarem que el vector director de l ha de ser perpendicular al vector $\vec{FF'}$ i que el punt mitjà entre F i F' , que anomenarem M , ha de ser un punt de l . Per una banda, $\vec{FF'} = (x_0, -2a)$, per tant, el vector director de l és $(2a, x_0)$. Per altra banda, $M = (\frac{x_0}{2}, 0) \in l$. Per tant, la recta l té equació:

$$y = \frac{x_0}{2a}x - \frac{x_0^2}{4a}$$

I aquesta equació és exactament (3.3.1). Per tant, queda vist que l és tangent a la paràbola. □

Aquest resultat que acabem de veure sobre paràboles i rectes tangents es relaciona amb la papiroflèxia de la següent manera:

Observació 3.3.3. Recordem que l'axioma *O5*, donats dos punts diferents α i β i una recta r , construeix una recta l que passa per β i tal que el punt simètric d' α respecte l pertany a r . Si suposem $\alpha \notin r$ podem considerar la paràbola amb focus α i directriu r . Aleshores, pel Lema (3.3.2), l és la recta tangent a aquesta paràbola que passa pel punt β .

Recordem, ara, que l'axioma *O6*, donats dos punts diferents α_1 i α_2 i dues rectes r_1 i r_2 construeix una recta l tal que el punt simètric d' α_1 respecte l pertany a r_1 i el punt simètric d' α_2 respecte l pertany a r_2 . Si suposem que $\alpha_1 \notin r_1$ i $\alpha_2 \notin r_2$, podem considerar les dues paràboles: una amb focus α_1 i directriu r_1 i l'altra amb focus α_2 i directriu r_2 . Per tant, pel Lema (3.3.2) tenim que la recta l és tangent a les dues paràboles a la vegada.

Veiem ara com a partir de tenir una recta tangent a dues paràboles podem trobar solucions a una equació de tercer grau:

Observació 3.3.4. Volem trobar solucions de l'equació de tercer grau $x^3 + ax + b = 0$, on $a, b \in \mathbb{R}$ amb $b \neq 0$. Considerem les següents paràboles:

$$(y - \frac{1}{2}a)^2 = 2bx \quad \text{i} \quad y = \frac{1}{2}x^2 \quad (3.3.2)$$

Sigui l una recta amb pendent m que és tangent a aquestes dues paràboles a la vegada, en els punts (x_1, y_1) i (x_2, y_2) , respectivament. Calculem m utilitzant que és el pendent d'una recta tangent a $(y - \frac{1}{2}a)^2 = 2bx$ en el punt (x_1, y_1) . Per fer-ho, derivem implícitament l'equació d'aquesta paràbola i obtenim:

$$2(y - \frac{1}{2}a)y' = 2b \implies y' = \frac{b}{y - \frac{1}{2}a}$$

Com el pendent de la recta tangent en un punt és el valor de la derivada en aquest punt obtenim que:

$$m = \frac{b}{y_1 - \frac{1}{2}a}$$

Com hem escollit $b \neq 0$, tenim que $m \neq 0$. Observem que $y_1 = \frac{1}{2}a$ quan $x_1 = 0$, en aquest cas la recta l tindria equació $x = 0$, per tant, no seria tangent a l'altra paràbola, així que no tindrem en compte aquest cas. Ara, a partir de $y_1 - \frac{1}{2}a = \frac{b}{m}$, podem escriure x_1 i y_1 en funció de m :

$$\begin{aligned} y_1 &= \frac{b}{m} + \frac{a}{2} \\ x_1 &= \frac{(y_1 - \frac{1}{2}a)^2}{2b} = \frac{(\frac{b}{m})^2}{2b} = \frac{b}{2m^2} \end{aligned}$$

Anàlogament, trobem m utilitzant que és el pendent d'una recta tangent a $y = \frac{1}{2}x^2$ en el punt (x_2, y_2) . Per fer-ho, derivem l'equació d'aquesta paràbola i obtenim que $y' = x$. Per tant, $m = x_2$. Escrivim, ara, x_2 i y_2 en funció de m :

$$\begin{aligned} x_2 &= m \\ y_2 &= \frac{1}{2}m^2 \end{aligned}$$

Observem que una forma alternativa de descriure m és utilitzant el vector que va de (x_1, y_1) a (x_2, y_2) . És a dir, $m = \frac{y_2 - y_1}{x_2 - x_1}$. A partir d'aquesta igualtat obtenim la següent equació:

$$m = \frac{y_2 - y_1}{x_2 - x_1} = \frac{\frac{1}{2}m^2 - (\frac{b}{m} + \frac{a}{2})}{m - \frac{b}{2m^2}} = \frac{m^4 - 2bm - am^2}{2m^3 - b}$$

Per tant, com $m \neq 0$ obtenim:

$$2m^4 - bm = m^4 - 2bm - am^2 \implies m^4 + bm + am^2 = 0 \implies m^3 + am + b = 0$$

Per tant, acabem de veure que els pendents de les rectes tangents a les dues paràboles (3.3.2) a la vegada són solucions d'equacions de tercer grau. Per tant, utilitzant papiroflèxia podem trobar les solucions reals d'equacions de tercer grau.

Observació 3.3.5. Recordem que tota equació de tercer grau, $ax^3 + bx^2 + cx + d = 0$, es pot escriure en la forma reduïda $z^3 + pz + q = 0$ mitjançant el canvi de variable $x = z - \frac{b}{3a}$. Per tant, per l'Observació anterior podem assegurar que amb papiroflèxia podem trobar solucions de qualsevol equació de tercer grau que tingui per coeficients nombres construïts amb papiroflèxia prèviament, sempre i quan aquesta equació tingui solucions reals.

Exemple 3.3.6. Considerem un cas particular de l'Observació 3.3.4 amb $a = 2$ i $b = 1$. Així doncs, ens proposem calcular les solucions reals de l'equació $x^3 + 2x + 1 = 0$ utilitzant papiroflèxia.

Seguint l'Observació 3.3.4, amb $a = 2$ i $b = 1$ tenim les paràboles:

$$(y - 1)^2 = 2x \quad \text{i} \quad y = \frac{1}{2}x^2$$

Fàcilment, obtenim que la primera paràbola té focus $P_1 = (\frac{1}{2}, 1) = \frac{1}{2} + i$ i directriu $x = -\frac{1}{2}$ i la segona té focus $P_2 = (0, \frac{1}{2}) = \frac{1}{2}i$ i directriu $y = -\frac{1}{2}$. Comencem doncs construint aquests punts i rectes.

Donats 0 i 1 aplicant $O1$ obtenim l'eix d'abscisses i, per tant, fent la recta perpendicular a l'eix d'abscisses que passa per 0 obtenim l'eix d'ordenades. Utilitzant $O3$ obtenim la mediatriu entre 0 i 1 i intersecant-la amb l'eix d'abscisses aconseguim el punt $\frac{1}{2}$. Aplicant $O5$ construïm la recta que passa per 0 i envia $\frac{1}{2}$ sobre l'eix d'ordenades. Per tant, podem construir $\frac{1}{2}i$. A partir dels punts $\frac{1}{2}i$ i 1 podem construir el punt P_1 . Anàlogament, es construeix P_2 . Aplicant $O5$ de la mateixa manera es construeixen $-\frac{1}{2}$ i $-\frac{1}{2}i$ i, per tant, aconseguim les dues rectes directrius.

Ara, aplicant $O6$ fent que cada focus vagi a parar a la directriu de la mateixa paràbola podem construir una recta l que és tangent a les dues paràboles a la vegada. Un cop construïda la recta l , per l'Observació 3.3.4, sabem que el seu pendent m és solució de l'equació $x^3 + 2x + 1 = 0$. De fet, en aquest cas concret podem construir una única recta tangent a les dues paràboles, ja que l'equació $x^3 + 2x + 1 = 0$ té una única arrel real (es veu estudiant el creixement de la funció $f(x) = x^3 + 2x + 1$). Per tant, utilitzant aquest mètode només podrem trobar una de les solucions de l'equació $x^3 + 2x + 1 = 0$, ja que el pendent de les rectes és un nombre real.

La següent figura mostra les dues paràboles amb les quals estem treballant (en blau i vermell) i la recta tangent l que acabem de construir (en verd).

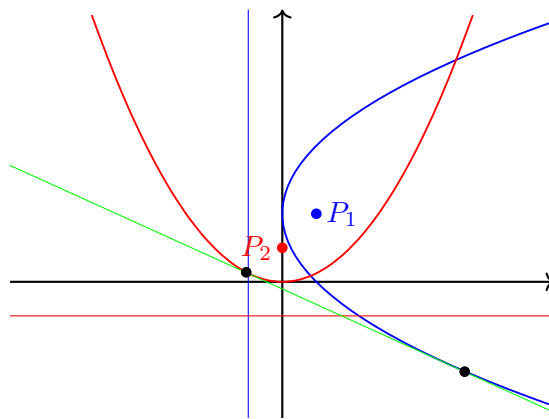


Figura 3.12. La recta tangent a les dues paràboles.

Així doncs, només ens queda construir el punt $(m, 0)$. Per fer-ho suposem que l'equació de la recta l és $y = mx + c$, amb $c \in \mathbb{R}$. Considerem dos punts de l : $A = (0, c)$ i $B = (1, m + c)$ que són fàcilment construïbles utilitzant $O2$ a partir de la recta l i les rectes verticals $x = 0$ i $x = 1$. Ara, podem construir la recta paral·lela a l'eix d'abscisses que passen una per B i l'intersequem amb l'eix d'ordenades construint el punt $C = (0, m + c)$, tal com mostra la següent figura:

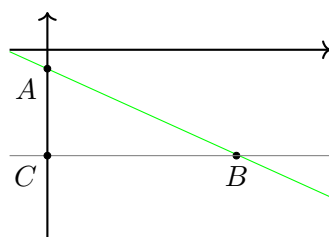


Figura 3.13. Construcció per a trobar el pendent de la recta tangent.

La distància d'A a C és exactament m . Observem que m és negativa, ja que aquesta recta és decreixent. Per tant, l'últim pas que falta és traslladar aquesta distància sobre l'eix d'abscisses, que en ser $m < 0$ quedarà a la part negativa de l'eix. Veurem amb més detall com traslladar distàncies en el següent apartat. Un cop hàgim traslladat aquesta distància ja tindrem construït el punt $(0, m)$ tal com volíem, per tant, haurem construït la solució d'una equació de tercer grau utilitzant només papiroflèxia.

3.4 Translació de distàncies

Aquesta última secció del capítol 3 la dediquem a estudiar les translacions de distàncies amb papiroflèxia, que són una construcció bàsica per a fer altres construccions importants com, per exemple, trobar el punt simètric d'un punt respecte a una recta.

La següent proposició ens mostra com construir aquestes translacions de distàncies.

Proposició 3.4.1. *Donat un segment AB i un punt P que no està alineat amb A i B , podem construir el segment paral·lel i de la mateixa llargada que AB que comença o acaba en el punt P .*

Demostració. Mitjançant $O1$, comencem traçant la recta que passa per P i A i la recta que passa per P i B . Hem construït el triangle APB . Ara, podem construir la recta paral·lela a AB que passa per P i la recta paral·lela a AP que passa per B . En intersecar aquestes dues rectes aconseguim el punt C de tal manera que el segment PC és un segment paral·lel i de la mateixa llargada que AB que comença en el punt P .

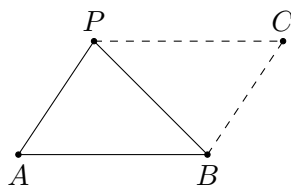


Figura 3.14. Translació de distàncies amb papiroflèxia.

Per a fer la construcció del segment que acaba en el punt P cal construir la recta paral·lela a AB que passa per P , igual que abans, i la recta paral·lela a BP que passa per A . I de la mateixa manera aconseguirem el segment CP que és paral·lel i de la mateixa llargada que AB acabant en el punt P . $\square$

Observació 3.4.2. Sota la notació de la proposició anterior, si P està alineat amb A i B , per a construir un segment paral·lel i de la mateixa llargada que AB que comenci o acabi en P caldrà fer dues translacions. La primera translació mourem el segment AB fins a un punt Q que no estigui alineat a A i B . I tot seguit, tornarem a moure el segment fins al punt P .

A partir de fer translacions amb papiroflèxia podem aconseguir la següent construcció:

Proposició 3.4.3. *Donat un punt P i una recta r tal que $P \notin r$, podem construir el punt simètric a P respecte r .*

Demostració. Comencem construint la recta perpendicular a r que passa per P . Anomenem A al punt d'intersecció d'aquesta recta amb r . Utilitzant l'Observació 3.4.2 podem fer una translació que ens mogui el segment PA a un segment AB . El punt B és el punt simètric a P respecte r .

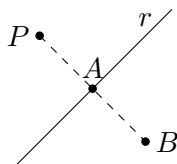


Figura 3.15. Construcció d'un punt simètric respecte a una recta amb papiroflèxia. $\square$

Proposició 3.4.4. *Donades dues rectes diferents r i s , podem construir la recta simètrica a s respecte r .*

Demostració. Siguin A i B dos punts diferents de la recta s . Per la proposició anterior construïm els seus punts simètrics respecte r , els anomenem A' i B' . La recta que passa per A' i B' és exactament la recta simètrica a s respecte r . $\square$

Durant aquest capítol hem deixat dues construccions pendents: calcular l'angle doble i traslladar una distància en l'Exemple 3.3.6. Vegem-les:

- Angle doble: Siguin r i s dues rectes no paral·leles i θ l'angle que formen. Volem construir l'angle 2θ . Utilitzant la Proposició 3.4.4 construïm la recta l que és la recta simètrica a s respecte r . L'angle format entre les rectes s i l és exactament 2θ . Intercanviant els papers de r i s també obtindríem 2θ .
- Exemple 3.3.6: Ens havíem quedat sabent que la distància entre $A = (0, c)$ i $C = (0, m - c)$ era exactament m , amb $m < 0$, per tant, A i C eren dos punts de l'eix d'ordenades negatiu. Volem ara construir el punt $(m, 0)$. Per *O4* podem construir la recta l que biseca l'angle format entre l'eix d'ordenades negatiu i l'eix d'abscisses negatiu, és a dir, l és la recta d'equació $y = x$. Per la Proposició 3.4.3 podem trobar els punts simètrics d' A i C respecte l , els anomenem A' i C' , respectivament. Aleshores, $A' = (c, 0)$ i $C' = (m - c, 0)$. Finalment, per l'Observació 3.4.2 podem aplicar dues translacions i moure el segment $A'C'$ a un segment que acaba al punt $(0, 0)$ i comença al punt $(m, 0)$. Per tant, podem dir que m és construïble.

4 La papiroflèxia equivalent al regle i compàs

Durant la secció 3 hem descrit com fer construccions amb papiroflèxia i hem vist com a partir dels sis axiomes podem fer moltes de les construccions amb regle i compàs i algunes de les construccions impossibles. Per tant, d'alguna manera podem intuir que amb la papiroflèxia podem construir tot el que és construïble amb regle i compàs i molt més. En aquesta secció ens proposem demostrar que aquesta intuïció és certa, és a dir, veurem que tots els nombres construïbles amb regle i compàs són nombres construïbles amb papiroflèxia.

Per a fer aquesta demostració veurem que $\mathcal{C}$, el conjunt dels nombres construïbles amb regle i compàs, és exactament el mateix conjunt que generen els axiomes $O1$, $O2$, $O3$, $O4$ i $O5$. Donem, doncs, les següents definicions:

Definició 4.0.1. Diem que $\alpha \in \mathbb{C}$ és un *número construïble amb els axiomes $O1 - O5$* si existeix una seqüència finita de construccions $O1$, $O2$, $O3$, $O4$ i $O5$ que comença amb els punts donat 0 i 1 i acaba amb α .

Definició 4.0.2. Definim $\mathcal{A}$ com el següent conjunt:

$$\mathcal{A} := \{\alpha \in \mathbb{C} \mid \alpha \text{ és construïble amb els axiomes } O1 - O5\}$$

i l'anomenem *conjunt dels nombres construïbles amb els axiomes $O1 - O5$* .

Així doncs, el que veurem en aquest capítol és que $\mathcal{C} = \mathcal{A}$. Per fer-ho començarem veient que a partir dels axiomes $O1$, $O2$, $O3$, $O4$ i $O5$ també podem definir les operacions suma, multiplicació i arrel quadrada tal com hem fet amb regle i compàs.

Observació 4.0.3. Observem que algunes construccions que hem descrit per a papiroflèxia com la construcció de rectes paral·leles, rectes perpendiculars o la translació de distàncies les hem fet sense utilitzar l'axioma $O6$. Per tant, són construccions que podem continuar utilitzant per a construir nombres en $\mathcal{A}$.

4.1 Suma

Comencem veient com sumar nombres construïbles amb els axiomes $O1 - O5$. Siguin $\alpha, \beta \in \mathcal{A}$, volem veure que aleshores $\alpha + \beta \in \mathcal{A}$. Com $0 \in \mathcal{A}$, utilitzant $O1$ podem construir la recta que passa per 0 i α . En particular, tindrem els segments de 0 a α . Utilitzant la translació de distàncies amb papiroflèxia descrita en la secció 3.4 podem traslladar el segment de 0 a α a un segment paral·lel i de la mateixa distància que comenci al punt β . El punt final d'aquest segment que acabem de construir és exactament el punt $\alpha + \beta$. Podríem obtenir la mateixa construcció agafant el segment que va de 0 a β i traslladant-lo perquè comenci en α .

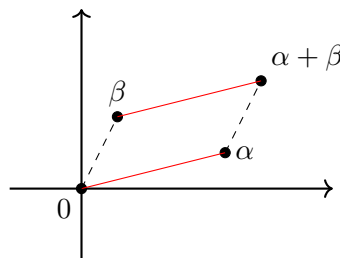


Figura 4.1. Construcció de la suma en $\mathcal{A}$.

Així doncs, queda vist que amb papiroflèxia, utilitzant els axiomes $O1 - O5$ podem construir la suma de nombres construïbles. És a dir, que $\mathcal{A}$ és un conjunt tancat per la suma.

Observem que fent una construcció similar podem construir l'element oposat, és a dir, donat $\alpha \in \mathcal{A}$ podem obtenir $-\alpha \in \mathcal{A}$. Donat que $0 \in \mathcal{A}$ tenim el segment que va de 0 a α . Utilitzant la translació de distàncies amb papiroflèxia dues vegades consecutives podem traslladar el segment de 0 a α a un segment paral·lel i de la mateixa llargada que acabi en 0. El punt d'inici d'aquest segment és exactament $-\alpha$. Per tant, $-\alpha \in \mathcal{A}$.

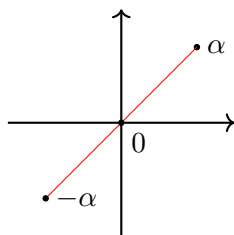


Figura 4.2. Construcció de l'element oposat en $\mathcal{A}$.

Proposició 4.1.1. $\mathcal{A}$ amb la suma és subgrup de $(\mathbb{C}, +)$.

Demostració. Per veure que és subgrup cal provar tres punts:

- $\mathcal{A}$ és un subconjunt no buit de $\mathbb{C}$: Per definició de $\mathcal{A}$ tenim que està inclòs dins de $\mathbb{C}$. Com $0, 1 \in \mathcal{A}$, tenim que $\mathcal{A} \neq \emptyset$.
- Si $\alpha, \beta \in \mathcal{A}$, aleshores $\alpha + \beta \in \mathcal{A}$: Ho hem vist fa un moment.
- $\mathcal{A}$ té estructura de grup amb la suma: Sí que té estructura de grup, ja que compleix les següents propietats:
 - La suma és associativa per ser-ho en $\mathbb{C}$.
 - L'element neutre és $0 \in \mathcal{A}$.
 - L'element oposat d' $\alpha \in \mathcal{A}$ és $-\alpha \in \mathcal{A}$, pel que hem vist fa un moment.

□

4.2 Multiplicació

Passem a veure com multiplicar nombres construïbles amb els axiomes $O1 - O5$. Per fer-ho primer demostrem el següent resultat:

Proposició 4.2.1. Sigui $\alpha = a + ib \in \mathbb{C}$, amb $a, b \in \mathbb{R}$. Aleshores, $\alpha \in \mathcal{A}$ si, i només si, $a, b \in \mathcal{A}$.

Demostració. Veiem les dues implicacions per separat:

⊞ Suposem que $a, b \in \mathcal{A}$. Com tenim que $a, b \in \mathbb{R}$ tindrem que a i b es troben sobre l'eix d'abscisses. El primer pas que hem de fer és transportar b sobre l'eix d'ordenades per tal de construir el punt ib . Una possible manera de fer-ho és aplicant $O5$ per a construir una recta r tal que $0 \in r$ i el punt simètric de b respecte r pertanyi a l'eix d'ordenades (positiu o negatiu segon el signe de b). Tot seguit, podem construir la recta que passa per b i és perpendicular a r . El punt de tall d'aquesta recta amb l'eix d'ordenades és exactament ib . Un cop tenim a i ib podem construir la seva suma tal com hem descrit fa un moment. Per tant, acabem obtenint que $\alpha = a + ib \in \mathcal{A}$.

$\Rightarrow$ Suposem que $\alpha \in \mathcal{A}$. Per una banda, podem construir la recta perpendicular a l'eix d'abscisses que passa per α . La intersecció d'aquesta recta amb l'eix d'abscisses és exactament el punt a . Per l'altra banda, podem construir la recta perpendicular a l'eix d'ordenades que passa per α . La intersecció d'aquesta recta amb l'eix d'ordenades és exactament el punt ib . De la mateixa manera que abans, utilitzant $O5$ podem construir b a partir de ib . Per tant, tenim que $a, b \in \mathcal{A}$ tal com volíem veure. $\square$

Ara, volem veure que si $\alpha, \beta \in \mathcal{A}$, aleshores $\alpha\beta \in \mathcal{A}$. Utilitzarem les mateixes idees que quan ho hem fet per a regla i compàs en la demostració del Teorema 2.3.2. Començarem veient el cas en què $\alpha, \beta \in \mathcal{A} \cap \mathbb{R}$. Si α o β valen 0, aleshores $\alpha\beta = 0 \in \mathcal{A}$. Així doncs, suposem que $\alpha, \beta > 0$. Per ser nombres reals positius tenim que α i β es troben sobre l'eix d'abscisses positiu. Tal com hem fet abans, a partir de β podem construir $i\beta$. De la mateixa manera, a partir de 1 podem construir i . Per $O1$ construïm la recta r que passa per i i per α . Tot seguit, construïm la recta s paral·lela a aquesta que passa per $i\beta$. Pel primer teorema de Tales (Teorema 6.1.3), el punt de tall entre s i l'eix d'abscisses és exactament $\alpha\beta \in \mathcal{A} \cap \mathbb{R}$. Anàlogament, obtenim el mateix resultat per a la resta de casos on el signe d' α o β canvia. Per tant, queda vist que si $\alpha, \beta \in \mathcal{A} \cap \mathbb{R}$, aleshores $\alpha\beta \in \mathcal{A} \cap \mathbb{R}$.

Passem, ara, a veure el cas general per a $\alpha, \beta \in \mathcal{A}$. Posem $\alpha = a + ib$ i $\beta = c + id$, per $a, b, c, d \in \mathbb{R}$. Per la proposició anterior (Proposició 4.2.1) tenim que com $\alpha, \beta \in \mathcal{A}$, aleshores, $a, b, c, d \in \mathcal{A} \cap \mathbb{R}$. Per la definició del producte en els complexos tenim:

$$\alpha\beta = (a + ib)(c + id) = ac - bd + i(ad + bc)$$

Com $a, b, c, d \in \mathcal{A} \cap \mathbb{R}$, pel que acabem de veure tenim que $ac, bd, ad, bc \in \mathcal{A} \cap \mathbb{R}$ i, per ser $(\mathcal{A}, +)$ subgrup de $(\mathbb{C}, +)$ tenim que $ac - bd, ad + bc \in \mathcal{A} \cap \mathbb{R}$. I, de nou, per la proposició anterior (Proposició 4.2.1), com $ac - bd, ad + bc \in \mathcal{A}$ tenim que $\alpha\beta \in \mathcal{A}$.

Així doncs, queda vist que amb papiroflèxia, utilitzant els axiomes $O1 - O5$, podem construir la multiplicació de nombres construïbles. És a dir, que $\mathcal{A}$ és un conjunt tancat per la multiplicació.

Observem que fent una construcció similar podem construir l'element invers, és a dir, donat $\alpha \in \mathcal{A} \setminus \{0\}$ podem construir $\alpha^{-1} \in \mathcal{A}$. Tal com hem fet per a la multiplicació, comencem amb el cas $\alpha \in (\mathcal{A} \setminus \{0\}) \cap \mathbb{R}$. Suposem que $\alpha > 0$. Com hem fet abans, podem construir el punt i i el punt $i\alpha$. Per $O1$ construïm la recta r que passa per $i\alpha$ i 1. Tot seguit, construïm la recta s paral·lela a r que passa per i . Pel Primer teorema de Tales (Teorema 6.1.3), el punt de tall entre s i l'eix d'abscisses és exactament $\alpha^{-1} \in (\mathcal{A} \setminus \{0\}) \cap \mathbb{R}$. Anàlogament, obtenim el mateix resultat per a $\alpha < 0$. Per tant, acabem de veure que si $\alpha \in (\mathcal{A} \setminus \{0\}) \cap \mathbb{R}$, aleshores $\alpha^{-1} \in (\mathcal{A} \setminus \{0\}) \cap \mathbb{R}$.

Veiem, ara, el cas general per a $\alpha \in \mathcal{A} \setminus \{0\}$. Posem $\alpha = a + ib$, amb $a, b \in \mathbb{R}$ tals que no són els dos 0. Per la Proposició 4.2.1, com $\alpha \in \mathcal{A}$ tenim que $a, b \in \mathcal{A}$. Per la definició d'element invers en els complexos tenim:

$$\frac{1}{\alpha} = \frac{1}{a + ib} \cdot \frac{a - ib}{a - ib} = \frac{a - ib}{a^2 + b^2} = a \cdot (a^2 + b^2)^{-1} - i(b \cdot (a^2 + b^2)^{-1})$$

Com $a, b \in \mathcal{A} \cap \mathbb{R}$ tenim que $a^2, b^2 \in \mathcal{A} \cap \mathbb{R}$. Per ser $(\mathcal{A}, +)$ subgrup de $(\mathbb{C}, +)$ i a i b no ser els dos 0, tenim que $a^2 + b^2 \in (\mathcal{A} \setminus \{0\}) \cap \mathbb{R}$. Així doncs, pel que acabem de veure

tenim que $(a^2 + b^2)^{-1} \in (\mathcal{A} \setminus \{0\}) \cap \mathbb{R}$, per tant, $a \cdot (a^2 + b^2)^{-1}, (b \cdot (a^2 + b^2)^{-1}) \in \mathcal{A} \cap \mathbb{R}$. I, finalment, per la Proposició 4.2.1 tenim que $\alpha^{-1} \in \mathcal{A}$.

Proposició 4.2.2. *El conjunt $\mathcal{A}$ és subcòs de $\mathbb{C}$.*

Demostració. Per a provar que $\mathcal{A}$ és subcòs de $\mathbb{C}$ cal veure que $\mathcal{A}$ és subanell de $\mathbb{C}$ i que $\alpha^{-1} \in \mathcal{A}$ per a tot $\alpha \in \mathcal{A} \setminus \{0\}$. La segona condició l'hem demostrada fa un moment. Per tant, només ens queda veure que $\mathcal{A}$ és subanell de $\mathbb{C}$. Per una banda, $(\mathcal{A}, +)$ és subgrup de $(\mathbb{C}, +)$ per la Proposició 4.1.1. Per l'altra banda, $\mathcal{A}$ és tancat respecte al producte de $\mathbb{C}$ pel que hem vist fa un moment.

Així doncs, queda demostrat que $\mathcal{A}$ és subcòs de $\mathbb{C}$. $\square$

4.3 Arrel quadrada

Per acabar, volem veure com construir l'arrel quadrada utilitzant papiroflèxia, és a dir, donat $\alpha \in \mathcal{A}$ volem veure com construir $\sqrt{\alpha}$. Per fer-ho seguirem les construccions donades en les pàgines 10-12 de [1].

Si $\alpha = 0$, aleshores $\sqrt{\alpha} = \sqrt{0} = 0 \in \mathcal{A}$. Suposem, doncs, que $\alpha \neq 0$. Escrivim α en forma polar: $\alpha = r \cdot e^{i\theta}$, amb $r \in \mathbb{R}$ tal que $r = |\alpha| > 0$ i $\theta \in [0, 2\pi)$. Per tant,

$$\sqrt{\alpha} = \sqrt{r \cdot e^{i\theta}} = \sqrt{r} \cdot e^{i\frac{\theta}{2}}$$

Així doncs, per veure que $\sqrt{\alpha} \in \mathcal{A}$ veurem que $\sqrt{r} \in \mathcal{A}$ i $e^{i\frac{\theta}{2}} \in \mathcal{A}$. Per una banda, podem construir $e^{i\frac{\theta}{2}}$ a partir de bisecar $e^{i\theta}$ utilitzant l'axioma O4. Falta construir $\sqrt{r}$.

Sense pèrdua de generalitat, considerem la paràbola K amb focus $F = (0, 1)$ i directriu la recta s d'equació $y = -1$. Primer de tot, observem que $(0, 1)$ és el mateix punt que i , per tant, és construïble. De la mateixa manera que tenim i també podem construir $-i$ i, per tant, construir la recta paral·lela a l'eix d'abscisses que passa per $-i$, que és exactament la recta d'equació $y = -1$. Per tant, el focus i la directriu d'aquesta paràbola són construïbles. Observem també que agafant aquesta paràbola podem reutilitzar part dels càlculs fets durant la demostració del Lema 3.3.2.

Amb focus F i directriu s tenim que K és la paràbola d'equació $y = \frac{1}{4}x^2$. Com hem vist en la secció 3.3, amb l'axioma O5 podem construir la recta l que és tangent a K i passa pel punt $P = (x_0, y_0)$, sempre que aquest punt sigui construïble. L'equació de la recta construïble l és:

$$y = \frac{x_0}{2}x - \frac{x_0^2}{4}$$

Ara, intersecant l amb l'eix d'ordenades i construïm concretament el punt $Q = (0, \frac{-x_0^2}{4})$.

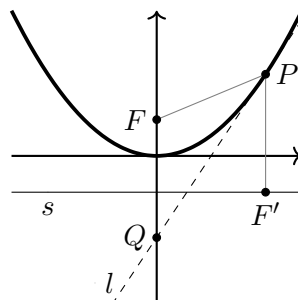


Figura 4.3. Construcció de l'arrel quadrada de r en $\mathcal{A}$.

D'aquesta manera, donada la paràbola K podem aplicar $O5$ per a construir la recta l' que porti F sobre la recta s i passi per Q . I aquesta recta l' és exactament la mateixa recta que l . Per tant, l' també passarà pel punt P . És a dir, si construïm l' podrem construir també el punt simètric de F respecte l' que és F' . Aleshores, podrem construir la recta perpendicular a l'eix d'abscisses que passa per F' i en interseccar-la amb l' obtindrem el punt P .

Amb tot el que acabem de veure ja podem construir $\sqrt{r}$. Agafem $Q = (0, \frac{-r}{4})$, que és un punt construïble per ser r construïble. Aleshores, un cop construïda la recta l' podem obtenir el punt $P = (\sqrt{r}, y_0)$, ja que per la tria de Q que hem fet tenim $x_0^2 = r$, per tant, $x_0 = \sqrt{r}$. Així doncs, acabem de veure que $\sqrt{r} \in \mathcal{A}$. I, en conseqüència, tenim $\sqrt{\alpha} \in \mathcal{A}$. Per tant, $\mathcal{A}$ és un conjunt tancat respecte a l'operació arrel quadrada.

Finalment, veiem que el conjunt dels nombres construïbles amb regla i compàs és exactament el mateix conjunt que generen els axiomes $O1 - O5$.

Teorema 4.3.1. *Tenim la igualtat de conjunts $\mathcal{C} = \mathcal{A}$.*

Demostració. Veurem les dues inclusions per separat:

$\subseteq$ Pel Corol·lari 2.3.4 sabem que $\mathcal{C}$ és el subcòs de més petit de $\mathbb{C}$ tancat respecte a l'operació arrel quadrada. En aquest capítol acabem de veure que $\mathcal{A}$ és subcòs de $\mathbb{C}$ i és tancat respecte a l'operació arrel quadrada. Per tant, queda provat que $\mathcal{C} \subset \mathcal{A}$.

$\supseteq$ Sigui $\alpha = a + ib \in \mathcal{A}$, amb $a, b \in \mathbb{R}$. Volem utilitzar el Teorema 2.3.3 per veure que $\alpha \in \mathcal{C}$, és a dir, veurem que existeix una torre de subcossos:

$$\mathbb{Q} = F_0 \subset F_1 \subset \cdots \subset F_{n-1} \subset F_n \subset \mathbb{C}$$

tal que $\alpha \in F_n$ i $[F_i : F_{i-1}] = 2, \forall i \in \{1, \dots, n\}$.

Per fer-ho seguirem la mateixa estratègia que en la demostració del Teorema 2.3.3, és a dir, veurem que existeix una torre de subcossos:

$$\mathbb{Q} = F_0 \subset \cdots \subset F_{n-1} \subset \mathbb{C} \quad (4.3.1)$$

tal que $[F_i : F_{i-1}] = 2$, per a $1 \leq i \leq n-1$, i F_{n-1} conté la part real i la part imaginària de tots els nombres que cal construir per acabar construint α . Veurem que, aleshores, a i b pertanyen a F_{n-1} o a una extensió quadràtica de F_{n-1} . I a partir d'aquí quedarà el teorema demostrat.

Per fer-ho aplicarem inducció sobre el nombre N de vegades que utilitzem $O2$ per a construir α . Si $N = 0$ tenim que $\alpha = 0$ o 1 i, aleshores, $F_{n-1} = F_0 = \mathbb{Q}$.

Ara, suposem que tenim una torre com (4.3.1) per a $N \leq k-1$, amb $k > 0$, i volem demostrar el cas $N = k$. Per a passar del pas $k-1$ al pas k només podem haver aplicat una vegada l'axioma $O2$ que consisteix en interseccar dues rectes. Si les dues rectes tenen equacions amb coeficients en F_{n-1} o en una extensió quadràtica de F_{n-1} , aleshores seguint les idees utilitzades durant la demostració del cas $RC3$ del Teorema 2.3.3 obtindrem que $a, b \in F_{n-1}$ o en l'extensió quadràtica de F_{n-1} i ja tindrem el teorema demostrat. Així doncs, primer de tot, cal estudiar les equacions de les rectes que podem construir amb els diferents axiomes i veure que en tots els casos les rectes construïbles en $\mathcal{A}$ tenen coeficients en F_{n-1} o en una extensió quadràtica de F_{n-1} :

- Cas O1: Donats $\alpha_1, \beta_1 \in \mathcal{A}$ tal que F_{n-1} conté la part real i imaginària d'aquests dos punts, volem construir la recta l que passa per α_1 i β_1 . Aquesta construcció és idèntica a la construcció feta a partir de $RC1$, per tant, seguint les idees utilitzades durant la demostració del cas $RC3$ del Teorema 2.3.3 tenim que l'equació de la recta l té coeficients en F_{n-1} .
- Cas O3: Donats $\alpha_1, \beta_1 \in \mathcal{A}$ volem construir la mediatriu l del segment que connecta α_1 i β_1 . Posem $\alpha_1 = a_1 + ib_1$ i $\beta_1 = c_1 + id_1$, on per hipòtesi $a_1, b_1, c_1, d_1 \in F_{n-1}$. Definim $m_1x + n_1y + p_1 = 0$ l'equació de la recta l . Com l és la mediatriu del segment que connecta α_1 amb β_1 , el seu vector director és perpendicular al vector $\alpha_1\beta_1$ i ha de passar pel punt mitjà entre α_1 i β_1 . Anomenem γ_1 a aquest punt mitjà, aleshores, $\gamma_1 = \frac{a_1+c_1}{2} + i\frac{b_1+d_1}{2}$. Com $\alpha_1\beta_1 = (c_1 - a_1, d_1 - b_1)$ el vector director de l és $(b_1 - d_1, c_1 - a_1)$. Per tant, l'equació de la recta mediatriu l és:

$$(a_1 - c_1)x + (b_1 - d_1)y + \frac{c_1^2 - a_1^2 + d_1^2 - b_1^2}{2} = 0$$

I queda vist que les coeficients de l pertanyen a F_{n-1} .

- Cas O4: Donades dues rectes r_1 i r_2 volem construir la recta bisectriu l . Observem que per $N = 1$ només podem aplicar $O1$ o $O3$ i ja hem vist que aquestes construccions ens donen rectes amb coeficients en F_{n-1} . Per tant, podem suposar que les equacions de les rectes r_1 i r_2 tenen coeficients en F_{n-1} . Per $j = 1, 2$ posem $m_jx + n_jy + p_j = 0$ l'equació de la recta r_j que, pel que acabem de comentar, tenim $m_j, n_j, p_j \in F_{n-1}$.

La recta bisectriu l és la recta dels punts equidistants a les dues rectes r_1 i r_2 a la vegada. Utilitzant la fórmula de distància de punt a recta, s'ha de satisfer:

$$\frac{|m_1x + n_1y + p_1|}{\sqrt{m_1^2 + n_1^2}} = \frac{|m_2x + n_2y + p_2|}{\sqrt{m_2^2 + n_2^2}}$$

Manipulant aquesta igualtat trobem les equacions de les dues possibles bisectrius entre r_1 i r_2 :

$$\left(\frac{m_1}{\sqrt{m_1^2 + n_1^2}} \pm \frac{m_2}{\sqrt{m_2^2 + n_2^2}}\right)x + \left(\frac{n_1}{\sqrt{m_1^2 + n_1^2}} \pm \frac{n_2}{\sqrt{m_2^2 + n_2^2}}\right)y + \left(\frac{p_1}{\sqrt{m_1^2 + n_1^2}} \pm \frac{p_2}{\sqrt{m_2^2 + n_2^2}}\right) = 0$$

Per tant, les dues possibles equacions de les rectes bisectrius tenen els coeficients en F_{n-1} o en una extensió quadràtica de F_{n-1} .

- Cas O5: Donats $\alpha_1, \beta_1 \in \mathcal{A}$ i una recta r volem construir la l que passa per β_1 i fa que el punt simètric d' α_1 respecte a l pertanyi a r . A partir d'ara, anomenarem α'_1 al punt simètric d' α_1 respecte a l . Posem $\alpha_1 = a_1 + ib_1$ i $\beta_1 = c_1 + id_1$, que per hipòtesi $a_1, b_1, c_1, d_1 \in F_{n-1}$. Definim $m_1x + n_1y + p_1 = 0$ l'equació de la recta r que, com en el cas anterior, tenim que $m_1, n_1, p_1 \in F_{n-1}$. Si $\alpha_1 \in r$ aleshores l és la recta perpendicular a r que passa per β_1 . Aquest cas és molt similar al cas $O3$ i l'ometrem.

Si $\alpha_1 \notin r$, aleshores pel Lema 3.3.2 sabem que l és la recta que passa pel punt β_1 i és tangent a la paràbola amb focus α_1 i directriu r . Anomenem K a aquesta paràbola. Podem trobar l'equació de K imposant que la distància d'un punt de la paràbola a α_1 i a la recta r sigui igual:

$$\sqrt{(a_1 - x)^2 + (b_1 - y)^2} = \frac{|m_1x + n_1y + p_1|}{\sqrt{m_1^2 + n_1^2}}$$

Manipulant aquesta igualtat arribem a l'equació:

$$n_1^2 x^2 - 2m_1 n_1 x y + m_1^2 y^2 - 2(a_1(m_1^2 + n_1^2) + m_1 p_1)x - 2(b_1(m_1^2 + n_1^2) + n_1 p_1)y + (a_1^2 + b_1^2)(m_1^2 + n_1^2) - p_1^2 = 0$$

Per tant, K té una equació amb coeficients en F_{n-1} . A partir d'ara posem $a_2 x^2 + b_2 x y + c_2 y^2 + d_2 x + e_2 y + f_2 = 0$, l'equació de K que, pel que acabem de veure $a_2, b_2, c_2, d_2, e_2, f_2 \in F_{n-1}$.

L'equació de la recta l tangent a aquesta paràbola i que passa pel punt β_1 és:

$$y - d_1 = m(x - c_1)$$

Per a trobar m cal derivar l'equació de K a banda i banda:

$$2a_2 x + b_2 y + b_2 x \frac{dy}{dx} + 2c_2 y \frac{dy}{dx} + d_2 + e_2 \frac{dy}{dx} = 0$$

Aïllant $\frac{dy}{dx}$ tenim que:

$$\frac{dy}{dx}(x, y) = \frac{-(2a_2 x + b_2 y + d_2)}{b_2 x + 2c_2 y + e_2}$$

I acabem trobant m :

$$m = \frac{dy}{dx}(c_1, d_1) = \frac{-(2a_2 c_1 + b_2 d_1 + d_2)}{b_2 c_1 + 2c_2 d_1 + e_2} \in F_{n-1}$$

Per tant, l'equació de la recta l té coeficients en F_{n-1} tal com volíem veure.

Així doncs, podem concloure que $\mathcal{A} = \mathcal{C}$. □

5 El conjunt dels nombres construïbles amb papiroflèxia

Ja hem vist que els primers cinc axiomes de la papiroflèxia construeixen el mateix conjunt de nombres que les construccions amb regla i compàs. En aquest capítol estudiarem quin és el conjunt de nombres que podem construir afegint el sisè axioma. També demostrarem alguns teoremes i proposicions rellevants de les construccions amb papiroflèxia i els compararem amb els resultats anàlegs per a regla i compàs. Aquest capítol segueix la secció 10.3.B del llibre [2].

Comencem donant les següents definicions:

Definició 5.0.1. Diem que $\alpha \in \mathbb{C}$ és un *nombre construïble amb regla i compàs i papiroflèxia* si existeix una seqüència finita de construccions $RC1$, $RC2$, $RC3$, $RC4$, $RC5$ i $O6$ que comença amb els punts donats 0 i 1 i acaba amb α .

Definició 5.0.2. Definim $\mathcal{O}$ com el següent conjunt:

$$\mathcal{O} := \{\alpha \in \mathbb{C} \mid \alpha \text{ és un nombre construïble amb regla i compàs i papiroflèxia}\} \quad (5.0.1)$$

i l'anomenem *conjunt dels nombres construïbles amb regla i compàs i papiroflèxia*.

Observació 5.0.3. Fins ara teníem definits els conjunts $\mathcal{C}$, el conjunt dels nombres construïbles amb regla i compàs, $\mathcal{A}$, el conjunt dels nombres construïbles amb els axiomes $O1 - O5$, i $\mathcal{P}$, el conjunt dels nombres construïbles amb papiroflèxia.

En el capítol anterior hem demostrat que $\mathcal{C} = \mathcal{A}$, per tant, queda clar que afegint l'axioma $O6$ tenim que $\mathcal{O} = \mathcal{P}$.

En tot aquest apartat, utilitzarem el conjunt $\mathcal{O}$ en comptes de $\mathcal{P}$ per a demostrar aquests teoremes i proposicions que comentàvem. Escollir $\mathcal{O}$ ens permet utilitzar resultats ja vistos per al conjunt $\mathcal{C}$.

Teorema 5.0.4. *El conjunt $\mathcal{O}$ és subcòs de $\mathbb{C}$. A més a més,*

(a) *Segui $\alpha = a + bi$ amb $a, b \in \mathbb{R}$. Aleshores $\alpha \in \mathcal{O}$ si, i només si, $a, b \in \mathcal{O}$.*

(b) *$\alpha \in \mathcal{O}$ implica que $\sqrt{\alpha}, \sqrt[3]{\alpha} \in \mathcal{O}$.*

(c) *Segui $\alpha \in \mathbb{C}$. Aleshores, $\alpha \in \mathcal{O}$ si, i només si, existeixen subcossos:*

$$\mathbb{Q} = F_0 \subset F_1 \subset \cdots \subset F_{n-1} \subset F_n \subset \mathbb{C} \quad (5.0.2)$$

tals que $\alpha \in F_n$ i $[F_i : F_{i-1}] = 2$ o 3 , per a $1 \leq i \leq n$.

Demostració. En el Teorema 2.3.2 hem vist que $\mathcal{C}$ és subcòs de $\mathbb{C}$. Observem que les construccions en $\mathcal{C}$ també les podem fer en $\mathcal{O}$, per tant, podem construir la suma i el producte de la mateixa manera. Així doncs, seguint les idees del Teorema 2.3.2 es demostra que $\mathcal{O}$ és subcòs de $\mathbb{C}$. Pels mateixos motius i seguint la demostració del mateix teorema es proven l'apartat (a) i la primera part de l'apartat (b). Demostrem, doncs, la resta d'apartats.

(b) Falta veure que $\sqrt[3]{\alpha} \in \mathcal{O}$. Primer de tot escrivim α en forma polar: $\alpha = r \cdot e^{i\theta}$, amb $r \in \mathbb{R}$ tal que $r = |\alpha| > 0$ i $\theta \in [0, 2\pi)$. Per tant,

$$\sqrt[3]{\alpha} = \sqrt[3]{r \cdot e^{i\theta}} = \sqrt[3]{r} \cdot e^{i\frac{\theta}{3}}$$

Així doncs, per veure que $\sqrt[3]{\alpha} \in \mathcal{O}$ veurem que $\sqrt[3]{r} \in \mathcal{O}$ i $e^{i\frac{\theta}{3}} \in \mathcal{O}$:

- $e^{i\frac{\theta}{3}} \in \mathcal{O}$: Per *RC1* podem traçar la recta que passa per 0 i α . Aquesta recta amb l'eix d'abscisses generen l'angle θ . Com hem explicat en l'apartat 3.2 podem trisecar l'angle θ (observem que amb regla i compàs i l'axioma *O6* podem fer exactament la mateixa construcció). Així doncs, obtenim que $\frac{\theta}{3} \in \mathcal{O}$. Ara, per *RC2* construïm la circumferència amb centre 0 i radi 1. Per *RC4*, en intersecar aquesta circumferència amb la recta que triseca θ obtenim que $e^{i\frac{\theta}{3}} \in \mathcal{O}$.
- $\sqrt[3]{r} \in \mathcal{O}$: Considerem les paràboles de l'Observació 3.3.4 amb $a = 0$ i $b = -r$:

$$y^2 = -2rx \quad \text{i} \quad y = \frac{1}{2}x^2$$

La primera paràbola té focus $(-\frac{r}{2}, 0)$ i directriu $x = \frac{r}{2}$ i la segona paràbola té focus $(0, \frac{1}{2})$ i directriu $y = -\frac{1}{2}$. Per tant, com r és construïble podem construir el focus i la directriu de les dues paràboles utilitzant, simplement, regla i compàs. Ara, aplicant *O6* obtenim una recta l amb pendent m que és tangent a les dues paràboles a la vegada. De nou, per l'Observació 3.3.4 sabem que m és solució de l'equació $x^3 - r = 0$. Per tant, $m = \sqrt[3]{r}$. Com m és construïble amb regla i compàs (utilitzant l'anàleg del procediment fet en l'Exemple 3.3.6 per a papiroflèxia), queda vist que $\sqrt[3]{r} \in \mathcal{O}$.

Ara, com $\sqrt[3]{r} \in \mathcal{O}$, $e^{i\frac{\pi}{3}} \in \mathcal{O}$ i $\mathcal{O}$ és subcòs de $\mathbb{C}$ obtenim que $\sqrt[3]{\alpha} = \sqrt[3]{r} \cdot e^{i\frac{\pi}{3}} \in \mathcal{O}$, tal com volíem veure.

(c) Sigui $\alpha \in \mathbb{C}$. Demostrem les dues implicacions per separat:

⇐ Suposem que existeixen subcossos

$$\mathbb{Q} = F_0 \subset F_1 \subset \cdots \subset F_{n-1} \subset F_n \subset \mathbb{C}$$

tals que $\alpha \in F_n$ i $[F_i : F_{i-1}] = 2$ o 3 , per a $1 \leq i \leq n$. Volem provar que $\alpha \in \mathcal{O}$. Per fer-ho, veurem que $F_n \subset \mathcal{O}$ per inducció.

Comencem veient el cas inicial $F_0 = \mathbb{Q}$. Per ser $\mathcal{O}$ subcòs de $\mathbb{C}$ tenim, directament, que $\mathbb{Q} \subset \mathcal{O}$. Suposem ara que $F_{n-1} \subset \mathcal{O}$ i volem veure que $F_n \subset \mathcal{O}$. Sabem que $\alpha \in F_n$ i com per hipòtesi $[F_n : F_{n-1}] = 2$ o 3 tenim que α és arrel d'un polinomi $f \in \mathcal{O}[X]$ de grau com a màxim 3. Si $gr(f) = 1$ immediatament tenim que $\alpha \in \mathcal{O}$. Si $gr(f) = 2$ o 3 , aleshores, per la fórmula de Cardano per a resoldre equacions de tercer grau o per la fórmula de resolució d'equacions de segon grau tenim que podem expressar α en funció d'arrels quadrades, arrels cúbiques i elements de $\mathcal{O}$. Per tant, pels apartats (a) i (b) d'aquest mateix teorema tenim que $\alpha \in \mathcal{O}$, tal com volíem veure.

⇒ Sigui $\alpha = a + ib \in \mathcal{O}$, amb $a, b \in \mathbb{R}$. Seguirem la mateixa estratègia que en el Teorema 2.3.3, veurem que existeix una torre de subcossos:

$$\mathbb{Q} = F_0 \subset \cdots \subset F_{n-1} \subset \mathbb{C} \tag{5.0.3}$$

tal que $[F_i : F_{i-1}] = 2$ o 3 , per a $1 \leq i \leq n-1$, i F_{n-1} conté la part real i la part imaginària de tots els nombres que cal construir per acabar construint α . Veurem que, aleshores, a i b pertanyen a F_{n-1} o a una extensió de F_{n-1} de màxim grau 3. I a partir d'aquí quedarà el teorema demostrat.

Per fer-ho aplicarem inducció sobre el nombre N de vegades que utilitzem *RC3*, *RC4* o *RC5* per a construir α . Si $N = 0$ tenim que $\alpha = 0$ o 1 i, aleshores, $F_n = F_0 = \mathbb{Q}$.

Ara, suposem que tenim una torre com (5.0.3) per a $N \leq k - 1$, amb $k > 0$, i volem demostrar el cas $N = k$. Per a passar del pas $k - 1$ al pas k només podem haver aplicat una de les tres construccions *RC3*, *RC4* o *RC5*. Estudiarem cada un dels casos per separat:

- Cas *RC3*: Suposem que l'últim pas per a construir α ha estat interseccar dues rectes l_1 i l_2 diferents i no paral·leles. Si les dues rectes han estat construïdes utilitzant *RC1* ja ho tenim demostrat en el Teorema 2.3.3.

Suposem que l_1 s'ha construït a partir d'*O6*. Aleshores, pel que hem vist en la secció 3.3, l_1 és tangent a dues paràboles a la vegada, on el focus i la directriu de cada una d'elles ha sigut construïda prèviament. Volem veure que l'equació de la recta l_1 té coeficients que pertanyen a F_{n-1} o a una extensió de F_{n-1} de grau màxim 3.

Considerem el cas particular de l'Observació 3.3.4 amb les paràboles:

$$(y - \frac{1}{2}a_1)^2 = 2b_1x \quad \text{i} \quad y = \frac{1}{2}x^2 \quad (5.0.4)$$

amb $a_1, b_1 \in \mathbb{R}$ tal que $b_1 \neq 0$. A aquestes paràboles les anomenem K_1 i L_1 , respectivament. Tenim que K_1 té focus $\gamma_1 = \frac{1}{2}b_1 + i\frac{1}{2}a_1$ i directriu $x = \frac{-1}{2}b_1$ i L_1 té focus $\delta_1 = i\frac{1}{2}$ i directriu $y = \frac{-1}{2}$. Per hipòtesi tenim que F_{n-1} conté la part real i la imaginària de γ_1, δ_1 i dels punts que han calgut per construir les directrius. En particular, tenim que $a_1, b_1 \in F_{n-1}$.

Per la mateixa Observació 3.3.4 sabem que el pendent m_1 de la recta l_1 és solució de l'equació $x^3 + ax + b = 0$, per tant, m_1 pertany a F_{n-1} o a una extensió de F_{n-1} de grau màxim 3. Posem F_n a aquesta extensió i tenim $a_1, b_1, m_1 \in F_n$.

Anomenem α_1 al punt de tangència de l_1 amb K_1 i β_1 al punt de tangència de l_1 amb L_1 . Aleshores, de nou per l'Observació 3.3.4, tenim que aquests punts de tangència són:

$$\alpha_1 = \frac{b_1}{2m_1^2} + i \cdot \left(\frac{b_1}{m_1} + \frac{a_1}{2} \right)$$

$$\beta_1 = m_1 + i \cdot \frac{m_1^2}{2}$$

Per tant, la part real i imaginària d' α_1 i β_1 pertanyen a F_n . Per tant, pel que hem vist en la demostració del cas *RC3* del Teorema 2.3.3, podem dir que l'equació de la recta l_1 té coeficients en F_n .

Si en comptes de les paràboles (5.0.4) tenim dues paràboles qualssevol, utilitzant arguments similars arribem a les mateixes conclusions.

Aleshores, tant si l_1 i l_2 totes dues han estat construïdes amb *O6* o només una d'elles, tenim que els coeficients de les respectives equacions pertanyen a F_{n-1} o a una extensió de F_{n-1} de màxim grau 3. Com a i b són la solució del sistema que formen les equacions d'aquestes dues rectes, seguint la demostració del cas *RC3* del Teorema 2.3.3 obtenim que $a, b \in F_{n-1}$ o en una extensió de F_{n-1} de màxim grau 3. I aquest cas queda demostrat.

- Cas *RC4*: Suposem que l'últim pas per a construir α ha estat interseccar una recta l amb una circumferència C . Pel que acabem de veure, tant si

l ha estat construïda utilitzant *RC1* o *O6* tenim que els coeficients de la seva equació pertanyen a F_{n-1} o a una extensió de F_{n-1} de grau màxim 3. Per tant, seguint la demostració del cas *RC4* del Teorema 2.3.3 aquest cas queda demostrat.

- Cas *RC5*: Aquest cas és idèntic al cas *RC5* del Teorema 2.3.3. □

Teorema 5.0.5. *Sigui $\alpha \in \mathbb{C}$ algebraic sobre $\mathbb{Q}$ i sigui $\mathbb{Q} \subset L$ el cos de descomposició del polinomi irreductible de α sobre $\mathbb{Q}$. Aleshores, $\alpha \in \mathcal{O}$ si, i només si, $[L : \mathbb{Q}] = 2^a 3^b$, per enters $a, b \geq 0$.*

Demostració. Posem $f := \text{Irr}(\alpha, \mathbb{Q})$. Provem cada una de les implicacions:

⊆ Suposem que $[L : \mathbb{Q}] = 2^a 3^b$, per enters $a, b \geq 0$.

Primer de tot, observem que per hipòtesi tenim que l'extensió $L/\mathbb{Q}$ és finita. Ara, per la Proposició 6.2.32 es té que $L/\mathbb{Q}$ és normal, ja que L és el cos de descomposició de $f \in \mathbb{Q}[X]$.

Per altra banda, com $f \in \mathbb{Q}[X]$ és irreductible sobre $\mathbb{Q}$ i $\text{car}(\mathbb{Q}) = 0$, per la Proposició 6.2.37, f és separable. Per tant, com $L = \mathbb{Q}(\alpha, \alpha_1, \dots, \alpha_n)$ (on $\alpha_1, \dots, \alpha_n$ són les arrels de f diferents de α), tenim que $\alpha, \alpha_1, \dots, \alpha_n$ són separables sobre $\mathbb{Q}$. I així obtenim que $L/\mathbb{Q}$ és separable.

Com $L/\mathbb{Q}$ és normal i separable podem dir que $L/\mathbb{Q}$ és una extensió de Galois. I pel Teorema fonamental de la teoria de Galois (Teorema 6.2.43) tenim doncs que:

$$|\text{Gal}(L/\mathbb{Q})| = [L : \mathbb{Q}] = 2^a 3^b \quad (5.0.5)$$

Ara, pel Teorema 6.2.6 tenim que $\text{Gal}(L/\mathbb{Q})$ és un grup resoluble. És a dir, existeix una cadena finita de subgrups

$$\{e\} = G_0 \subset G_1 \subset \dots \subset G_n = \text{Gal}(L/\mathbb{Q})$$

tals que, per a $i = 0, \dots, n-1$, G_i és normal en G_{i+1} i $[G_{i+1} : G_i]$ és primer. Per tant, $[G_{i+1} : G_i] = 2$ o 3 . Aleshores, per les correspondències de Galois tenim una torre:

$$\mathbb{Q} = L^{\text{Gal}(L/\mathbb{Q})} = L^{G_n} \subset L^{G_{n-1}} \subset \dots \subset L^{G_1} \subset L^{G_0} = L^{\{e\}} = L \subset \mathbb{C} \quad (5.0.6)$$

amb $[L^{G_{i-1}} : L^{G_i}] = 2$ o 3 . I com $\alpha \in L$, pel Teorema 5.0.4 tenim que $\alpha \in \mathcal{O}$.

⇒ Suposem que $\alpha \in \mathcal{O}$.

Per començar, volem veure que $\mathcal{O}/\mathbb{Q}$ és una extensió normal. Per fer-ho veurem que f descompon totalment sobre $\mathcal{O}$. Com $\alpha \in \mathcal{O}$, pel Teorema 5.0.4 tenim que existeixen subcossos:

$$\mathbb{Q} = F_0 \subset F_1 \subset \dots \subset F_{n-1} \subset F_n \subset \mathbb{C} \quad (5.0.7)$$

tals que $\alpha \in F_n$ i $[F_i : F_{i-1}] = 2$ o 3 , $\forall i = 1, \dots, n$.

Aleshores, tenim que l'extensió $F_n/\mathbb{Q}$ és finita. Per ser finita, també sabem que és una extensió algebraica i com, a més a més, $\text{car}(\mathbb{Q}) = 0$, per la Proposició 6.2.37 tenim que $F_n/\mathbb{Q}$ és separable.

Per tant, per la Proposició 6.2.44 sabem que existeix un cos M que és clausura de Galois de $F_n/\mathbb{Q}$. És a dir, que $F_n \subset M$ i $M/\mathbb{Q}$ és de Galois.

A més a més, pel Teorema Fonamental de l'Àlgebra sabem que $\mathbb{C}$ és algebraicament

tancat i, per tant, $M \subset \mathbb{C}$.

Com $M/\mathbb{Q}$ és de Galois, per definició sabem que $M/\mathbb{Q}$ és normal i separable. Per ser normal, obtenim que f descompon totalment en M , ja que f és irreductible sobre $\mathbb{Q}$ i α , que és arrel de f , està en M . Sigui doncs $\beta \in M$ una arrel de f . Pel Corol·lari 6.2.33 tenim que existeix $\sigma \in \text{Gal}(M/\mathbb{Q})$ tal que $\sigma(\alpha) = \beta$. Aplicant σ a (5.0.7) obtenim:

$$\mathbb{Q} = \sigma(\mathbb{Q}) = \sigma(F_0) \subset \sigma(F_1) \subset \cdots \subset \sigma(F_{n-1}) \subset \sigma(F_n) \subset \mathbb{C} \quad (5.0.8)$$

amb $[\sigma(F_i) : \sigma(F_{i-1})] = [F_i : F_{i-1}] = 2$ o 3 , $\forall i = 1, \dots, n$.

Com $\beta = \sigma(\alpha) \in \sigma(F_n)$ pel Teorema 5.0.4 tenim que $\beta \in \mathcal{O}$. Així doncs, acabem de veure que f descompon totalment sobre $\mathcal{O}$ i, per tant, per la Proposició 6.2.32 $\mathcal{O}/\mathbb{Q}$ és una extensió normal.

Com f descompon totalment sobre $\mathcal{O}$, aleshores $\mathcal{O}$ conté un cos de descomposició de f sobre $\mathbb{Q}$ que, per unicitat del cos de descomposició (Proposició 6.2.30), ha de ser L . Per tant, $L \subset \mathcal{O}$.

Observem que $L/\mathbb{Q}$ és una extensió finita. Per ser finita, també sabem que és una extensió algebraica i com, a més a més, $\text{car}(\mathbb{Q}) = 0$, per la Proposició 6.2.37 tenim que $L/\mathbb{Q}$ és separable.

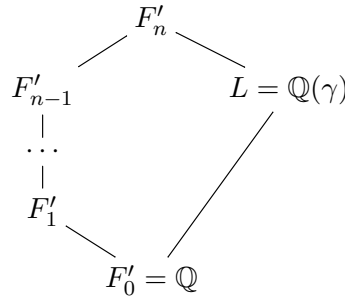
Ara, com $\mathbb{Q}$ és infinit i $L/\mathbb{Q}$ és finita i separable, pel Teorema de l'element primitiu (Teorema 6.2.39) existeix $\gamma \in L$ tal que $L = \mathbb{Q}(\gamma)$.

Si $\gamma \in L$, també tenim que $\gamma \in \mathcal{O}$. Pel Teorema 5.0.4 existeixen subcossos:

$$\mathbb{Q} = F'_0 \subset F'_1 \subset \cdots \subset F'_{n-1} \subset F'_n \subset \mathbb{C} \quad (5.0.9)$$

tals que $\gamma \in F'_n$ i $[F'_i : F'_{i-1}] = 2$ o 3 , $\forall i = 1, \dots, n$.

Com $\gamma \in F'_n$ i, recordem, $L = \mathbb{Q}(\gamma)$, aleshores $\gamma \in L \subset F'_n$, tenim el següent diagrama:



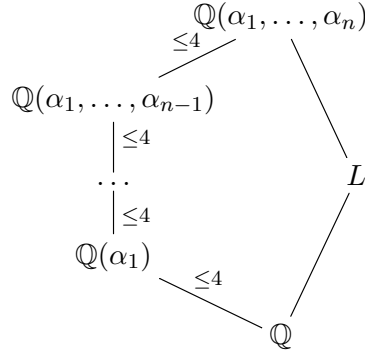
I com $[F'_i : F'_{i-1}] = 2$ o 3 , $\forall i = 1, \dots, n$ tenim que $[F'_n : \mathbb{Q}] = 2^{a'} 3^{b'}$, per enters $a', b' \geq 0$. I, per tant, per la fórmula de graus (Proposició 6.2.15) $[L : \mathbb{Q}] = 2^a 3^b$, per enters $a, b \geq 0$. $\square$

Corol·lari 5.0.6. *Sigui $f(x) \in \mathbb{Q}[X]$ un polinomi tal que $\text{gr}(f) \leq 4$. Aleshores les arrels de $f(x)$ pertanyen a $\mathcal{O}$, és a dir, podem resoldre $f(x) = 0$ amb papiroflèxia.*

Demostració. Siguin $\alpha_1, \dots, \alpha_n$ les arrels de f , amb $n \leq 4$. Sigui α_1 una de les arrels de f . Per definició de polinomi irreductible tenim que f ha de ser múltiple de $\text{Irr}(\alpha_1, \mathbb{Q})$. Aleshores, $[\mathbb{Q}(\alpha_1) : \mathbb{Q}] = \text{gr}(\text{Irr}(\alpha_1, \mathbb{Q})) \leq \text{gr}(f) \leq 4$. De la mateixa manera, si $n \neq 1$, com f també compleix que $f \in \mathbb{Q}(\alpha_1)[X]$ i $f(\alpha_2) = 0$, aleshores $[\mathbb{Q}(\alpha_1, \alpha_2) : \mathbb{Q}(\alpha_1)] = \text{gr}(\text{Irr}(\alpha_2, \mathbb{Q}(\alpha_1))) \leq \text{gr}(f) \leq 4$. És a dir, de forma general obtenim que:

$$[\mathbb{Q}(\alpha_1, \dots, \alpha_n) : \mathbb{Q}(\alpha_1, \dots, \alpha_{n-1})] = \text{gr}(\text{Irr}(\alpha_n, \mathbb{Q}(\alpha_1, \dots, \alpha_{n-1}))) \leq \text{gr}(f) \leq 4$$

Observem també que $\mathbb{Q}(\alpha_1, \dots, \alpha_n)$ és cos de descomposició de f sobre $\mathbb{Q}$. Si L és el cos de descomposició de $\text{Irr}(\alpha_1, \mathbb{Q})$ en $\mathbb{Q}$, aleshores $L \subset \mathbb{Q}(\alpha_1, \dots, \alpha_n)$. Per tant, tenim la següent torre de cossos:



Per tant, per la fórmula de graus (Proposició 6.2.15), $[L : \mathbb{Q}] = 2^a 3^b$ per enters $a, b \geq 0$. I pel Teorema 5.0.5, $\alpha_1 \in \mathcal{O}$. Com hem triat α_1 una arrel arbitrària de f queda provat que les arrels de f pertanyen a $\mathcal{O}$. $\square$

5.1 Polígons regulars construïbles amb papiroflèxia

En la secció 2.4 hem estudiat quins polígons regulars podem construir amb regle i compàs. Ara ens proposem fer l'estudi anàleg per a construccions amb papiroflèxia. Tot i que parlem de construccions amb papiroflèxia, encara treballarem amb el conjunt $\mathcal{O}$ dels nombres construïbles amb regle i compàs i papiroflèxia.

Comencem donant la següent definició:

Definició 5.1.1. Considerem un polígon regular de n costats, amb $n > 2$ enter. Sense pèrdua de generalitat el situem amb centre en el 0 i un dels vèrtexs en l'1. Direm que un *polígon regular de n costats és construïble amb papiroflèxia* si els seus vèrtexs són punts del conjunt $\mathcal{O}$.

Observació 5.1.2. Observem que els vèrtexs d'un polígon regular de n costats es corresponen amb les potències de l'arrel n -èsima primitiva de la unitat, ζ_n . Per tant, un polígon regular de n costats és construïble amb papiroflèxia si, i només si, $\zeta_n \in \mathcal{O}$.

Definició 5.1.3. Un *nombre primer de Pierpont* és un nombre primer de la forma $\mathcal{T}_{k,l} := 2^k 3^l + 1$, per enters $k, l \geq 0$.

Observació 5.1.4. Els nombres primers de Pierpont van ser introduïts per James Pierpont l'any 1895 en [8] on va demostrar el resultat que veurem en el Teorema 5.1.5, però utilitzant les còniques com a eina de construcció en comptes de la papiroflèxia.

Els cinc nombres primers de Pierpont més petits són:

$$\mathcal{T}_{0,0} = 2 \quad \mathcal{T}_{1,0} = 3 \quad \mathcal{T}_{2,0} = 5 \quad \mathcal{T}_{1,1} = 7 \quad \mathcal{T}_{2,1} = 13$$

Teorema 5.1.5. *Si $n > 2$ és un enter. Un polígon regular de n costats es pot construir amb papiroflèxia si, i només si, $n = 2^a 3^b p_1 \cdots p_s$, on $a, b \geq 0$ enters i $p_1, \dots, p_s$ són $s \geq 0$ nombres primers de Pierpont diferents.*

Demostració. Provarem cada una de les implicacions.

⇒ Suposem que tenim un polígon regular de n costats construïble amb papiroflèxia. Aleshores, per l'Observació 5.1.2 tenim que $\zeta_n \in \mathcal{O}$.

Sigui $f = \text{Irr}(\zeta_n, \mathbb{Q})$ i L el cos de descomposició de f sobre $\mathbb{Q}$. Pel Teorema 5.0.5 tenim que $[L : \mathbb{Q}] = 2^{a'} 3^{b'}$, amb $a', b' \geq 0$.

Com ζ_n és arrel primitiva de la unitat, per la Proposició 6.2.50 tenim que $f = \Phi_n(X)$ i $L = \mathbb{Q}(\zeta_n)$, per tant, $2^{a'} 3^{b'} = [L : \mathbb{Q}] = [\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \text{gr}(\Phi_n(X)) = \varphi(n)$. Aleshores, si $n = q_1^{k_1} \cdots q_s^{k_s}$, amb $q_1, \dots, q_s$ primers diferents, tenim:

$$\begin{aligned} 2^{a'} 3^{b'} = \varphi(n) &= n \cdot \prod_{p|n} \left(1 - \frac{1}{p}\right) = q_1^{k_1} \cdots q_s^{k_s} \cdot \left(1 - \frac{1}{q_1}\right) \cdots \left(1 - \frac{1}{q_s}\right) = \\ &= (q_1^{k_1} - q_1^{k_1-1}) \cdots (q_s^{k_s} - q_s^{k_s-1}) = q_1^{k_1-1} (q_1 - 1) \cdots q_s^{k_s-1} (q_s - 1) \end{aligned}$$

Per tal que es compleixi la igualtat cal que cada q_i , $\forall i = 1, \dots, s$, compleixi un dels següents casos:

- $q_i = 2$. Aleshores $q_i^{k_i-1}$ és una potència de 2 i $(q_i - 1) = 1$.
- $q_i = 3$. Aleshores $q_i^{k_i-1}$ és una potència de 3 i $(q_i - 1) = 2$.
- $q_i = 2^k 3^l + 1$, amb $k, l \geq 0$, i $k_i = 1$. Aleshores $q_i^{k_i-1} = 1$ i $(q_i - 1) = 2^k 3^l$.

Per tant, com teníem $n = q_1^{k_1} \cdots q_s^{k_s}$, podem reescriure $n = 2^a 3^b p_1 \cdots p_r$, on $a, b \geq 0$ i $p_1, \dots, p_r$ són nombres primers de Pierpont.

⇐ Suposem que $n = 2^a 3^b p_1 \cdots p_r$, on $a, b \geq 0$ i $p_1, \dots, p_r$ són nombres primers de Pierpont. Per a provar que un polígon regular de n costats és construïble amb papiroflèxia veurem que $\zeta_n \in \mathcal{O}$.

Com abans, utilitzem que $\text{Irr}(\zeta_n, \mathbb{Q}) = \Phi_n(X)$ i que el cos de descomposició de $\Phi_n(X)$ en $\mathbb{Q}$ és $\mathbb{Q}(\zeta_n)$. Per tant, $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$ i per provar que $\zeta_n \in \mathcal{O}$ ens cal veure que $\varphi(n) = 2^{a'} 3^{b'}$ per $a', b' \geq 0$.

Per les propietats de la funció φ d'Euler, com $2^a, 3^b, p_1, \dots, p_r$ són coprimers tenim que:

$$\begin{aligned} \varphi(n) &= \varphi(2^a 3^b p_1 \cdots p_r) = \varphi(2^a) \cdot \varphi(3^b) \cdot \varphi(p_1) \cdots \varphi(p_r) = \\ &= \begin{cases} 2^{a-1} 3^{b-1} 2(p_1 - 1) \cdots (p_s - 1), & \text{si } a, b \leq 1 \\ 3^{b-1} 2(p_1 - 1) \cdots (p_s - 1), & \text{si } a = 0, b \leq 1 \\ 2^{a-1} (p_1 - 1) \cdots (p_s - 1), & \text{si } a \leq 1, b = 0 \\ (p_1 - 1) \cdots (p_s - 1), & \text{si } a = b = 0 \end{cases} \end{aligned}$$

Com $p_i = 2^k 3^l + 1$, $\forall i = 1, \dots, s$, queda que $\varphi(n) = 2^{a'} 3^{b'}$ i, per tant, $\zeta_n \in \mathcal{O}$. $\square$

Amb aquest teorema queden determinats quins són els polígons regulars construïbles amb papiroflèxia.

Recordem que en el Teorema 2.4.5 hem vist que un polígon regular de n costats és construïble amb regla i compàs si, i només si, $n = 2^a p_1 \cdots p_s$, on $a \geq 0$ enter i $p_1, \dots, p_s$ són $s \geq 0$ nombres primers de Fermat diferents. Per tant, amb papiroflèxia, a part de poder construir tots els polígons construïbles amb regla i compàs també en podem construir d'altres com, per exemple, l'heptàgon, l'enneàgon i el tridecàgon regular. De tota manera, continuem tenint polígons impossibles de construir com és el cas de l'hendecàgon regular.

5.2 Construccions impossibles

Dediquem aquesta secció a estudiar quines de les tres construccions impossibles amb regla i compàs descrites en la secció 2.5 són possibles de construir amb papiroflèxia.

- Duplicació del cub: En la secció 2.5 hem vist que fer aquesta construcció és equivalent a poder construir $\alpha = \sqrt[3]{2}$. Aleshores, com tenim que:

$$[\mathbb{Q}(\alpha) : \mathbb{Q}] = \text{gr}(X^3 - 2) = 3.$$

Pel Teorema 5.0.4 sabem que $\alpha \in \mathcal{O}$ i, per tant, la duplicació del cub és un problema possible de resoldre utilitzant papiroflèxia.

- Trisecció de l'angle: En la secció 3.2 hem descrit com fer aquesta construcció amb papiroflèxia. Per tant, aquest problema també és possible de resoldre.
- Quadratura del cercle: Hem vist que la quadratura del cercle és una construcció impossible amb regla i compàs perquè π és transcendent. Amb els mateixos arguments obtenim que també és un problema impossible de resoldre amb papiroflèxia.

6 Requisits matemàtics

Dediquem aquest últim capítol a fer una recollida de definicions, teoremes i proposicions que són necessaris per a seguir les demostracions escrites en aquest treball.

6.1 Requisits geomètrics

Definició 6.1.1. Una *ceviana* d'un triangle és un segment que uneix un vèrtex amb un punt qualsevol del seu costat oposat. Observem que les mitjanes i les altures són cevianes.

Teorema 6.1.2 (Teorema de Ceva). *En un triangle qualsevol, tres cevianes (una des de cada vèrtex) són concurrents si, i només si,*

$$\frac{\overline{AF}}{\overline{FB}} \cdot \frac{\overline{BD}}{\overline{DC}} \cdot \frac{\overline{CE}}{\overline{EA}} = 1$$

on A, B i C són els vèrtexs del triangle i D, E i F punts que pertanyen cada un a un dels costats del triangle tal com indica la següent figura:

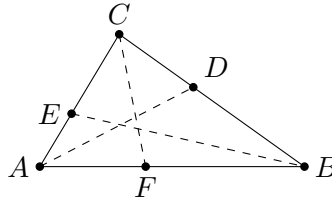


Figura 6.1. Teorema de Ceva.

Teorema 6.1.3 (Primer teorema de Tales). *Siguin dues rectes r i s concurrents en un punt O . Siguin A i A' dos punts de r i B i B' dos punts de s . Aleshores:*

$$\frac{\overline{OA'}}{\overline{OA}} = \frac{\overline{OB'}}{\overline{OB}} \iff \text{Les rectes } AB \text{ i } A'B' \text{ són paral·leles.}$$

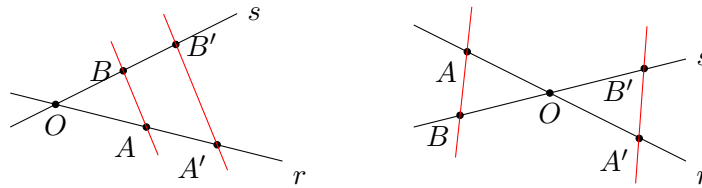


Figura 6.2. Primer teorema de Tales.

Teorema 6.1.4 (Segon teorema de Tales). *Considerem una circumferència de diàmetre $\overline{AB}$. Siguí C un punt de la circumferència diferent d' A i de B . Aleshores, l'angle ACB és un angle recte.*

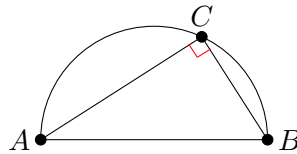


Figura 6.3. Segon teorema de Tales.

Teorema 6.1.5 (Teorema de l'altura). *Sigui ABC un triangle rectangle. Considerem l'altura del triangle respecte a la hipotenusa, és a dir, el segment perpendicular a la hipotenusa que passa per B . Anomenem H el punt de la hipotenusa que pertany al segment altura. Aleshores,*

$$\overline{BH}^2 = \overline{AH} \cdot \overline{HC}$$

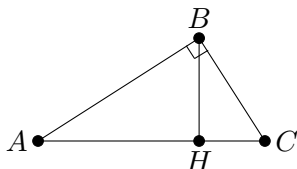


Figura 6.4. Teorema de l'altura.

6.2 Requisits algebraics

A continuació afegim les definicions i resultats utilitzats per a demostrar gran part dels teoremes vistos durant el treball. Tots aquests continguts han sigut directament extrets dels apunts de les assignatures “*Estructures algebraiques*” i “*Equacions algebraiques*” de la Universitat de Barcelona.

6.2.1 Grups

Definició 6.2.1. Un *grup* és un conjunt G dotat d'una operació binària interna que compleix:

1. la propietat associativa, és a dir, $(x \cdot y) \cdot z = x \cdot (y \cdot z), \forall x, y, z \in G$.
2. té element neutre, és a dir, $\exists e \in G$ tal que $e \cdot x = x \cdot e = x, \forall x \in G$.
3. té element simètric, és a dir, $\forall x \in G, \exists x' \in G$ tal que $x \cdot x' = x' \cdot x = e$.

Definició 6.2.2. Sigui G un grup. Diem que G és un *grup abelià* si l'operació de G és commutativa, és a dir, $x \cdot y = y \cdot x, \forall x, y \in G$.

Definició 6.2.3. Un *subgrup* d'un grup G és un subconjunt no buit H de G tal que:

1. H és tancat respecte l'operació de G , és a dir, si $x, y \in H \longrightarrow x \cdot y \in H$.
2. H és un grup amb l'operació de G .

Definició 6.2.4. Diem que un grup finit G és *resoluble* si existeix una cadena finita de subgrups

$$\{e\} = G_0 \subset G_1 \subset \dots \subset G_n = G \quad (6.2.1)$$

tals que, per a $i = 0, \dots, n-1$, es compleix les dues condicions següents:

1. G_i és normal en G_{i+1} .
2. $[G_{i+1} : G_i]$ és primer.

Teorema 6.2.5. *Tot grup d'ordre p^n , amb p primer i $n \geq 0$, és un grup soluble.*

Teorema 6.2.6. *Tot grup d'ordre $p^n q^m$, amb p i q primers diferents i $n, m \geq 0$, és un grup soluble.*

6.2.2 Anells i cossos

Definició 6.2.7. Un *anell* és un conjunt A dotat de dues operacions binàries internes:

1. L'operació suma, $+$, tal que $(A, +)$ és un grup abelià.
2. L'operació producte, $\cdot$, que compleix:
 - (a) la propietat associativa, és a dir, $(a \cdot b) \cdot c = a \cdot (b \cdot c), \forall a, b, c \in A$.
 - (b) la propietat distributiva respecte de la suma, és a dir, $a \cdot (b + c) = a \cdot b + a \cdot c$ i $(b + c) \cdot a = b \cdot a + c \cdot a, \forall a, b, c \in A$.

A més a més, si el producte és commutatiu, és a dir, $a \cdot b = b \cdot a, \forall a, b \in A$, direm que A és un *anell commutatiu*. Si existeix un element neutre del producte, és a dir, $\exists u \in A$ tal que $u \cdot a = a \cdot u = a, \forall a \in A$, direm que A és un *anell unitari*.

Definició 6.2.8. Sigui A un anell i B un subconjunt d' A . Direm que B és un *subanell* d' A si compleix:

1. $(B, +)$ és un subgrup de $(A, +)$.
2. B és tancat pel producte d' A , és a dir, si $b, c \in B$, aleshores, $b \cdot c \in B$.

Si A és un anell unitari direm que un subanell B d' A és un *subanell unitari* si conté l'element neutre d' A .

A partir d'ara i durant tot el document, tots els anells considerats són commutatius i unitaris.

Definició 6.2.9. Sigui A un anell i $a \in A$ no nul. Diem que a és un *divisor de 0* si existeix $b \in A$ no nul tal que $a \cdot b = 0$.

Definició 6.2.10. Sigui A un anell. Direm que A és un *domini d'integritat* si no té divisors de 0. Equivalentment, si per $a, b \in A$ tal que $a \cdot b = 0$, aleshores $a = 0$ o bé $b = 0$.

Definició 6.2.11. Sigui A un anell i $a \in A$. Direm que a és *invertible* o *unitat* si existeix un element $b \in A$ tal que $a \cdot b = b \cdot a = 1$. Direm que b és l'*invers* d' a . Designem A^* el conjunt dels elements invertibles d' A .

Definició 6.2.12. Un *cos* és un anell no trivial en què tot element no nul és invertible.

Definició 6.2.13. Sigui K un cos i L un subanell de K . Diem que L és un *subcòs* de K si $x^{-1} \in L, \forall x \in L \setminus \{0\}$, on x^{-1} designa l'invers de x .

6.2.3 Extensions de cossos

D'ara endavant considerem que L és un cos i K un subcòs de L . Posem $K \subset L$ o L/K per a denotar que L és cos extensió de K . Si L/K és extensió de cossos, el cos L és un K -espai vectorial.

Definició 6.2.14. Diem *grau de l'extensió* L/K i denotem per $[L : K]$ la dimensió de L com a K -espai vectorial. Diem que l'extensió L/K és *finita* si el grau és finit. Si el grau és infinit diem que l'extensió és *infinita*.

Proposició 6.2.15 (Fórmula de graus). *Siguin K, L i M cossos tals que $K \subset L \subset M$. L'extensió M/K és finita si, i només si, les extensions M/L i L/K són finites i, en aquest cas, es compleix la igualtat:*

$$[M : K] = [M : L][L : K]$$

6.2.4 Elements algebraics i transcendent

Definició 6.2.16. Sigui $\alpha \in L$. Diem que α és *algebraic sobre K* si existeix un polinomi no nul $P(X) \in K[X]$ tal que $P(\alpha) = 0$. En cas contrari diem que α és *transcendent*.

Notació 6.2.17. Si $\alpha \in L$ és algebraic sobre K , definim $K(\alpha) := \{P(\alpha) \mid P \in K[X]\}$ que és un cos.

Definició 6.2.18. Una extensió de cossos L/K es diu *algebraica* si tot element de L és algebraic sobre K . En cas contrari, diem que l'extensió L/K és *transcendent*.

Proposició 6.2.19. Si una extensió de cossos L/K és finita, aleshores és algebraica.

6.2.5 Polinomi irreductible o mínim

Lema 6.2.20. Si $\alpha \in L$ algebraic sobre K , aleshores existeix un únic polinomi mònic no constant $p \in K[x]$ amb les següents dues propietats:

1. α és arrel de p , és a dir, $p(\alpha) = 0$.
2. Si $f \in K[x]$ és tal que $f(\alpha) = 0$, aleshores f és múltiple de p .

Proposició 6.2.21. Sigui $\alpha \in L$ algebraic sobre K i sigui $p \in K[X]$ el polinomi del Lema anterior (Lema 6.2.20). Si $f \in K[X]$ és un polinomi mònic no constant, aleshores:

$$\begin{aligned} f = p &\iff f \text{ és un polinomi de grau mínim tal que } f(\alpha) = 0 \\ &\iff f \text{ és irreductible sobre } K \text{ i } f(\alpha) = 0 \end{aligned}$$

Definició 6.2.22. Sigui $\alpha \in L$. Si α és algebraic sobre K , aleshores el polinomi p del Lema 6.2.20 s'anomena el *polinomi mínim o irreductible de α sobre K* . Posem $\text{Irr}(\alpha, K)$ per designar el polinomi mínim o irreductible de α sobre K .

Proposició 6.2.23. Si $\alpha \in L$ és algebraic sobre K , aleshores $[K(\alpha) : K] = \text{gr}(\text{Irr}(\alpha, K))$.

6.2.6 Grup de Galois d'una extensió

Definició 6.2.24. Si L/K és una extensió de cossos, el conjunt d'automorfismes de L/K té estructura de grup amb la composició d'aplicacions. Aquest grup s'anomena *grup de Galois de l'extensió L/K* . Posem $\text{Gal}(L/K)$ per a designar el grup de Galois de l'extensió L/K .

Proposició 6.2.25. Si $K(\alpha)/K$ és una extensió algebraica, l'ordre de $\text{Gal}(K(\alpha)/K)$ és igual al nombre d'arrels diferents de $\text{Irr}(\alpha, K)$ a $K(\alpha)$.

6.2.7 Cos de descomposició d'un polinomi

Definició 6.2.26. Siguin K un cos i $f \in K[X]$ de grau $n > 0$. Sigui L un cos extensió de K . Diem que f *descompon totalment sobre L* si existeixen elements $\alpha_1, \alpha_2, \dots, \alpha_n \in L$ tal que es compleix a $L[X]$ la igualtat:

$$f(X) = a(X - \alpha_1)(X - \alpha_2) \cdots (X - \alpha_n)$$

on a és el coeficient de X^n a f .

Definició 6.2.27. Siguin K un cos i $f \in K[X]$ de grau $n > 0$. Sigui L un cos extensió de K . Diem que L és *cos de descomposició de f sobre K* si f descompon totalment sobre L i, a més a més, es compleix $L = K(\alpha_1, \alpha_2, \dots, \alpha_n)$.

Observació 6.2.28. Si $f \in K[X]$ i L és un cos extensió de K on f descompon totalment, aleshores L conté un cos de descomposició de f : el cos generat sobre K per les arrels de f a L .

Proposició 6.2.29 (Existència del cos de descomposició). *Siguin K un cos i $f \in K[X]$ un polinomi de grau $n > 0$. Aleshores existeix un cos de descomposició de f sobre K .*

Proposició 6.2.30 (Unicitat del cos de descomposició). *Siguin $\sigma : K_1 \rightarrow K_2$ un isomorfisme de cossos i $f \in K[X]$ un polinomi de grau $n > 0$. Sigui L_1 un cos de descomposició de f sobre K_1 i sigui L_2 un cos de descomposició de $\sigma(f)$ sobre K_2 . Aleshores existeix un isomorfisme de L_1 en L_2 sobre σ .*

6.2.8 Extensió normal

Definició 6.2.31. Sigui L/K una extensió de cossos. Direm que L/K és *normal* si tot polinomi de $K[X]$, irreductible sobre K , que tingui una arrel a L descompon totalment sobre L .

Proposició 6.2.32. *Sigui L/K una extensió finita de cossos. Aleshores L/K és normal si, i només si, L és el cos de descomposició d'algun polinomi de $K[X]$.*

Corol·lari 6.2.33. *Sigui L/K una extensió de cossos, normal i finita i sigui $f \in K[X]$ irreductible sobre K . Si α, β són arrels de f a L , existeix $\sigma \in \text{Gal}(L/K)$ tal que $\sigma(\alpha) = \beta$.*

6.2.9 Extensió separable

Definició 6.2.34. Siguin K un cos i $f \in K[X]$ un polinomi irreductible sobre K . Diem que f és *separable sobre K* si les arrels de f en un cos de descomposició de K són totes diferents. Si f no és separable sobre K diem que és *inseparable sobre K* .

Definició 6.2.35. Sigui L/K una extensió de cossos. Sigui $\alpha \in L$ algebraic sobre K . Diem que α és *separable sobre K* si $\text{Irr}(\alpha, K)$ és separable sobre K .

Definició 6.2.36. Una extensió algebraica de cossos L/K és *separable* si tot element de L és separable sobre K .

Proposició 6.2.37. *Si K és un cos de característica 0, aleshores:*

- (a) *Tot polinomi irreductible de $K[X]$ és separable.*
- (b) *Tota extensió algebraica de K és separable.*

6.2.10 Element primitiu

Definició 6.2.38. Sigui L/K una extensió de cossos. Un element $\alpha \in L$ es diu *element primitiu de l'extensió L/K* si $L = K(\alpha)$.

Teorema 6.2.39 (Teorema de l'element primitiu). *Sigui K un cos infinit i L/K una extensió finita i separable. Aleshores existeix un element $\alpha \in L$ tal que $L = K(\alpha)$.*

6.2.11 Extensió de Galois

Definició 6.2.40. Una extensió finita de cossos L/K diem que és *de Galois* si és normal i separable.

Definició 6.2.41. Si L/K és extensió de cossos, diem *cos intermedi de l'extensió L/K* a un subcòs de L que conté K com a subcòs.

Definició 6.2.42. Sigui L/K una extensió de cossos. Si E és un cos intermedi de L/K , $\text{Gal}(L/E)$ és clarament un subgrup de $\text{Gal}(L/K)$. Si H és un subgrup de $\text{Gal}(L/K)$ el subcòs L^H de L fix per H és un cos intermedi de L/K . Posem $\mathcal{E}$ el conjunt de cossos intermedis de L/K i $\mathcal{H}$ el conjunt de subgrups de $\text{Gal}(L/K)$. Les aplicacions

$$\begin{array}{ll} \Phi : \mathcal{E} \rightarrow \mathcal{H} & \Psi : \mathcal{H} \rightarrow \mathcal{E} \\ E \mapsto \text{Gal}(L/E) & H \mapsto L^H \end{array}$$

s'anomenen *correspondències de Galois*.

Teorema 6.2.43 (Teorema fonamental de la teoria de Galois). *Sigui L/K una extensió de Galois de grau n . Es compleixen els enunciats següents:*

1. El grup $\text{Gal}(L/K)$ té ordre n .
2. Les correspondències de Galois són bijectives i inverses l'una de l'altra i es compleixen les igualtats:

$$[L : E] = |\text{Gal}(L/E)| \quad i \quad [E : K] = [\text{Gal}(L/K) : \text{Gal}(L/E)]$$

per a tot cos intermedi E de L/K .

3. Si E és el cos intermedi de L/K , l'extensió E/K és normal si, i només si, $\text{Gal}(L/E)$ és subgrup normal de $\text{Gal}(L/K)$. En aquest cas, es té un isomorfisme de grups $\text{Gal}(E/K) \simeq \text{Gal}(L/K) / \text{Gal}(L/E)$.

6.2.12 Clausura de Galois

Proposició 6.2.44. *Sigui L/K una extensió finita i separable. Aleshores, existeix una extensió M/L tal que:*

- (a) M/K és una extensió de Galois.
- (b) Si M'/L és una altra extensió tal que M'/K és de Galois, aleshores existeix un isomorfisme de cossos $\phi : M \rightarrow M'$ que és identitat en L .

Diem que M és la *clausura de Galois de L/K* .

6.2.13 Cossos ciclotòmics

Definició 6.2.45. Anomenem *cos ciclotòmic n -èsim* el cos de descomposició del polinomi $X^n - 1$ sobre $\mathbb{Q}$.

Observació 6.2.46. Les arrels d'aquest polinomi en el seu cos de descomposició són les *arrels n -èsimes de la unitat*. Si $\zeta_n := e^{\frac{2\pi i}{n}}$, que és arrel n -èsima primitiva de la unitat, les arrels de $X^n - 1$ són les potències de ζ_n . El cos ciclotòmic n -èsim és doncs $\mathbb{Q}(\zeta_n)$, on ζ_n és una arrel n -èsima primitiva de la unitat.

Definició 6.2.47. Anomenem $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ *extensió ciclotòmica n -èsima*. Aquesta extensió és de Galois.

Definició 6.2.48. La funció φ d'Euler és la següent:

$$\varphi(n) = n \cdot \prod_{p|n} \left(1 - \frac{1}{p}\right), \text{ per a } p \text{ primer.}$$

Definició 6.2.49. Posem $\mathcal{P}$ el conjunt de les arrels n -èsimes primitives de la unitat i definim el *polinomi ciclotòmic n -èsim*:

$$\Phi_n(X) := \prod_{\zeta \in \mathcal{P}} (X - \zeta)$$

Proposició 6.2.50. *Es compleix*

- (a) $\Phi_n(X) \in \mathbb{Q}[X]$;
- (b) $\Phi_n(X)$ és irreductible sobre $\mathbb{Q}$.

Per tant, $\Phi_n(X)$ és el polinomi irreductible de ζ_n sobre $\mathbb{Q}$ i $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$.

Observació 6.2.51. Considerem el polinomi $X^n - 1$. Les seves arrels són arrels n -èsimes de la unitat i cada una d'aquestes arrels és arrel d -èsima primitiva per a algun divisor positiu d de n . Tenim doncs:

$$X^n - 1 = \prod_{d|n} \Phi_d(X) \tag{6.2.2}$$

Prenent graus a banda i banda de (6.2.2), obtenim $n = \sum_{d|n} \varphi(d)$, amb d els divisors positius de n .

6.2.14 Criteri de Gauss

Teorema 6.2.52 (Criteri de Gauss). *Considerem el següent polinomi amb coeficients racionals:*

$$f(X) = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_0$$

amb a_n, a_0 enters diferents de 0. Aleshores les possibles arrels racionals d'aquest polinomi són de la forma $x = \frac{p}{q}$ on:

- p és divisor d' a_0 .
- q és divisor d' a_n .
- p i q són coprimers.

7 Conclusions

En aquest treball hem pogut explorar amb profunditat les construccions amb papiroflèxia demostrant que amb aquesta eina és possible replicar totes les construccions amb regla i compàs i superar-ne les limitacions. A més a més, hem pogut relacionar totes aquestes construccions geomètriques amb continguts algebraics apresos durant el grau com les estructures algebraiques o la teoria de Galois.

A part de la papiroflèxia, existeixen altres eines que ens permeten també superar els límits de les construccions amb regla i compàs i, de fet, algunes generen el mateix conjunt de nombres que el generat amb papiroflèxia. Dues d'aquestes eines alternatives són el regla graduat (amb només dues marques indicant la distància de 0 a 1) i la intersecció de còniques. Per a una introducció a aquestes eines es pot consultar la secció 10.3.C del llibre [2], una extensió de la intersecció de còniques es troba en [11] i un estudi exhaustiu de més eines de construcció geomètrica es desenvolupa al llarg de [7].

Aquest treball, i parlant ja en primera persona, he pogut gaudir-lo molt en tot el seu procés. Més enllà d'enriquir-me amb nous coneixements sobre papiroflèxia i àlgebra, també m'ha permès adquirir certes habilitats. He après a escriure i fer figures amb relativa fluïdesa en $\text{\LaTeX}$, he millorat la comprensió de textos matemàtics i he après a redactar i estructurar un text matemàtic. A més a més, el tema escollit per a aquest treball m'ha permès poder compartir les matemàtiques amb gent del meu volant que no està familiaritzada amb aquesta disciplina. En definitiva, ha sigut una molt bona experiència final del grau.

Referències

- [1] Alperin, Roger C. *A mathematical theory of origami constructions and numbers*. New York J. Math. 6, pages 119-133, 2000.
- [2] Cox, David A. *Galois theory*. Second edition. Pure and Applied Mathematics (Hoboken). John Wiley & Sons, Inc., Hoboken, NJ, 2012. ISBN: 978-1-118-07205-9.
- [3] Greene, Julia. *Geometric Constructions, Origami, and Galois Theory*. y. Department of Mathematics, UNION COLLEGE, Schenectady, New York, 2019.
- [4] Lang, Robert J. *Origami and Geometric Constructions*. 1996–2015.
https://langorigami.com/wp-content/uploads/2015/09/origami_constructions.pdf
- [5] Lee, Hwa Young. *Origami-constructible numbers*. PhD thesis, University of Georgia, 2017.
- [6] Lindemann, Ferdinand. *Ueber die Zahl π* . Mathematische Annalen 20, pages 213-225. 1882.
- [7] Martin, George E. *Geometric Constructions*. Undergraduate Texts in Mathematics. Springer-Verlag New York, Inc. 1998. ISBN: 978-1-4612-6845-1.
- [8] Pierpont, James. *On an undemonstrated theorem of the Disquisitiones Arithmeticae*. American Mathematical Society Bulletin, 2, pages 77-83, 1895-1896.
- [9] Row, T. Sundara. *Geometric Exercises in Paper Folding*. The Open Court Publishing Co, P. O. Drawer F, Chicago, 1901.
- [10] Schwartz, Randy K. *Pi is Transcendental: Von Lindemann's Proof Made Accessible to Today's Undergraduates*. 2006
https://home.agh.edu.pl/~rudol/Pi_TranscendentalLindemann.pdf
- [11] Videla, Carlos R. *On points constructible from conics*. The Mathematical Intelligencer, Volume 19, pages 53-57, 1997. DOI: 10.1007/BF03024434.