UNIVERSITAT DE BARCELONA
Facultat de Matemàtiques i Informàtica

GRAU DE MATEMÀTIQUES

Treball final de grau

Construcció de polígons regulars sobre la lemniscata

Autor: Toni Soler Terricabras

Director: Dra. Teresa Crespo Vicente
Realitzat a: Departament de Matemàtiques i Informàtica

Barcelona, 13 de juny de 2023

Abstract

The main goal of this study is to set a theoretical framework that allows us to determine in general sense which regular polygons can be constructed with ruler and compass on the lemniscate. To accomplish this, we compute the Galois groups arising from the division points of the curve. It is through the construction of *lemnatomic extensions*, analogous to cyclotomic extensions associated with the circle, that the constructibility of the desired polygons is determined. The present study puts forth two complementary formulations to address this problem: the first one, based on a purely geometric foundation, and the second one, with a broader approach incorporating the use of elliptic functions and elliptic curves.

Resum

L'objectiu principal d'aquest treball és desenvolupar un marc teòric que permeti determinar de manera general quins polígons regulars són construïbles amb regle i compàs sobre la lemniscata. Per a fer-ho, s'estudia els grups de Galois que sorgeixen dels punts de divisió de la corba. És a través de la construcció d'extensions *lemnatòmiques*, anàlogues a les ciclotòmiques associades a la circumferència, que es determina la constructibilitat dels polígons desitjats. El treball presenta dues formulacions complementàries per a donar resposta a aquest problema: la primera, de fonament purament geomètric, i la segona, amb un enfocament més ampli amb l'ús de funcions i corbes el·líptiques.

2020 Mathematics Subject Classification. 11R32, 12F05, 11G15, 33E05

Agraïments

En primer lloc, m'agradaria agrair a la meva tutora, la Dra.Teresa Crespo, la seva paciència, consell i suport durant les reunions que hem mantingut cada setmana durant el semestre. La seva perspectiva aclaridora i didàctica ha estat enriquidora no només durant l'elaboració d'aquest treball, sinó també al llarg de tot el grau. Gràcies a ella, he tingut l'oportunitat de descobrir un tema tan fascinant com la teoria de Galois. També voldria donar les gràcies als meus pares per permetre'm completar els meus estudis i per donar-me el seu suport incondicionalment. Per acabar, és amb estima i determinació que abraço la llengua catalana en aquest treball amb la voluntat d'apropar conceptes i adaptar terminologies a la nostra llengua per a fer els continguts matemàtics més accessibles i facilitar-ne el diàleg en la nostra parla.

Índex

1 Introducció

Aquest treball pretén explorar detalladament quins polígons regulars són construïbles amb regle i compàs sobre la corba de la lemniscata. Per a determinar-ho, n'hi ha prou amb trobar en quants trossos de mateixa longitud d'arc es pot dividir amb regle i compàs la corba en qüestió, és a dir, identificar quins són els punts de divisió construïbles.

Per començar, a la Secció 2 es presenten conceptes bàsics que permetran caracteritzar les nocions geomètriques essencials de la lemniscata, com ara la *constant lemniscàtica* ϖ, que jugarà el paper equivalent al valor π a la circumferència. D'entre els diferents conceptes, el més rellevant serà la definició d'una funció ϕ que permetrà atribuir a la longitud d'arc de la corba des de l'origen a un punt donat la distància entre els extrems d'aquest arc. Veurem que aquesta funció, a priori, està definida a l'interval $[0, \frac{\varpi}{2}]$.

A continuació, estendrem la funció ϕ a tot $\mathbb{R}$ a la Secció 3. En el procés, desenvoluparem fórmules d'addició i multiplicació per a ϕ i les usarem per a demostrar que $\phi\left(\frac{2\varpi}{n}\right)$ són les arrels d'un polinomi amb coeficients a $\mathbb{Z}$, que anomenarem *polinomi de n-divisió*. Demostrarem que aquestes arrels són construïbles si, i només si, tots els n-punts de torsió de la lemniscata són construïbles amb regle i compàs. Posteriorment, a la Secció 4 portarem més enllà aquesta extensió i aconseguirem definir ϕ com una funció doblement periòdica i meromorfa a $\mathbb{C}$. En el cas complex, trobarem fórmules d'addició i multiplicació anàlogues al cas real fent servir algunes nocions característiques de l'anell d'enters de Gauss, $\mathbb{Z}[i]$. Estirant aquest fil, podrem definir *polinomis de β-divisió* a $\mathbb{Z}[i][x]$ per analogia als trobats pel cas real.

Un cop adquirida una comprensió sòlida del comportament de la funció ϕ en el seu sentit més ampli, s'obrirà pas a una secció fonamental per al nostre estudi: la teoria de Galois a la lemniscata (Secció 5). En aquest apartat, es desenvoluparà una teoria anàloga a la dels cossos ciclòtomics en el cas de la circumferència però, aquesta vegada, pel cas de la lemniscata. Per a fer-ho, s'analitzaran els grups de Galois d'unes extensions que anomenarem *lemnatòmiques* (per analogia a les extensions ciclotòmiques) a partir de dues estratègies diferents.

Per una banda, construirem les extensions que resulten d'adjuntar a $\mathbb{Q}(i)$ els valors $\phi\left(\frac{2\varpi}{n}\right)$. L'aparició del nombre complex i pot ser inesperada però cobrarà sentit una vegada s'hagin vist les operacions complexes de ϕ a la Secció 4. Ens referirem a aquest plantejament com a *natural* perquè, geomètricament, els elements adjuntats en el cos extensió són les distàncies dels punts de n-divisió de la lemniscata.

D'altra banda, utilitzarem un altre plantejament més general per a construir les extensions lemnatòmiques, que batejarem com *alternatiu*. En aquest enfocament, les extensions es construiran adjuntant a $\mathbb{Q}(i)$ els valors $\phi\left(\frac{2\varpi}{\beta}\right)$, on $\beta \in \mathbb{Z}[i]$. Clarament, el plantejament *natural* quedarà englobat dins de l'*alternatiu*. Gràcies a un marc previ que es proporcionarà sobre funcions i corbes el·líptiques, podrem caracteritzar els grups de Galois resultants d'aquestes extensions més sofisticades. Per a completar l'analogia amb el cas de la circumferència, definirem els *polinomis lemnatòmics*, que seran els equivalents als polinomis ciclotòmics, i demostrarem que són irreductibles sobre $\mathbb{Q}(i)$.

En qualsevol de les dues estratègies usades en aquest treball, l'ordre del grup de Galois determinarà per quins valors concrets seran possibles les divisions corresponents de la lemniscata amb regle i compàs. Finalment, a l'Apèndix A es realitza amb tot detall les primeres construccions possibles amb regle i compàs (per a $n \leq 12$). En particular, en aquest apartat s'ofereixen contribucions de construccions pràctiques de polígons sobre la lemniscata així com la forma dels polinomis lemnatòmics corresponents que, fins al moment, en alguns casos no figuren explícitament a la literatura.

En resum, aquest treball s'articula a través de diverses seccions que, malgrat semblin força diferents, convergeixen per a poder donar resposta al problema de quins polígons són construïbles amb regle i compàs sobre la lemniscata. En aquest treball s'assumeixen coneixements previs en els següents àmbits: Equacions Algebraiques, Estructures Algebraiques i Anàlisi Complexa.

NOTA HISTÒRICA

Les primeres figures geomètriques en forma de 8 de les quals tenim constància s'atribueixen a Procle [1], un matemàtic i filòsof neoplatònic que visqué al S.V a.C., i les considerava com a seccions transversals d'un tor per un pla paral·lel a l'eix de la figura. Tanmateix, la noció de lemniscata tal com la coneixem avui dia (i com definirem a la Secció 2) va aparèixer per primera vegada a la literatura matemàtica l'any 1680.

Cassini, un matemàtic i astrònom francoitalià que visqué a cavall dels segles XVII i XVIII, va introduir la lemniscata com a cas particular d'una família de corbes que coneixem com a *òvals de Cassini* [2]. De manera paral·lela i independent, Jacob Bernoulli també va deduir l'equació d'aquesta corba l'any 1691 [3]. En les seves paraules, ≪[té] la forma de la figura 8 de costat, o la d'una banda doblegada en un nus, o la d'un *lemniscus*, o la d'un nus d'una cinta francesa≫[4]. En aquest context, *lemniscus* és una paraula llatina (prèviament grega, $\lambda\eta\mu\nu\iota\sigma\kappa o\varsigma$) que es refereix a una cinta penjant enganxada a les garnaldes que portaven els guanyadors de competicions d'atletisme. Bernoulli va trobar aquesta corba de manera indirecta a través del seu estudi de la corba elàstica. Es pot consultar [5] per a llegir una discussió en disputa de prelació entre Bernoulli i el seu germà Johann, qui també va descobrir independentment la lemniscata l'any 1964 en un context diferent. En particular, l'ús de coordenades polars que va implementar Bernoulli per a calcular la longitud d'arc de la lemniscata (que apareixerà a la Secció 2) va ser el primer ús de la longitud d'arc en aquestes coordenades. D'aquesta manera, a principis de S.XVIII ja es coneixien tant la lemniscata com els seus atributs principals. És per això que el problema de dividir aquesta corba en segments de mateixa longitud d'arc fos un tema familiar en la comunitat matemàtica del moment.

A continuació, va ser Fagnano qui va prendre el relleu en la recerca d'aquesta qüestió. A partir de 1718 va aconseguir dividir la lemniscata en tres[2] i cinc segments de mateixa longitud d'arc amb regle i compàs [6]. Fagnano va trametre les seves troballes a l'Acadèmia de Berlín com a part de la seva sol·licitud com a membre. L'encarregat de llegir

[2]El cas de dos segments de mateixa longitud d'arc és trivial.

la seva feina va ser Euler i, a través d'aquesta interacció, van ser capaços de generalitzar els càlculs de Fagnano fins a desenvolupar la teoria d'*integrals el·líptiques*, que posteriorment seria explorada amb tot detall per Lagrange i Legendre.

La primera persona a considerar la funció ϕ, entesa com la inversa de la longitud d'arc de la lemniscata, fou Gauss l'any 1797 [7], malgrat que la seva obra no va ser publicada fins el 1855, després de la seva mort. Per altra banda, Abel i Jacobi van introduir les inverses de funcions el·líptiques el 1827 [8]. Un dels descobriments crucials de Gauss, Abel i Jacobi va ser que les funcions inverses d'integrals el·líptiques són funcions doblement periòdiques en variable complexa, com veurem a la Secció 5. Eisenstein també va jugar un paper important en aquesta història ja que va ser ell el primer en demostrar el Teorema 4.19, que serà la pedra angular del nostre treball. Per últim, les primeres demostracions completes del Teorema 5.32, que es mencionaran al plantejament *alternatiu* de la Secció 5, van ser aportades per Takagi i Fueter cap a la dècada de 1920 a partir del naixement de la teoria de cossos de classe [9].

2 Conceptes bàsics

2.1 Definició de lemniscata

Definició 2.1. *Anomenem lemniscata el lloc geomètric tal que el producte de les distàncies de cada punt η a dos punts fixats η_1, η_2, anomenats focus, té un valor constant k^2.*

Aquesta definició dóna lloc a una família de corbes. Per això, triem que els focus siguin $\eta_1 = \left(\frac{\sqrt{2}}{2}, 0\right)$ i $\eta_2 = \left(-\frac{\sqrt{2}}{2}, 0\right)$ i que la constant sigui $k^2 = \frac{1}{2}$. D'aquesta manera, l'equació de la lemniscata s'expressa respectivament en coordenades cartesianes i en coordenades polars com

$$(x^2 + y^2)^2 = x^2 - y^2, \qquad r^2 = cos(2\theta) \tag{2.1}$$

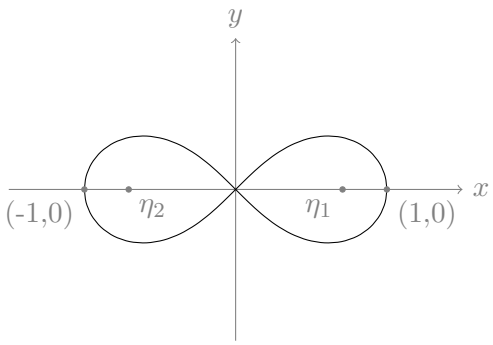

Figura 1: Lemniscata definida segons (2.1).

2.2 Longitud d'arc de la lemniscata

La longitud d'arc es pot calcular a partir de

$$ds^2 = dr^2 + r^2 d\theta^2 \Rightarrow \left(\frac{ds}{dr}\right)^2 = 1 + \left(r\frac{d\theta}{dr}\right)^2$$

Com que l'equació polar de la lemniscata és $r^2 = cos(2\theta)$, tenim $\theta = \frac{1}{2} arccos(r^2)$. Llavors

$$\frac{d\theta}{dr} = \frac{-r}{\sqrt{1 - r^4}} \Rightarrow \left(\frac{ds}{dr}\right)^2 = 1 + \frac{r^4}{1 - r^4}$$

Així doncs, la longitud d'arc de la lemniscata és

$$ds = \frac{dr}{\sqrt{1 - r^4}} \Rightarrow s = \int_0^r \frac{dt}{\sqrt{1 - t^4}} \tag{2.2}$$

Tal com hem definit la lemniscata a (2.1), el radi màxim que pot assolir és 1. Aleshores, al primer quadrant podem assegurar que $r \in [0, 1]$. Sovint ens referim a la integral (2.2) com integral lemniscàtica.

Definició 2.2. *Definim constant lemniscàtica el valor ϖ tal que*

$$\frac{\varpi}{2} = \int_0^1 \frac{dt}{\sqrt{1 - t^4}} \tag{2.3}$$

Observació 2.3. (i) Com que la integral de (2.3) és convergent, podem afirmar que $\varpi/2$ és la longitud d'arc de la porció del primer quadrant de la lemniscata. Així doncs, atesa la simetria de la corba, és immediat veure que la longitud d'arc total de la lemniscata és 2ϖ. De mateixa manera, és clar que la longitud d'arc entre successius punts de n-divisió de la lemniscata és $2\varpi/n$.

(ii) La constant ϖ és l'anàleg a π a la circumferència. Més concretament, podem dir que ϖ proporciona una relació entre la longitud d'arc de la lemniscata des de l'origen fins a un punt qualsevol de la corba i el radi d'aquest últim.

(iii) La integral (2.3) és no elemental. Per tant, sabem que ϖ és irracional. En particular, d'acord amb [10], $\varpi = 2.622057554292119810464839589891119413682754951431 6...$

2.3 Funció inversa ϕ

Ara fixem-nos que la longitud d'arc s a (2.2) descriu una funció monòtona creixent per a $r \in [0, 1]$. Per consegüent, podem expressar també r en funció de s segons una funció inversa ϕ que està definida a $[0, \frac{\varpi}{2}]$, i.e. $r = \phi(s)$. Equivalentment, doncs, podem escriure

$$\begin{gathered} \phi\colon \left[0, \frac{\varpi}{2}\right] \longrightarrow [0,1] \\ \int_0^r \frac{dt}{\sqrt{1-t^4}} = s \mapsto \phi(s) = r \end{gathered} \tag{2.4}$$

on s representa la longitud d'arc des de l'origen a un punt al primer quadrant de la lemniscata. Notem que $\phi(s)$ està definida a $[0, \frac{\varpi}{2}]$. En les properes seccions, però, veurem de quines maneres és possible estendre aquesta funció ϕ a $\mathbb{R}$ i, posteriorment, a $\mathbb{C}$.

3 La funció lemniscàtica real

Aquesta secció es fonamenta en la informació proporcionada per les següents fonts: [4], [11], [12] i [13]. Per a obtenir una comprensió més exhaustiva i detallada sobre el tema, es pot consultar aquesta selecció de textos.

3.1 Extensió de ϕ a una funció real

A la Secció 2 s'ha definit la funció ϕ d'acord amb la relació

$$r = \phi(s) \iff s(r) = \int_0^r \frac{dt}{\sqrt{1-t^4}}$$

on s representa la longitud d'arc des de l'origen a un punt al primer quadrant de la lemniscata i $\phi(s)$ està definida a $[0, \frac{\varpi}{2}]$.

Podem estendre fàcilment ϕ a $\mathbb{R}$. Donat $s \in \mathbb{R}$, $\phi(s)$ és la distància al punt de la lemniscata tal que la seva longitud d'arc des de l'origen és s. Ens adonem que quan $|s|$ és prou gran, és necessari fer unes quantes voltes per a trobar el punt de la lemniscata associat. Tanmateix, com que la longitud d'arc total de la lemniscata és 2ϖ, sabem que s i $s + 2k\varpi, k \in \mathbb{Z}$, tindran associat el mateix punt a la lemniscata. A més, com que s i $-s$ correspondran a punts simètrics respecte a l'origen a la lemniscata, tindrem

$$\phi(-s) = -\phi(s) \tag{3.1}$$

Similarment, ens adonem que s i $\varpi - s$ són simètrics respecte de l'eix d'abscisses. Per tant,

$$\phi(\varpi - s) = \phi(s) \tag{3.2}$$

Proposició 3.1. *Sigui $\phi(s)$ la funció definida a* (2.4)*. Aleshores,*

$$\phi'(s) = \sqrt{1-\phi^4(s)}, \quad s \in \left[0, \frac{\varpi}{2}\right]$$

Demostració. Observem que (2.4) ens dóna la identitat

$$s = \int_0^{\phi(s)} \frac{dt}{\sqrt{1-t^4}}, \quad s \in \left[0, \frac{\varpi}{2}\right]$$

En virtut del teorema fonamental del càlcul i de la regla de la cadena, si derivem respecte de s ambdues bandes de l'expressió anterior, obtenim

$$1 = \frac{\phi'(s)}{\sqrt{1-\phi^4(s)}}, \quad s \in \left[0, \frac{\varpi}{2}\right)$$

I d'aquí se segueix que

$$\phi'(s) = \sqrt{1-\phi^4(s)}, \quad s \in \left[0, \frac{\varpi}{2}\right)$$

Fixem-nos que, en aquest raonament, cal excloure el valor $s = \frac{\varpi}{2}$ perquè $\sqrt{1-\phi^4(s)}$ s'anul·laria ja que $\phi\left(\frac{\varpi}{2}\right) = 1$. No obstant això, com que 1 és el valor màxim que assoleix $\phi(s)$, veiem que $\phi'(s)$ s'anul·laria per a $\frac{\varpi}{2}$. Per la qual cosa, podem estendre la definició de la derivada a tot l'interval (tancat), com volíem demostrar. □

3.2 Lleis d'addició

3.2.1 Duplicació de la longitud d'arc de la lemniscata

La integral (2.4) pot recordar a la fórmula anàloga a la longitud d'arc de la circumferència

$$\arcsin(r) = \int_0^r \frac{dt}{\sqrt{1-t^2}}, \quad r \in [0,1] \tag{3.3}$$

que, com bé sabem, el seu integrant pot ser racionalitzat a través de la substitució

$$r = \frac{2t}{1+t^2}, \quad t \in [0,1] \tag{3.4}$$

de manera que

$$\sqrt{1-r^2} = \frac{1-t^2}{1+t^2}, \quad \frac{dr}{dt} = 2\frac{1-t^2}{(1+t^2)^2} \Rightarrow \frac{dr}{\sqrt{1-r^2}} = \frac{2\,dt}{1+t}$$

En el nostre cas, observem que la integral lemniscàtica conté $\sqrt{1-r^4}$ en lloc de $\sqrt{1-r^2}$. Per analogia, això suggereix l'ús de la següent substitució:

$$r^2 = \frac{2t^2}{1+t^4}, \quad t \in [0,1] \tag{3.5}$$

la qual cosa ens duu a

$$\sqrt{1-r^4} = \frac{1-t^4}{1+t^4}, \quad r = \frac{\sqrt{2}\,t}{\sqrt{1+t^4}}, \quad \frac{dr}{dt} = \frac{\sqrt{2}}{\sqrt{1+t^4}}\frac{1-t^4}{1+t^4}$$

I per tant, arribem a

$$\frac{dr}{\sqrt{1-r^4}} = \sqrt{2}\frac{dt}{\sqrt{1+t^4}}, \quad t \in [0,1] \tag{3.6}$$

Com que la relació (3.5) defineix una aplicació monòtona creixent de l'interval $t \in [0,1]$ a l'interval $s \in [0,1]$, tenim

$$\int_0^r \frac{d\tilde{r}}{\sqrt{1-\tilde{r}^4}} = \sqrt{2}\int_0^t \frac{d\tilde{t}}{\sqrt{1+\tilde{t}^4}}, \quad r \in [0,1] \tag{3.7}$$

La substitució (3.5) no ha racionalitzat l'integrant de la integral lemniscàtica com esperàvem, la qual cosa pot fer-nos pensar que la substitució aplicada no presenta cap avantatge. Però això no és cert. Si apliquem la següent substitució a la part dreta de (3.7)

$$t^2 = \frac{2u^2}{1-u^4}, \quad u \in [0,1] \tag{3.8}$$

de manera que

$$\sqrt{1+t^4} = \frac{1+u^4}{1-u^4}, \quad t = \frac{\sqrt{2}\,u}{\sqrt{1-u^4}}, \quad \frac{dt}{du} = \frac{\sqrt{2}}{\sqrt{1-u^4}}\frac{1+u^4}{1-u^4}$$

i llavors

$$\frac{dt}{\sqrt{1+t^4}} = \sqrt{2}\frac{du}{\sqrt{1-u^4}}, \quad u \in [0,1] \tag{3.9}$$

Si tenim en compte (3.7), veiem que tenim

$$\int_0^r \frac{d\tilde{r}}{\sqrt{1-\tilde{r}^4}} = 2\int_0^u \frac{d\tilde{u}}{\sqrt{1-\tilde{u}^4}}, \quad u \in [0,1] \tag{3.10}$$

És a dir, acabem de trobar la construcció geomètrica per a duplicar una longitud d'arc donada de la lemniscata. Si ajuntem les dues substitucions (3.5) i (3.8), tenim

$$r = \frac{2u\sqrt{1-u^4}}{1+u^4} \tag{3.11}$$

Observem que les consideracions anteriors estan restringides al primer quadrant de la lemniscata. Això significa que l'arc que es pretengui duplicar seguint aquest procediment ha de ser tal que el punt de l'extrem de l'arc duplicat ha d'estar contingut al primer quadrant.

3.2.2 Teorema d'addició

A l'apartat anterior, la substitució (3.4) racionalitzava la integral (3.3) per l'expressió $\arcsin(r)$. Similarment al que ja s'ha vist, es pot introduir una reparametrització que permeti duplicar la longitud d'arc de la circumferència com s'ha fet pel cas de la lemniscata. Més concretament, si posem

$$r = 2u\sqrt{1-u^2} \tag{3.12}$$

obtenim

$$\int_0^r \frac{d\tilde{r}}{\sqrt{1-\tilde{r}^2}} = 2\int_0^u \frac{d\tilde{u}}{\sqrt{1-\tilde{u}^2}}, \quad u \in [0,1] \tag{3.13}$$

Aquest resultat també es pot comprovar immediatament a través de la substitució $u = sinx$, la qual cosa ens portaria a la relació trigonomètrica $sin(2x) = 2sinx\,cosx$. Aquesta identitat no és més que un cas particular del teorema d'addició trigonomètrica

$$\sin(x+y) = \sin x\, \cos y + \cos x\, \sin y \tag{3.14}$$

Aquesta darrera expressió es pot obtenir mitjançant les substitucions $u = \sin x \quad v = \sin y$, de manera que $\sin(x+y) = u\sqrt{1-v^2} + v\sqrt{1-u^2}$ i la generació de les funcions inverses és de la forma

$$\int_0^r \frac{d\tilde{u}}{\sqrt{1-\tilde{u}^2}} + \int_0^v \frac{d\tilde{v}}{\sqrt{1-\tilde{v}^2}} = \int_0^r \frac{d\tilde{r}}{\sqrt{1-\tilde{r}^2}}, \quad r = u\sqrt{1-v^2} + v\sqrt{1-u^2} \tag{3.15}$$

Cal tenir en compte que aquests raonaments estan considerant que u i v són prou petits com per a ser valors no-negatius (al primer quadrant).

La pregunta òbvia que ens plantegem en aquest punt és si existeix un teorema d'addició similar a (3.14) per a la integral lemniscàtica. La resposta, afortunadament, és positiva i l'enunciem en forma de teorema.

Teorema 3.2. *(Teorema d'addició real a la lemniscata) Sigui $r = \phi(s)$ com s'ha definit a (2.4) i siguin $u, v \in \mathbb{R}$. Aleshores,*

$$\phi(u+v) = \frac{\phi(u)\phi'(v) + \phi(v)\phi'(u)}{1 + \phi(u)^2\phi(v)^2} \tag{3.16}$$

Demostració. Sigui $g(x,y)$ una funció diferenciable a $\mathbb{R}^2$ i definim $h(u,v) = g\left(\frac{1}{2}(u+v), \frac{1}{2}(u-v)\right)$. Tenint en compte el canvi de variables $x(u,v) = \frac{1}{2}(u+v)$, $y(u,v) = \frac{1}{2}(u-v)$, podem aplicar la regla de la cadena de manera que

$$\frac{\partial h}{\partial v}(u,v) = \frac{\partial g}{\partial x}\left(x(u,v), y(u,v)\right)\frac{\partial x}{\partial v}(u,v) + \frac{\partial g}{\partial y}\left(x(u,v), y(u,v)\right)\frac{\partial y}{\partial v}(u,v)$$

$$= \frac{1}{2}\frac{\partial}{\partial x}\, g\left(\frac{1}{2}(u+v), \frac{1}{2}(u-v)\right) - \frac{1}{2}\frac{\partial}{\partial y}\, g\left(\frac{1}{2}(u+v), \frac{1}{2}(u-v)\right)$$

Volem veure que a $\mathbb{R}^2$, $g(x,y) = g(x+y,0) \iff \frac{\partial g}{\partial x} = \frac{\partial g}{\partial y}$.
Suposem que $g(x,y) = g(x+y,0), \forall x, y \in \mathbb{R}$. Llavors podem definir $f(x) = g(x,0)$. Clarament, f és una funció diferenciable i $g(x,y) = f(x+y)$. Per la regla de la cadena,

$$\frac{\partial g}{\partial x}(x,y) = f'(x+y) = \frac{\partial g}{\partial y}(x,y)$$

la qual cosa demostra que $\frac{\partial g}{\partial x} = \frac{\partial g}{\partial y}$.
Recíprocament, suposem que $\frac{\partial g}{\partial x} = \frac{\partial g}{\partial y}$ a $\mathbb{R}^2$. Aleshores, per tot $(u,v) \in \mathbb{R}^2$,

$$\frac{\partial h}{\partial v}(u,v) = \frac{1}{2}\frac{\partial}{\partial x}\, g\left(\frac{1}{2}(u+v), \frac{1}{2}(u-v)\right) - \frac{1}{2}\frac{\partial}{\partial y}\, g\left(\frac{1}{2}(u+v), \frac{1}{2}(u-v)\right) = 0$$

Això significa que, fixat $u_0 \in \mathbb{R}$, l'aplicació $v \mapsto h(u_0, v)$ té derivada nul·la, cosa que indica que és una constant $h(u_0,v) = h(u_0,0), \forall v \in \mathbb{R}$. I com que això es compleix per tot $u_0 \in \mathbb{R}$, és clar que $h(u,v) = h(u,0), \forall (u,v) \in \mathbb{R}^2$. Escrivim $f(u) = h(u,0)$, per tot $u \in \mathbb{R}$. Llavors f és diferenciable i $h(u,v) = f(u)$, per tot $(u,v) \in \mathbb{R}^2$. Per definició de h, això significa que

$$f(u) = g\left(\frac{1}{2}(u+v), \frac{1}{2}(u-v)\right), \quad \forall (u,v) \in \mathbb{R}^2$$

Podem triar $v = u$ de manera que

$$f(u) = g(u,0) = h(u,u) = h(u,0) = h(u,v) = g\left(\frac{1}{2}(u+v), \frac{1}{2}(u-v)\right)$$

és a dir,

$$g(u,0) = g\left(\frac{1}{2}(u+v), \frac{1}{2}(u-v)\right)$$

Per qualsevol parella $(x,y) \in \mathbb{R}^2$, existeix una única parella $(u,v) \in \mathbb{R}^2$ tal que $x = \frac{1}{2}(u+v)$, $y = \frac{1}{2}(u-v)$, donada per $u = x+y$, $v = x-y$. Per tant, la igualtat anterior implica que $g(x+y,0) = g(x,y), \forall (x,y) \in \mathbb{R}^2$.

Havent vist això, definim $g : \mathbb{R}^2 \to \mathbb{R}$ per

$$g(x,y) = \frac{\phi(x)\phi'(y) + \phi(y)\phi'(x)}{1 + \phi(x)^2\phi(y)^2} \tag{3.17}$$

La derivada parcial de g definida segons (3.17) respecte de x verifica

$$\left[1 + \phi(x)^2\phi(y)^2\right]^2 \frac{\partial g}{\partial x}(x,y) = \phi'(x)\phi'(y) + \phi(y)\phi''(x) + \phi'(x)\phi'(y)\phi(x)^2\phi(y)^2 +$$

$$+\phi(y)^3\phi(x)^2\phi''(x) - 2\phi(x)^2\phi(y)\phi'(x)\phi'(y) - 2\phi(x)\phi(y)^2\phi'(x)^2$$

Fent servir la proposició 3.1, $\phi'(x)^2 = 1 - \phi^4(x)$, i la seva expressió derivada, $\phi''(x) = -2\phi(x)^3$, podem simplificar l'expressió anterior a

$$\left[1 + \phi(x)^2\phi(y)^2\right] \frac{\partial g}{\partial x}(x,y) = \phi'(x)\phi'(y) - 2\phi(x)^3\phi(y) + \phi'(x)\phi'(y)\phi(x)^2\phi(y)^2 -$$

$$-2\phi(x)\phi^3(y) - 2\phi(x)^2\phi(y)^2\phi'(x)\phi'(y)$$

Notem que en aquesta expressió hi ha una simetria respecte de les variables x i y. Clarament $\left[1 + \phi(x)^2\phi(y)^2\right] \frac{\partial g}{\partial x}(x,y) = \left[1 + \phi(y)^2\phi(x)^2\right] \frac{\partial g}{\partial y}(x,y)$. Per tant, $\frac{\partial g}{\partial x} = \frac{\partial g}{\partial y}$ a $\mathbb{R}^2$. Com que hem vist que $\frac{\partial g}{\partial x} = \frac{\partial g}{\partial y}$ si, i només si, $g(x,y) = g(x+y,0)$, fent servir que $\phi(0) = 0$, $\phi'(0) = 1$ i l'expressió (3.17), tenim

$$\frac{\phi(x)\phi'(y) + \phi(y)\phi'(x)}{1 + \phi(x)^2\phi(y)^2} = \phi(x+y)$$

com volíem demostrar. □

Corol·lari 3.3 (Llei d'addició)**.** *Sigui*

$$s(u) = \int_0^u \frac{dx}{\sqrt{1-x^4}}$$

i siguin $u, v, r \in \mathbb{R}$*. Aleshores,*

$$s(u) + s(v) = s(r), \quad r = \frac{u\sqrt{1-v^4} + v\sqrt{1-u^4}}{1 + u^2v^2}$$

Demostració. És immediat del teorema 3.2. □

Aquest resultat ens permet afirmar que dos arcs lemniscàtics donats pels seus punts dels extrems poden ser sumats de manera geomètrica.

Com a conseqüència d'aquest resultat, i fent servir que ϕ és senar (3.1), és immediat veure que per a $u, v \in \mathbb{R}$

$$\phi(u - v) = \frac{\phi(u)\phi'(v) - \phi(v)\phi'(u)}{1 + \phi(u)^2\phi(v)^2} \tag{3.18}$$

Combinant (3.18) amb el teorema 3.2, trobem una identitat que ens serà molt útil:

$$\phi(u + v) + \phi(u - v) = \frac{2\phi(u)\phi'(v)}{1 + \phi(u)^2\phi(v)^2} \tag{3.19}$$

3.2.3 Multiplicació per enters

Imposant $u = v$ a (3.16), trobem que la duplicació de la longitud d'arc de la lemniscata ens proporciona la següent fórmula:

$$\phi(2x) = \frac{2\phi(x)\phi'(x)}{1 + \phi(x)^4} \tag{3.20}$$

Ara ens interessa generalitzar aquesta fórmula per a expressar $\phi(nx)$ en termes de $\phi(x)$ i $\phi'(x)$ per qualsevol $n \in \mathbb{Z}_+$.

Teorema 3.4. *Donat $n \in \mathbb{Z}_+$, existeixen polinomis coprimers $P_n(x), Q_n(x) \in \mathbb{Z}[x]$ tals que si n és senar,*

$$\phi(nx) = \phi(x)\frac{P_n(\phi^4(x))}{Q_n(\phi^4(x))}$$

i, si n és parell,

$$\phi(nx) = \phi(x)\phi'(x)\frac{P_n(\phi^4(x))}{Q_n(\phi^4(x))}$$

A més, $Q_n(0) = 1$.

Demostració. Demostrarem aquest teorema per inducció sobre n.
Per a $n = 1$, n'hi ha prou amb agafar $P_1(x) = Q_1(x) = 1$. Per a $n = 2$, fixem-nos que (3.20) es pot escriure trivialment com

$$\phi(2x) = \phi(x)\phi'(x)\frac{2}{1+\phi^4(x)}$$

de manera que el teorema es verifica prenent $P_2(x) = 2$ i $Q_2(x) = 1 + x$. Suposem ara, per hipòtesi d'inducció, que es verifica per a n i $n-1, n > 3$. Fem servir la identitat (3.19) amb $u = nx$ i $v = x$:

$$\phi((n+1)x) = -\phi((n-1)x) + \frac{2\phi(nx)\phi'(x)}{1+\phi(nx)^2\phi(x)^2} \tag{3.21}$$

Si n és parell, aleshores $n-1$ és senar. Aplicant la nostra hipòtesi d'inducció a (3.21), tenim

$$\phi((n+1)x) = -\left[\phi(x)\frac{P_{n-1}(\phi^4(x))}{Q_{n-1}(\phi^4(x))}\right] + \frac{2\left[\phi(x)\phi'(x)\frac{P_n(\phi^4(x))}{Q_n(\phi^4(x))}\right]\phi'(x)}{1+\left[\phi(x)\phi'(x)\frac{P_n(\phi^4(x))}{Q_n(\phi^4(x))}\right]^2\phi(x)^2} \tag{3.22}$$

Invoquem la relació $\phi'^2(x) = 1-\phi^4(x)$ vista a la proposició 3.1, de manera que l'expressió (3.22) se simplifica a

$$\phi((n+1)x) = \phi(x)\frac{P_{n+1}(\phi^4(x))}{Q_{n+1}(\phi^4(x))}$$

amb

$$P_{n+1}(x) = -P_{n-1}(x)\left[Q_n^2(x) + x(1-x)P_n^2(x)\right] + 2(1-x)P_n(x)Q_n(x)Q_{n-1}(x) \tag{3.23}$$

$$Q_{n+1}(x) = Q_{n-1}(x)\left[Q_n^2(x) + x(1-x)P_n^2(x)\right] \tag{3.24}$$

Si n és senar, aleshores $n-1$ és parell. Procedint anàlogament, tenim

$$\phi((n+1)x) = -\left[\phi(x)\phi'(x)\frac{P_{n-1}(\phi^4(x))}{Q_{n-1}(\phi^4(x))}\right] + \frac{2\left[\phi(x)\frac{P_n(\phi^4(x))}{Q_n(\phi^4(x))}\right]\phi'(x)}{1+\left[\phi(x)\frac{P_n(\phi^4(x))}{Q_n(\phi^4(x))}\right]^2\phi(x)^2} =$$

$$= \phi(x)\phi'(x)\left\{-\frac{P_{n-1}(\phi^4(x))}{Q_{n-1}(\phi^4(x))} + \frac{2\frac{P_n(\phi^4(x))}{Q_n(\phi^4(x))}}{1+\left[\phi(x)\frac{P_n(\phi^4(x))}{Q_n(\phi^4(x))}\right]^2\phi(x)^2}\right\} \tag{3.25}$$

Operant com abans, arribem a escriure

$$\phi((n+1)x) = \phi(x)\phi'(x)\frac{P_{n+1}(\phi^4(x))}{Q_{n+1}(\phi^4(x))}$$

amb

$$P_{n+1}(x) = -P_{n-1}(x)\left[Q_n^2(x) + xP_n^2(x)\right] + 2P_n(x)Q_n(x)Q_{n-1}(x) \tag{3.26}$$

$$Q_{n+1}(x) = Q_{n-1}(x)\left[Q_n^2(x) + xP_n^2(x)\right] \tag{3.27}$$

Així doncs, $P_{n+1}(x), Q_{n+1}(x) \in \mathbb{Z}[x]$ per inducció. Observem que $Q_{n+1}(0) = 1$ és conseqüència de la hipòtesi $Q_{n-1}(0) = Q_n(0) = 1$ tant a (3.24) com a (3.27). Finalment, si dividim $P_{n+1}(x)$ i $Q_{n+1}(x)$ entre el seu màxim comú divisor veiem que són coprimers a $\mathbb{Z}[x]$. □

Definició 3.5. *Anomenem polinomi de n-divisió el polinomi de* $\mathbb{Z}[x]$

$$D_n(x) := \begin{cases} xP_n(x^4), & n = 2k+1 \\ x(1-x^2)P_n(x^4), & n = 2k \end{cases}$$

Observació 3.6. La distància (polar) dels punts de n-divisió de la lemniscata són $\phi(m\frac{2\varpi}{n})$, $m \in \{0, ..., n-1\}$.

- Quan n és senar, la periodicitat de ϕ i el teorema 3.4 impliquen que

$$0 = \phi(m2\varpi) = \phi\left(nm\frac{2\varpi}{n}\right) = \phi\left(m\frac{2\varpi}{n}\right)\frac{P_n\left(\phi(m\frac{2\varpi}{n})^4\right)}{Q_n(\phi\left(m\frac{2\varpi}{n}\right)^4)}$$

  de manera que les distàncies $\phi\left(m\frac{2\varpi}{n}\right)$ anul·len el polinomi de n-divisió en el cas senar $D_n(x) = xP_n(x^4)$. Més endavant veurem que $\mathrm{gr}(P_n(x)) = \frac{n-1}{4}$, amb $n \in \mathbb{Z}_+$. Llavors, $\mathrm{gr}(D_n(x)) = \mathrm{gr}(xP_n(x^4)) = \mathrm{gr}(x) + \mathrm{gr}(P_n(x^4)) = 1 + 4\frac{n-1}{4} = n$. Consegüentment, sabem que les distàncies $\phi\left(m\frac{2\varpi}{n}\right)$ amb $m \in \{0, ..., n-1\}$ són totes les arrels que té el polinomi de n-divisió $D_n(x)$.

- Anàlogament, quan n és parell,

$$0 = \phi(m2\varpi) = \phi\left(nm\frac{2\varpi}{n}\right) = \phi\left(m\frac{2\varpi}{n}\right)\phi'\left(m\frac{2\varpi}{n}\right)\frac{P_n\left(\phi(m\frac{2\varpi}{n})^4\right)}{Q_n(\phi\left(m\frac{2\varpi}{n}\right)^4)}$$

  Així doncs, els valors $\phi\left(m\frac{2\varpi}{n}\right)$ anul·len la funció $x\sqrt{1-x^4}P_n(x^4)$. Les solucions reals del factor $x\sqrt{1-x^4}$ són $\{0, \pm 1\}$. Per tant, en particular podem afirmar que les arrels $\phi\left(m\frac{2\varpi}{n}\right)$ anul·len el polinomi $x(1-x^2)P_n(x^4)$, la qual cosa dota de sentit la definició de polinomi de n-divisió pel cas parell.

4 La funció lemniscàtica complexa

L'estructura d'aquesta secció està inspirada en [4]. S'hi incorporen resultats interessants presentats a [11] i [14]. Amb l'objectiu de verificar l'adequació i la precisió en qüestions d'anàlisi complexa, s'ha consultat [15] i [16].

4.1 Caracterització de ϕ al pla complex

Vegem ara com podem estendre la funció ϕ sobre el cos $\mathbb{C}$. Considerem $\phi(iy)$ amb $y \in \mathbb{R}$. Sabem que $r = \phi(y)$ és la funció inversa de $y = \int_0^r (1-t^4)^{-1/2} dt$. Per tant, aplicant el canvi de variables $t = iu$,

$$\int_0^{ir} \frac{dt}{\sqrt{1-t^4}} = i \int_0^r \frac{du}{\sqrt{1-u^4}} = iy$$

Per tant, podem definir

$$\phi(iy) = i\phi(y) \tag{4.1}$$

Així doncs, podem aplicar la llei d'addició del Corol·lari 3.3 per a definir $\phi(x+iy)$ com

$$\phi(x+iy) = \frac{\phi(x)\phi'(iy) + \phi(iy)\phi'(x)}{1+\phi(x)^2\phi(iy)^2} \tag{4.2}$$

Veurem que $\phi(z)$ és una funció analítica. Així, fent servir la proposició 3.1 i (4.1), tenim

$$\phi'(iy) = \sqrt{1-\phi(iy)^4} = \sqrt{1-(i\phi(y))^4} = \sqrt{1+\phi^4(y)}$$

és a dir,

$$\phi'(iy) = \phi'(y) \tag{4.3}$$

Si incloem les relacions (4.1) i (4.3) a (4.2), podem *definir* $\phi(z)$, $z = x+iy \in \mathbb{C}$ $(x, y \in \mathbb{R})$, com

$$\phi(z) = \phi(x+iy) = \frac{\phi(x)\phi'(y) + i\phi(y)\phi'(x)}{1-\phi(x)^2\phi(y)^2} \tag{4.4}$$

Sobre $\mathbb{R}$, $\phi(x)$ és periòdica i està definida a tot arreu. En canvi, sobre $\mathbb{C}$, veurem que $\phi(z)$ és doblement periòdica i que té pols (notem que el denominador de (4.4) pot anul·lar-se). En aquesta secció aprofundirem en les conseqüències que té l'extensió de ϕ al pla complex. Algunes propietats de $\phi(z)$ jugaran un paper crucial en les futures seccions.

Proposició 4.1. *La funció $\phi(z)$ verifica les següents propietats:*

(a) $\phi(z)$ és analítica $\forall z \neq (a+bi)\frac{\varpi}{2}$, amb $a, b \in \mathbb{Z}$ senars.

(b) La llei d'addició

$$\phi(z+\omega) = \frac{\phi(z)\phi'(\omega) + \phi(\omega)\phi'(z)}{1+\phi^2(z)\phi^2(\omega)}$$

es compleix $\forall z, \omega \in \mathbb{C}$ allà on ambdues bandes de l'equació estan definides.

(c) $\forall z \in \mathbb{C}$ i $a, b \in \mathbb{Z}$, tenim

$$\phi(z + a\varpi + b\varpi i) = (-1)^{a+b}\phi(z)$$

Demostració. Sabem que $\phi(z)$ està definida sempre que $1-\phi^2(x)\phi^2(y)\neq 0$. La interpretació en distància polar de $\phi(x)$ indica que $\phi^2(x)\leq 1, \forall x\in\mathbb{R}$, amb la igualtat si i només si x és un múltiple senar de $\frac{\varpi}{2}$. És per això que $\phi(z)$ està definida a la regió $\Omega=\{z\in\mathbb{C}|z\neq(a+bi)\frac{\varpi}{2}$, amb $a,b\in\mathbb{Z}$ senars$\}$.
Siguin $u(x,y)$ i $v(x,y)$ les parts reals i imaginàries de $\phi(z)$ respectivament, i.e. $\phi(z)=\phi(x+iy)=u(x,y)+iv(x,y)$. És clar que $u(x,y)$ i $v(x,y)$ són diferenciables a Ω com a funcions de x,y ja que $\phi(x)$ i $\phi(y)$ són infinitament diferenciables a $\mathbb{R}$. Fent servir que $\phi^2(x)=1-\phi^4(z)$, per $x\in\mathbb{R}$, és immediat adonar-se que $u(x,y)$ i $v(x,y)$ verifiquen les equacions de Cauchy-Riemann

$$\frac{\partial u}{\partial x}=\frac{\partial v}{\partial y},\qquad \frac{\partial u}{\partial y}=-\frac{\partial v}{\partial x}$$

Així doncs, $\phi(z)$ és analítica a Ω.

Demostrem ara la propietat (b). Siguin $z,\omega\in\mathbb{Z}$ i definim

$$f(z,\omega)=\frac{\phi(z)\phi'(\omega)+\phi(\omega)\phi'(z)}{1+\phi^2(z)\phi^2(\omega)}$$

Fixem $x_0\in\mathbb{R}$. Notem que $\phi(x_0+\omega)$ i $f(x_0,\omega)$ són analítiques a ω i que coincideixen quan $\omega\in\mathbb{R}$ per la regla d'addició. En virtut del teorema de la identitat per a funcions analítiques, $\phi(x_0,\omega)=f(x_0,\omega)$ per totes les ω on ambdues estan definides. Anàlogament, per a $\omega_0\in\mathbb{C}$ fixat, $\phi(z+\omega_0)$ i $f(z,\omega_0)$ són analítiques a z i coincideixen quan $z\in\mathbb{R}$ sempre que ambdues estiguin definides. De nou, $\phi(z+\omega_0)=f(z,\omega_0)$ per totes les z tal que ambdues estan definides. Com que la tria de ω_0 és arbitrària, això demostra (b).

Finalment, demostrem (c). Sabem que $\phi(0)=0,\phi(\frac{\varpi}{2})=1,\phi(\varpi)=0,\phi(\frac{3\varpi}{2})=-1$ i que $\phi'(0)=1,\phi'(\frac{\varpi}{2})=0,\phi'(\varpi)=-1,\phi'(\frac{3\varpi}{2})=0$. Com que ϕ i ϕ' són 2ϖ-periòdiques a $\mathbb{R}$, això implica que

$$\phi(n\varpi)=\phi(n\varpi i)=0,\quad \phi'(n\varpi)=\phi'(n\varpi i)=(-1)^n$$

per a $n\in\mathbb{Z}$. Fent servir la llei d'addició, és immediat veure que

$$\phi(z+a\varpi)=(-1)^a\phi(z),\quad \phi'(z+b\varpi i)=(-1)^b\phi(z)$$

amb $a,b\in\mathbb{Z}$. Així doncs, $\phi(z+a\varpi+b\varpi i)=(-1)^{a+b}\phi(z)$, com volíem demostrar. □

La tercera propietat de la proposició 4.1 indica que ϕ és una funció doblement periòdica:

$$\phi(z)=\phi(z+(1+i)\varpi)=\phi(z+(1-i)\varpi) \tag{4.5}$$

Fixem-nos que els períodes $(1+i)\varpi$ i $(1-i)\varpi$ són linealment independents sobre $\mathbb{R}$. Aleshores definim la xarxa periòdica de ϕ com

$$\mathcal{L}=\{(a+bi)\varpi\,|\,a+b\equiv 0 \pmod 2\}=\{a(1+i)\varpi+b(1-i)\varpi\,|\,a,b\in\mathbb{Z}\} \tag{4.6}$$

La Figura 2 presenta punts complexes sobre la xarxa $\mathcal{L}$. La doble periodicitat de ϕ indica que, una vegada conegut el valor de $\phi(z)$ per tots els valors de z en un dels quadrats inclinats $\{(a+x)(1+i)\varpi+(b+y)(1-i)\varpi|\,x,y\in\mathbb{R},\,0\leq x,y<1\}$, coneixem el seu valor $\forall\, z\in\mathbb{C}$.

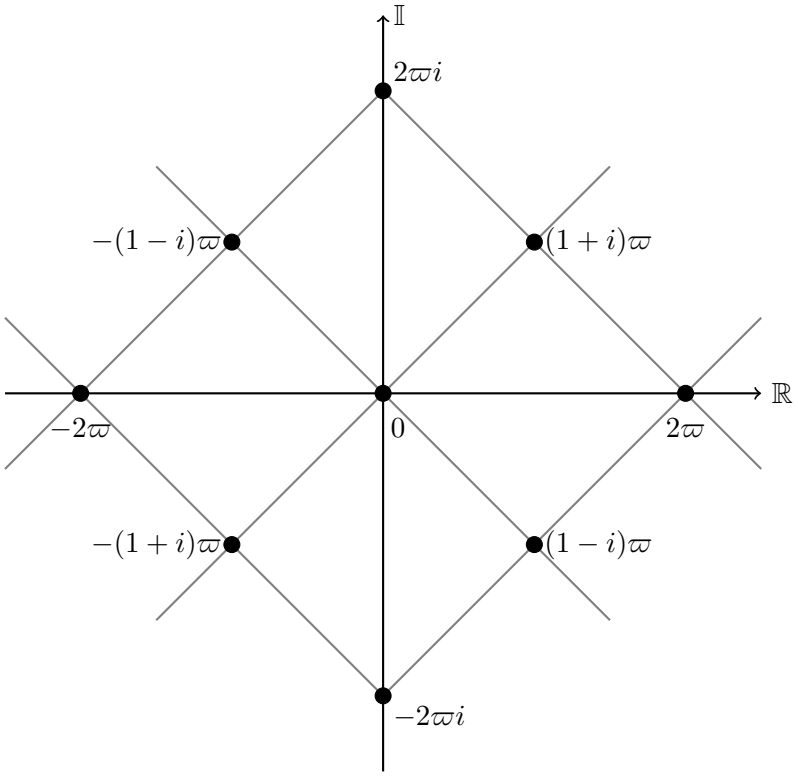

Figura 2: Xarxa periòdica $\mathcal{L}$ de ϕ.

Teorema 4.2. *$\phi(z)$ és meromorfa a $\mathbb{C}$ amb els següents zeros i pols:*

(i) Els zeros són tots simples i són a $z = (a+bi)\varpi$, per $a, b \in \mathbb{Z}$.

(ii) Els pols són tots simples i són a $z = (a+bi)\frac{\varpi}{2}$, per $a, b \in \mathbb{Z}$ senars.

Demostració. Com que $\phi(0) = 0$ i $\phi'(0) = 1$, per la propietat (c) de la proposició anterior, sabem que $\phi((a+bi)\varpi) = 0, \forall a, b \in \mathbb{Z}$. Fent servir la llei d'addició i els valors coneguts de ϕ, tenim

$$\phi\left(z + \frac{\varpi}{2}\right) = \frac{\phi(z)\phi'\left(\frac{\varpi}{2}\right) + \phi\left(\frac{\varpi}{2}\right)\phi'(z)}{1 + \phi^2(z)\phi^2\left(\frac{\varpi}{2}\right)} = \frac{\phi'(z)}{1+\phi^2(z)}$$

Similarment, trobem

$$\phi\left(z \pm \frac{\varpi}{2}i\right) = \pm i\frac{\phi'(z)}{1-\phi^2(z)}$$

Si multipliquem ambdues equacions arribem a

$$\phi\left(z + \frac{\varpi}{2}\right)\phi\left(z \pm \frac{\varpi}{2}i\right) = \left(\frac{\phi'(z)}{1+\phi^2(z)}\right)\left(\pm i\frac{\phi'(z)}{1-\phi^2(z)}\right) = \pm i\frac{\phi'^2(z)}{1-\phi^4(z)} = \pm i$$

Avaluant aquest producte a $z + \frac{\varpi}{2}$ i fent servir $\phi(z+\varpi) = -\phi(z)$, obtenim

$$\phi(z)\phi\left(z + (1 \pm i)\frac{\varpi}{2}\right) = \mp i \tag{4.7}$$

Ara suposem que $\phi(z_0) = 0$. Aleshores, per la relació anterior, $\phi\left(z_0 + (1 \pm i)\frac{\varpi}{2}\right)$ no està ben definit. Així doncs, per la propietat (a) de la proposició anterior,

$$z_0 + (1 \pm i)\frac{\varpi}{2} = (a+bi)\frac{\varpi}{2}$$

amb $a, b \in \mathbb{Z}$ senars. Així doncs, z_0 és un zero simple de la forma que volíem.

Analitzem ara els pols de ϕ.

$$\phi(z)\phi\left(z + (1 \pm i)\frac{\varpi}{2}\right) = \mp i \Rightarrow \phi\left(z + (1 \pm i)\frac{\varpi}{2}\right) = \frac{\mp i}{\phi(z)}$$

Com que $\phi(0) = 0$, veiem que ϕ té pols simples a $z = (1+i)\frac{\varpi}{2}$. Fent servir la doble periodicitat de ϕ, concloem que ϕ té pols simples a $(a+bi)\frac{\varpi}{2}$, per a $a, b \in \mathbb{Z}$ senars. I no n'hi ha més perquè aquestes són les úniques possibles singularitats de ϕ d'acord amb la proposició anterior. □

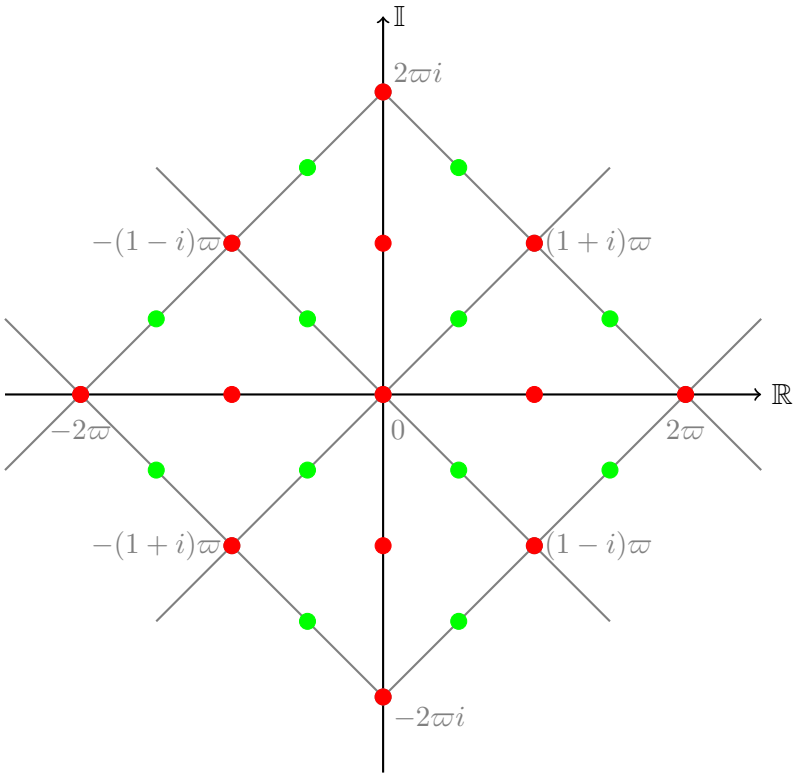

Figura 3: Distribució dels zeros i pols de $\phi(z)$. La figura presenta la xarxa periòdica $\mathcal{L}$ de fons en gris amb alguns valors de la xarxa. Els punts vermells representen els zeros de $\phi(z)$ i els punts verds simbolitzen els pols de $\phi(z)$.

Teorema 4.3. *Sigui $\omega_0 \in \mathbb{C}$ fixat. Aleshores l'equació $\phi(z) = \omega_0$ té una solució $z_0 \in \mathbb{C}$. A més, si z_0 és una solució, aleshores totes les solucions són de la forma*

$$z = (-1)^{a+b} z_0 + (a + bi)\varpi, \quad a, b \in \mathbb{Z}$$

Demostració. Sigui $f(x)$ analítica en una regió $\Omega \subset \mathbb{C}$ i sigui $\gamma \subset \Omega$ una corba tancada simple orientada antihoràriament. Pel principi de l'argument sabem que, si $f(x)$ no té zeros ni pols a γ, aleshores

$$\frac{1}{2\pi i}\int_\gamma \frac{f'(z)}{f(z)}dz = Z - P$$

on Z és el nombre de zeros de $f(z)$ en la regió que tanca la corba C i P és el nombre de pols de $f(z)$ dins la mateixa regió (comptant-ne la multiplicitat en ambdós casos). Posem $f(z) = \phi(z) - \omega_0$. Sabem que $f(z)$ té els mateixos pols que ϕ, que són $(a+bi)\frac{\varpi}{2}$ amb $a, b \in \mathbb{Z}$ senars pel teorema 4.2. Això significa que no podem fer servir els quadrats inclinats de la xarxa periòdica (4.6) per a definir γ. Malgrat això, com que els zeros de f són aïllats, podem aplicar una translació d'un d'aquests quadrats de manera que $f(z)$ no contingui ni pols ni zeros sobre la frontera del quadrat. Per simetria, la translació més petita per aconseguir això fa que a l'interior del quadrat hi hagi exactament dos pols, i.e $P = 2$. Per tant, podem definir γ com el perímetre d'aquest quadrat desplaçat.
Atès que $f(z) = \phi(z) - \omega_0$ té períodes $(1 \pm i)\varpi$, sabem que $f'(z)$ i $f'(z)/f(z)$ també. Els costats oposats del quadrat difereixen en $(1 \pm i)\varpi$, així que $f'(z)/f(z)$ pren el mateix valor als costats oposats. Això fa que

$$Z - 2 = Z - P = \frac{1}{2\pi i} \int_\gamma \frac{f'(z)}{f(z)} dz = 0$$

Clarament, doncs, a dins de γ, o bé $f(z) = \phi(z) - \omega_0$ té dos zeros simples o bé té un zero doble. Recordem que $\phi(z) = \omega_0$ ha de tenir una solució z_0 dins de γ. A partir d'això i de la proposició 4.1, per a $a, b \in \mathbb{Z}$, tenim una solució addicional

$$\phi((-1)^{a+b} z_0 + (a+bi)\varpi) = (-1)^{a+b} \phi((-1)^{a+b} z_0) = \phi(z_0) = \omega_0$$

on la segona igualtat es verifica perquè ϕ és senar per (3.1). Només cal veure, doncs, que no hi ha cap més solució possible. Sigui γ^* la regió que tanca γ incloent-hi la frontera. Si traslladem γ^* als elements de la xarxa periòdica $\mathcal{L}$ (4.6), podem recobrir tot el pla complex. En particular, $-z_0 + \varpi$ té un traslladat per $\mathcal{L}$ que rau a l'interior de γ^*, i.e. existeixen $a, b \in \mathbb{Z}$ amb $a + b$ parell tals que

$$-z_0 + \varpi + (a+bi)\varpi = (-1)^{a+b+1} z_0 + ((a+1) + bi)\varpi \tag{4.8}$$

cau dins la corba γ. Si (4.8) difereix de z_0, llavors ja hem trobat tots els zeros de $f(z) = \phi(z) - \omega_0$ dins de γ. Com que tot altre zero és una translació per $\mathcal{L}$ d'un zero dins de γ, se segueix que totes les solucions de $\phi(z) = \omega_0$ tenen la forma desitjada.
Finalment, si (4.8) coincideix amb z_0, és fàcil de comprovar que

$$z_0 = (m + ni)\frac{\varpi}{2}, \quad m, n \in \mathbb{Z}$$

amb $m + n$ senar. Això implica que $f'(z_0) = \phi'(z_0) = \phi'\left((m+ni)\frac{\varpi}{2}\right) = 0$. Pel que hem demostrat, doncs, z_0 és l'únic zero de $f(z)$ dins de γ. Com abans, concloem que les solucions són de la forma desitjada. □

4.2 Multiplicació complexa

A la Secció 3 s'han definit unes fórmules de multiplicació (3.4) per a $\phi(nx)$, amb $x \in \mathbb{R}$ i $n \in \mathbb{Z}_+$. Ara ens interessa estendre aquesta noció per a $\phi(nz)$, $z \in \mathbb{C}$. Sabem que $\phi(iz) = i\phi(z)$ vist a (4.1). Per tant, a part de multiplicar per $n \in \mathbb{Z}_+$, també podem multiplicar per i. Combinant això amb la llei d'addició, podrem trobar les fórmules per $\phi((n+im)z) = \phi(\beta z)$, on $\beta = n + im \in \mathbb{Z}[i]$ és un enter gaussià qualsevol. En altres paraules, $\phi(z)$ té multiplicació complexa per $\mathbb{Z}[i]$.

Exemple 4.4. Fem servir (4.4) i que ϕ és senar (3.1) i $\phi(iz) = i\phi(z)$ (4.1), de manera que

$$\phi((1+i)z) = \frac{\phi(z)\phi'(iz) + i\phi(z)\phi'(z)}{1-\phi(z)^4}$$

Usant $\phi'(iz) = \phi'(z)$ de (4.3), ens queda

$$\phi((1+i)z) = \phi(z)\phi'(z)\frac{1+i}{1-\phi(z)^4} \tag{4.9}$$

Podem raonar anàlogament per a $\phi((1-i)z)$ i trobem

$$\phi((1-i)z) = \phi(z)\phi'(z)\frac{1-i}{1-\phi(z)^4} \tag{4.10}$$

4.2.1 L'anell d'enters de Gauss $\mathbb{Z}[i]$

Definició 4.5. *Definim l'anell d'enters de Gauss com* $\mathbb{Z}[i] = \{a+bi \,|\, a,b \in \mathbb{Z}\}$.

Observació 4.6. Les unitats de $\mathbb{Z}[i]$ formen el grup $\mathbb{Z}[i]^* = \{i^\epsilon \,|\, \epsilon = 0,1,2,3\}$.

Definició 4.7. *Diem que* $\alpha, \beta \in \mathbb{Z}[i]$ *són associats si* $\alpha = i^\epsilon\beta$, *per algun* $i^\epsilon \in \mathbb{Z}[i]^*$.

Definició 4.8. *Sigui* $\alpha \in \mathbb{Z}[i]$ *un element no nul i no unitat. Diem que* α *és primer si* $\alpha|\beta\gamma \Rightarrow \alpha|\beta$ *o* $\alpha|\gamma$.

Observació 4.9. $\mathbb{Z}[i]$ és un domini de factorització única i tot element primer de $\mathbb{Z}[i]$ divideix un element primer de $\mathbb{Z}$. En particular,

- $2 = (1+i)(1-i)$, on $1+i$ i $1-i$ són primers associats a $\mathbb{Z}[i]$.
- Quan $p \equiv 3 \pmod 4$ és primer a $\mathbb{Z}$, aleshores p també és primer a $\mathbb{Z}[i]$.
- Quan $p \equiv 1 \pmod 4$ és primer a $\mathbb{Z}$, llavors existeixen $a, b \in \mathbb{Z}$ tals que $p = a^2+b^2 = (a+bi)(a-bi)$, on $a+bi$ i $a-bi$ són primers no associats a $\mathbb{Z}[i]$.

Definició 4.10. *Siguin* $\beta, \eta \in \mathbb{Z}[i]$ *tals que les seves factoritzacions en primers* p_m *de* $\mathbb{Z}[i]$ *són*

$$\beta = i^k \prod_m p_m^{\nu_m}\,, \qquad \eta = i^j \prod_m p_m^{\mu_m}$$

amb $\nu_m, \mu_m, j, k, m \in \mathbb{N}$. *Aleshores definim el màxim comú divisor entre* β *i* η *com*

$$mcd(\beta,\eta) = \prod_m p_m^{\lambda_m} \in \mathbb{Z}[i]\,, \quad \lambda_m = min\{\nu_m, \mu_m\}$$

Definició 4.11. *Diem que un element* $\beta \in \mathbb{Z}[i]$ *és senar si és coprimer a* $1+i$.

Observació 4.12. Són equivalents:

(i) $\beta \in \mathbb{Z}[i]$ senar

(ii) $\beta = a+ib$, amb $a, b \in \mathbb{Z}$ tals que $a+b$ és senar

(iii) $\beta \equiv i^\epsilon \pmod{2(1+i)}$, amb $\epsilon \in \{0,1,2,3\}$

Demostració. Vegem $(i) \iff (ii)$. Suposem que $\beta = a + ib$ és parell, és a dir que admet la factorització $a + bi = (m + ni)(1 + i)$, per alguns $m, n \in \mathbb{Z}$. Aleshores, $a + bi = m + ni + mi - n = (m - n) + (m + n)i$, la qual cosa implica que $a = m - n$ i que $b = m + n$. Per tant, $a + b = 2m$ és parell. Per a veure la implicació contrària, es pot resseguir el raonament anterior a la inversa.
Demostrem ara $(i) \iff (iii)$. Comencem estudiant quines són les classes de la congruència $\mathbb{Z}[i]/2(1 + i)\mathbb{Z}[i]$ sobre els enters de Gauss. Suposem $\beta \equiv \beta' \pmod{2(1+i)}$. Aleshores

$$\beta - \beta' = (a + bi)(2 + 2i) = 2(a - b) + 2(a + b)i, \quad a, b \in \mathbb{Z} \tag{4.11}$$

Sabem que al mòdul $2(1+i)$, existeixen vuit classes possibles: $\{\overline{0}, \overline{1}, \overline{i}, \overline{-1}, \overline{-i}, \overline{1+i}, \overline{1-i}, \overline{2}\}$. Com que, en vista de l'equivalència $(i) \iff (ii)$, l'única manera que tenim per tal que β sigui senar és tenint β' també senar per (4.11), les úniques classes que podem tenir són $\overline{1}, \overline{i}, \overline{-1}$ i $\overline{-i}$, és a dir, $\beta \equiv i^\epsilon \pmod{2(1+i)}$, amb $\epsilon \in \{0, 1, 2, 3\}$. □

Definició 4.13. *Diem que $\beta \in \mathbb{Z}[i]$ senar està <u>normalitzat</u> si $\beta \equiv 1 \pmod{2(1+i)}$.*

Lema 4.14. *Sigui $\beta \in \mathbb{Z}[i]$ senar. Aleshores el conjunt*

$$R_\beta = \{\phi(z) | z \in \mathbb{C}, \phi(\beta z) = 0\}$$

té exactament $N(\beta)$ elements i està format per tots els nombres complexos de la forma $\phi\left(\alpha\frac{\varpi}{\beta}\right)$, amb $\alpha \in \mathbb{Z}[i]$ senar.

Demostració. En primer lloc, observem que si $\alpha \in \mathbb{Z}[i]$ és senar, llavors $\phi\left(\alpha\frac{\varpi}{\beta}\right) \in R_\beta$, ja que $\phi\left(\beta\alpha\frac{\varpi}{\beta}\right) = \phi(\alpha\varpi) = 0$ pel teorema 4.2. En l'altre sentit, suposem $\phi(\beta z) = 0$. Pel teorema 4.2, $\beta z = (a + bi)\varpi$, per a $a, b \in \mathbb{Z}$. Sigui $\alpha = a + bi \in \mathbb{Z}[i]$. Aleshores $z = \alpha\frac{\varpi}{\beta}$, de manera que $\phi(z) = \phi\left(\alpha\frac{\varpi}{\beta}\right)$. Si α és senar, ja ho tenim. Si α és parell, llavors $\beta - \alpha$ és senar. Fent servir que $\phi(\varpi - z) = \phi(z)$, obtenim

$$\phi\left((\beta - \alpha)\frac{\varpi}{\beta}\right) = \phi\left(\varpi - \alpha\frac{\varpi}{\beta}\right) = \phi\left(\alpha\frac{\varpi}{\beta}\right)$$

Això demostra que els elements de R_β són de la forma indicada. Ara ens falta determinar la mida de R_β. Fixem $\phi\left(\alpha\frac{\varpi}{\beta}\right)$, per a $\alpha \in \mathbb{Z}[i]$ senar. Afirmem que α és únic mòdul $\beta\mathbb{Z}[i]$. Per a veure'n el perquè, suposem que existeixen $\alpha, \tilde{\alpha} \in \mathbb{Z}[i]$ senars tals que

$$\phi\left(\alpha\frac{\varpi}{\beta}\right) = \phi\left(\tilde{\alpha}\frac{\varpi}{\beta}\right)$$

Pel teorema 4.3, existeix $a + bi \in \mathbb{Z}[i]$ tal que

$$\tilde{\alpha}\frac{\varpi}{\beta} = (-1)^{a+b}\alpha + (a + bi)\beta$$

Com que $\alpha, \tilde{\alpha}$ i β són senars, $a + bi$ és parell. Aleshores $(-1)^{a+b} = 1$ i, d'aquí,

$$\tilde{\alpha} = \alpha + (a + bi)\beta$$

de manera que α i $\tilde{\alpha}$ representen el mateix element a $\mathbb{Z}[i]/\beta\mathbb{Z}[i]$. Com que cada classe de $\mathbb{Z}[i]/\beta\mathbb{Z}[i]$ es pot representar amb un enter gaussià senar (per qualsevol α, o bé α o bé $\alpha + \beta$ és senar), de manera que

$$|R_\beta| = |\mathbb{Z}[i]/\beta\mathbb{Z}[i]|$$

Només ens falta veure, doncs, que $|\mathbb{Z}[i]/\beta\mathbb{Z}[i]| = N(\beta)$. Sigui $\beta = m + ni = q(p_1 + p_2 i)$, on $q = mcd(m, n)$ i $mcd(p_1, p_2) = 1$. Agafem $r_1, r_2 \in \mathbb{Z}$ tals que $p_1 r_2 - p_2 r_1 = 1$. Considerem l'aplicació $\psi : \mathbb{Z}[i] \mapsto \mathbb{Z} \oplus \mathbb{Z}$ definida per $\psi(\mu+\nu i) = \mu(r_2, -p_2)+\nu(-r_1, p_1) = (\mu r_2 - \nu r_1, -\mu p_2 + \nu p_1)$. Volem veure que ψ és un isomorfisme de grups amb la suma. És immediat comprovar que ψ és un morfisme de grups ben definit. Vegem que és una aplicació injectiva. Siguin $\mu + \nu i, \tilde{\mu} + \tilde{\nu} i \in \mathbb{Z}[i]$ tals que $\psi(\mu + \nu i) = \psi(\tilde{\mu} + \tilde{\nu})$. Llavors,

$$\left.\begin{array}{c} \mu r_2 - \nu r_1 = \tilde{\mu} r_2 - \tilde{\nu} r_1 \\ -\mu p_2 + \nu p_1 = -\tilde{\mu} p_2 + \tilde{\nu} p_1 \end{array}\right\} \Rightarrow \left.\begin{array}{c} (\mu - \tilde{\mu}) r_2 = (\nu - \tilde{\nu}) r_1 \\ (\tilde{\mu} - \mu) p_2 = (\tilde{\nu} - \nu) p_1 \end{array}\right\}$$

Per tant, $(\mu - \tilde{\mu})(\tilde{\nu} - \nu) p_1 r_2 = (\tilde{\mu} - \mu)(\nu - \tilde{\nu}) p_2 r_1$. Si $\mu \neq \tilde{\mu}$ i $\nu \neq \tilde{\nu}$, llavors $p_1 r_2 = p_2 r_1 \equiv p_1 r_2 - p_2 r_1 = 0$, la qual cosa és una contradicció. Per tant, l'única situació possible és que $\mu = \tilde{\mu}$ i $\nu = \tilde{\nu}$. Del sistema anterior, observem que el fet que només que una de les dues igualtats ja es compleixi implica que l'altra també ho fa. Així doncs, ψ és injectiva. Trivialment, ψ és exhaustiva. Per la qual cosa, tenim que ψ és bijectiva.
Havent vist això, fixem-nos que $\psi(\beta) = \psi(m+ni) = q\psi(p_1+p_2 i) = q(p_1 r_2 - p_2 r_1, -p_1 p_2 + p_2 p_1) = q(1, 0) = (q, 0)$ i que $\psi(i\beta) = \psi(-n + mi) = q\psi(-p_2, p_1) = q(-p_2 r_2 - p_1 r_1, p_2^2 + p_1^2) = (-q(p_1 r_1 + p_2 r_2), q(p_1^2 + p_2^2))$. Per tant, ψ envia $\beta\mathbb{Z}[i] \subset \mathbb{Z}[i]$ al subgrup

$$q\mathbb{Z} \oplus q(p_1^2 + p_2^2)\mathbb{Z} \subset \mathbb{Z} \oplus \mathbb{Z}$$

Ja que ψ és un isomorfisme,

$$|\mathbb{Z}[i]/\beta\mathbb{Z}[i]| \cong |(\mathbb{Z} \oplus \mathbb{Z})/q\mathbb{Z} \oplus q(p_1^2 + p_2^2)\mathbb{Z}| = q^2(p_1^2 + p_2^2) = N(\beta) \tag{4.12}$$

□

Lema 4.15. *Sigui α un element primer de $\mathbb{Z}[i]$ i denotem per N_α la seva norma. Aleshores*

$$\mathbb{Z}[i]/\alpha\mathbb{Z}[i] \cong \mathbb{F}_{N_\alpha}$$

Demostració. Com α és primer, el quocient $\mathbb{Z}[i]/\alpha\mathbb{Z}[i]$ és un domini d'integritat. Ara, per (4.12) sabem que el quocient té N_α elements, la qual cosa indica que és finit. A més, sabem que tot domini d'integritat finit és cos. Això demostra, doncs, el lema en qüestió.

□

Observació 4.16. Notem que si $\beta \in \mathbb{Z}[i]$ és no nul i $\mathcal{L} = \mathbb{Z}(1+i)\varpi + \mathbb{Z}(1-i)\varpi$, aleshores

$$\frac{1}{\beta}\mathcal{L}/\mathcal{L} \cong \mathbb{Z}[i]/\beta\mathbb{Z}[i]$$

com a $\mathbb{Z}[i]$-mòduls.

4.2.2 Polinomis de β-divisió

Definició 4.17. *Diem que $\delta \in \frac{1}{\beta}\mathcal{L}$ és un β-generador de torsió si $[\delta] \in \frac{1}{\beta}\mathcal{L}/\mathcal{L}$ genera $\frac{1}{\beta}\mathcal{L}/\mathcal{L}$ com a $\mathbb{Z}[i]$-mòdul, és a dir, si per tot $[x] \in \frac{1}{\beta}\mathcal{L}/\mathcal{L}$ existeix $a \in \mathbb{Z}[i]$ tal que $[x] = a[\delta]$.*

Observació 4.18. (a) Per l'isomorfisme de l'observació 4.16, si δ és un β-generador de torsió, llavors es compleix que $a[\delta] = a'[\delta] \iff \beta$ divideix $(a' - a)$.

(b) Qualssevol dos β-generadors de torsió $\delta, \delta' \in \frac{1}{\beta}\mathcal{L}$ satisfan $\delta \equiv \alpha\delta' \pmod{\mathcal{L}}$ per algun $[\alpha] \in (\mathbb{Z}[i]/\beta\mathbb{Z}[i])^*$.

Demostració. La primera observació és trivial. Demostrem la segona. Com que $\delta, \delta' \in \frac{1}{\beta}\mathcal{L}$ són β-generadors de torsió diferents, existeixen $a, a' \in \mathbb{Z}[i]$ tals que $[\delta'] = a[\delta]$ i $[\delta] = a'[\delta']$. Això implica $[\delta] = a'a[\delta]$ i, per l'observació (a), sabem que β divideix $(1 - a'a)$, la qual cosa implica que a' i a són unitats de $\mathbb{Z}[i]/\beta\mathbb{Z}[i]$. □

Notació 1. *Denotem per δ_β el β-generador de torsió definit com $\delta_\beta = \frac{1+i}{\beta}\varpi$.*

Teorema 4.19. *Sigui $\beta \in \mathbb{Z}[i]$ senar. Aleshores existeixen polinomis coprimers $P_\beta(x), Q_\beta(x) \in \mathbb{Z}[i][x]$, $\epsilon \in \{0,1,2,3\}$ tals que*

(1) $\forall z \in \mathbb{C}$, es verifica

$$\phi(\beta z) = i^\epsilon \phi(z)^4 \frac{P_\beta(\phi(z)^4)}{Q_\beta(\phi(z)^4)}$$

(2) $\beta \equiv i^\epsilon \pmod{2(1+i)}$

(3) $P_\beta(x), Q_\beta(x)$ tenen grau $d := \frac{N(\beta)-1}{4}$, on $N(\beta)$ és la norma de β

(4) El polinomi $xP_\beta(x)$ té $N(\beta)$ arrels diferents donades per $\phi(\alpha\delta)$ per $[\alpha] \in \mathbb{Z}[i]/\beta\mathbb{Z}[i]$ i $\delta \in \frac{1}{\beta}\mathcal{L}$ un β-generador de torsió fixat.

(5) $P_\beta(x)$ és mònic, $Q_\beta(x) = x^d P_\beta\left(\frac{1}{x}\right)$ i $Q_\beta(0) = 1$.

(6) Sigui $\sigma \in \mathbb{Z}[i]$ un primer senar. Aleshores

$$P_\sigma(x) = x^d + a_1 x^{d-1} + ... + a_d \in \mathbb{Z}[i][x]$$

on cada a_k és divisible entre σ, per a $k \in \{1, ..., d\}$ i $a_d = i^{-\epsilon}\sigma$. A més, $P_\sigma(x^4)$ és irreductible sobre $\mathbb{Q}(i)$.

Abans d'endinsar-nos en la demostració d'aquest teorema, convé fixar-nos en el signficat intuïtiu que té. Siguin $P_\beta(x), Q_\beta(x) \in \mathbb{Z}[i][x]$ els polinomis donats al teorema. Les propietats (3) i (5) impliquen que $P_\beta(x), Q_\beta(x)$ es poden escriure en la forma

$$P_\beta(x) = x^d + a_1 x^{d-1} + ... + a_d$$

$$Q_\beta(x) = x^d P_\beta\left(\frac{1}{x}\right) = 1 + a_1 x + ... + a_d x^d$$

Aleshores la fórmula de multiplicació complexa de $\phi(\beta z)$ es pot escriure com

$$\phi(\beta z) = i^\epsilon \phi(z) \frac{\phi(z)^{4d} + a_1\phi(z)^{4d-4} + ... + a_d}{1 + a_1\phi(z)^4 + ... + a_d\phi(z)^{4d}} \tag{4.13}$$

on $\beta \equiv i^\epsilon \pmod{2(1+i)}$ d'acord amb la propietat (2).

Ara sí, demostrem el teorema 4.19.

Demostració. Demostrarem el teorema en sis passos.
Pas 1: Existència de $P_\beta(x)$ i $Q_\beta(x)$, $\forall\beta$. Donada $\beta \in \mathbb{Z}[i]$, afirmem que existeixen polinomis $P_\beta(x), Q_\beta(x) \in \mathbb{Z}[i][x]$ tals que $Q_\beta(0) = 1$ i, si β és senar,

$$\phi(\beta z) = \phi(z) \frac{P_\beta(\phi(z)^4)}{Q_\beta(\phi(z)^4)} \tag{4.14}$$

mentre que si β és parell,

$$\phi(\beta z) = \phi(z)\phi'(z)\frac{P_\beta(\phi(z)^4)}{Q_\beta(\phi(z)^4)} \tag{4.15}$$

Per a veure-ho, fem servir les relacions $\phi(iz) = i\phi(z)$, vista a (4.1), i (4.9), que indica

$$\phi((1+i)z) = \phi(z)\phi'(z)\frac{1+i}{1-\phi(z)^4}$$

Observem que verifiquen respectivament (4.14) i (4.15). Ara fem servir la identitat (3.19) juntament amb (4.1) i trobem

$$\phi((\beta+1)z) = -\phi((\beta-1)z) + \frac{2\phi(\beta z)\phi'(z)}{1+\phi(\beta z)^2\phi(z)^2} \tag{4.16}$$

$$\phi((\beta+i)z) = -\phi((\beta-i)z) + \frac{2i\phi(\beta z)\phi'(z)}{1-\phi(\beta z)^2\phi(z)^2} \tag{4.17}$$

Un ús repetit de la relació (4.16), demostra que per tot $n \in \mathbb{Z}_+$ existeixen polinomis $P_{n+i}(x), Q_{n+i}(x) \in \mathbb{Z}[i][x]$ que ens donen la forma desitjada per a $\phi((n+i)z)$. L'argument és similar a l'usat a la demostració del teorema 3.4. En particular, quan n és parell, obtenim la recursió

$$Q_{n+1+i}(x) = Q_{n-1+i}(x)\left[Q_{n+i}^2(x) + xP_{n+i}^2(x)(1-x)\right]$$

de manera similar a (3.24). Això fa que sigui fàcil demostrar que $Q_{n+i}(0) = 1$, $\forall n \in \mathbb{Z}_+$ parell. L'argument per a $n \in \mathbb{Z}_+$ senar és anàleg.
Ara fixem $n \in \mathbb{Z}_+$ i fem servir les fórmules $\phi((n+i)z)$ ja trobades i el teorema 3.4. Un ús repetit de (4.17) demostra que per tota $m \in \mathbb{Z}_+$ existeixen polinomis $P_{n+mi}(x), Q_{n+mi}(x) \in \mathbb{Z}[i][x]$ tals que ens donen la forma desitjada per a $\phi((n+mi)z)$ i se satisfà $Q_{n+mi}(0) = 1$. D'aquí traiem les fórmules per a $\phi((n+mi)z)$ per tots $n, m \in \mathbb{Z}_+$. Les relacions

$$\phi((-m+ni)z) = \phi(i(n+mi)z) = i\phi((n+mi)z)$$

$$\phi((-n-mi)z) = \phi(-(n+mi)z) = -\phi((n+mi)z)$$

$$\phi((m-ni)z) = \phi(-i(n+mi)z) = -i\phi((n+mi)z)$$

ens permeten construir $P_\beta(x), Q_\beta(x) \in \mathbb{Z}[i][x]$, $\forall \beta \in \mathbb{Z}[i]$.

Pas 2: Traiem factors comuns. D'ara endavant, assumirem que $\beta \in \mathbb{Z}[i]$ és senar. Els polinomis $P_\beta(x)$, $Q_\beta(x)$ construïts al Pas 1 a priori poden tenir algun factor en comú. Com que $\mathbb{Z}[i]$ és un domini de factorització única, també ho és $\mathbb{Z}[i][x]$. Llavors, podem escriure

$$P_\beta(x) = R_\beta(x)\tilde{P}_\beta(x), \qquad Q_\beta(x) = R_\beta(x)\tilde{Q}_\beta(x)$$

on $R_\beta(x), \tilde{P}_\beta(x), \tilde{Q}_\beta(x) \in \mathbb{Z}[i][x]$ i $\tilde{P}_\beta(x), \tilde{Q}_\beta(x)$ són coprimers. Sabem que $Q_\beta(0) = 1$. Per tant, podem multiplicar $R_\beta(x), \tilde{P}_\beta(x), \tilde{Q}_\beta(x)$ per un element de $\mathbb{Z}[i]^* = \{\pm 1, \pm i\}$ adient de manera que $\tilde{Q}_\beta(0) = 1$. Com que β és senar,

$$\phi(\beta z) = \phi(z)\frac{P_\beta(\phi(z)^4)}{Q_\beta(\phi(z)^4)} = \phi(z)\frac{R_\beta(z)\tilde{P}_\beta(z)}{R_\beta(z)\tilde{Q}_\beta(z)} = \phi(z)\frac{\tilde{P}_\beta(\phi(z)^4)}{\tilde{Q}_\beta(\phi(z)^4)}$$

Així doncs, podem assumir que $P_\beta(x), Q_\beta(x)$ són coprimers a $\mathbb{Z}[i][x]$ amb $Q_\beta(0) = 1$.

Pas 3: La constant i^ϵ. Considerem l'anell finit $\mathbb{Z}[i]/2(1+i)\mathbb{Z}[i]$. De la demostració de la propietat (iii) de l'observació 4.12, sabem que $(\mathbb{Z}[i]/2(1+i)\mathbb{Z}[i])^* = \{\pm[1], \pm[i]\}$, de manera que $\beta \equiv i^\epsilon \pmod{2(1+i)}$, per algun $\epsilon \in \{0,1,2,3\}$. Si multipliquem $P_\beta(x)$ per una unitat apropiada de $\mathbb{Z}[i]^*$, obtenim l'equació

$$\phi(\beta z) = i^\epsilon \phi(z) \frac{P_\beta(\phi(z)^4)}{Q_\beta(\phi(z)^4)} \tag{4.18}$$

D'acord amb (2.3), sabem que $\phi(\frac{\varpi}{2}) = 1$, de manera que $\phi\left(\beta\frac{\varpi}{2}\right) = i^\epsilon P_\beta(1)/Q_\beta(1)$. Tenint en compte les fórmules recursives que caracteritzen $P_\beta(x)$ i $Q_\beta(x)$ i avaluant a $x = 1$, trobem que $P_\beta(1) = Q_\beta(1)$, així que

$$\phi\left(\beta\frac{\varpi}{2}\right) = i^\epsilon \tag{4.19}$$

Pas 4: Arrels de $xP_\beta(x^4)$. Farem servir el lema 4.14 per a determinar les arrels del polinomi $D_\beta(x) := xP_\beta(x^4)$. Posem $B_\beta(x) = Q_\beta(x^4)$. Com que β és senar, (4.18) implica

$$\phi(\beta z) = i^\epsilon \frac{D_\beta(\phi(z))}{B_\beta(\phi(z))} \tag{4.20}$$

Com que $P_\beta(x)$, $Q_\beta(x)$ són coprimers a $\mathbb{Z}[i][x]$ i $Q_\beta(0) = 1$, sabem que $D_\beta(x)$ i $B_\beta(x)$ no tenen arrels en comú a $\mathbb{C}$. Fent servir això i (4.20),

$$D_\beta(\phi(z)) = 0 \iff \phi(\beta z) = 0$$

Pel teorema 4.3, concloem que les arrels de $D_\beta(x)$ formen el conjunt

$$R_\beta = \{\phi(z) \,|\, z \in \mathbb{C}, \phi(\beta z) = 0\}$$

com al lema 4.14. Això implica que les arrels es poden escriure com $\phi(\alpha\frac{\varpi}{\beta})$ amb $\alpha \in \mathbb{Z}[i]$ senar. Vegem que totes les arrels de $D_\beta(x)$ són simples. Suposem $x_0 = \phi(z_0)$ és una arrel múltiple. Aleshores $D_\beta(x_0) = D'_\beta(x_0) = 0$, i llavors $B_\beta(x_0) \neq 0$ pel que hem vist abans. Derivant (4.20) respecte de z i avaluant a $z = x_0$, tenim

$$\phi'(x_0)\beta = i^\epsilon \frac{D'_\beta(x_0)\phi'(x_0)B_\beta(x_0) - D_\beta(x_0)B'_\beta(x_0)\phi'(x_0)}{B_\beta(x_0)^2} = 0$$

Com que $\phi(\beta x_0) = 0$, ϕ té un zero múltiple a βx_0. Això entra en contradicció amb el teorema 4.2. És per això que $D_\beta(x)$ té arrels simples. Per tant, el grau de $D_\beta(x)$ ha de ser el nombre d'elements de R_β. Pel lema 4.14, sabem que $D_\beta(x) = xP_\beta(x^4)$ té grau $N(\beta)$, d'on veiem que $P_\beta(x)$ té grau $d = \frac{N(\beta)-1}{4}$.

Podem refinar encara més el nostre resultat. Sigui $\delta_\beta = \frac{1+i}{\beta}\varpi$. Per qualsevol $\alpha \in \mathbb{Z}[i]$, $\phi(\alpha\delta_\beta)$ és una arrel de $A_\beta(x)$ ja que ϕ s'anul·la per $\beta\alpha\delta_\beta \in \mathcal{L}$. Suposem que existeixen $\alpha, \tilde{\alpha} \in \mathbb{Z}[i]$ tals que $\phi(\alpha\delta_\beta) = \phi(\tilde{\alpha}\delta_\beta)$. Pel teorema 4.3, tenim

$$\alpha\delta_\beta = (-1)^{a+b}\tilde{\alpha}\delta_\beta + (a+bi)\varpi, \quad a, b \in \mathbb{Z}$$

Això implica que $\alpha(1+i) = (-1)^{a+b}\tilde{\alpha}(1+i) + (a+bi)\beta$, de manera que $a+bi$ és parell. Llavors $\alpha \equiv \tilde{\alpha} \pmod{\beta}$. Consegüentment, $D_\beta(x)$ té almenys $N(\beta) = |\mathbb{Z}[i]/\beta\mathbb{Z}[i]|$ arrels diferents, més concretament, $\phi(\alpha\delta_\beta)$, amb $[\alpha] \in \mathbb{Z}[i]/\beta\mathbb{Z}[i]$. Com que el polinomi té grau $N(\beta)$, aquestes són totes les arrels possibles. El mateix es compliria per qualsevol altre β-generador de torsió per l'observació 4.18.

Pas 5: Relació entre $P_\beta(x)$ i $Q_\beta(x)$. Una vegada haguem vist que $Q_\beta(x) = x^d P_\beta(\frac{1}{x})$, quedarà demostrat que $Q_\beta(x)$ té grau d i que $P_\beta(x)$ és mònic (perquè $Q_\beta(x)$ té terme independent 1). La identitat (4.7) implica

$$\phi(z)\phi\left(z + (1+i)\frac{\varpi}{2}\right) = \phi(z)\phi(w) = -i = i^3 \tag{4.21}$$

on hem definit $w = z + (1+i)\frac{\varpi}{2}$. Atesa la doble periodicitat de ϕ a $\mathcal{L}$ i que $\beta \equiv i^\epsilon \pmod{2(1+i)}$, és clar que

$$\phi(\beta z)\phi(\beta w) = i^{3+2\epsilon} \tag{4.22}$$

Llavors

$$\frac{\phi(\beta z)}{i^\epsilon \phi(z)} = \frac{i^\epsilon \phi(w)}{\phi(\beta w)} = \frac{Q_\beta(\phi(w)^4)}{P_\beta(\phi(w)^4)} = \frac{Q_\beta(1/\phi(z)^4)}{P_\beta(1/\phi(z)^4)} \tag{4.23}$$

on a la primera igualtat s'ha fet servir (4.21) i (4.22), la segona usa (4.18) i la tercera se segueix d'elevar (4.18) a la quarta, la qual cosa ens dóna $\phi(w)^4 = 1/\phi(z)^4$. Per comparació directa de (4.23) amb (4.18), arribem a

$$\frac{Q_\beta(1/x^4)}{P_\beta(1/x^4)} = \frac{P_\beta(x^4)}{Q_\beta(x^4)} \Rightarrow \frac{Q_\beta(1/x)}{P_\beta(1/x)} = \frac{P_\beta(x)}{Q_\beta(x)} \tag{4.24}$$

com a funcions racionals en x. Per (4.24) podem escriure la igualtat $(x^d Q_\beta(1/x))Q_\beta(x) = (x^d P_\beta(1/x))P_\beta(x)$, on la part de la dreta és un polinomi. Clarament, doncs, la part de l'esquerra de la igualtat també ho és i $\mathrm{gr}(Q_\beta) = \mathrm{gr}(P_\beta) = d$. A més, si considerem un factor irreductible $q|Q_\beta$, sabem que q també ha de dividir $(x^d P_\beta(1/x))P_\beta(x)$ i, com que $Q_\beta(x)$ i $P_\beta(x)$ són coprimers, q necessàriament ha de dividir $x^d P_\beta(1/x)$. Com que aquest raonament es pot aplicar per tot factor irreductible de Q_β, trobem que Q_β divideix $x^d P_\beta(1/x)$. Fent servir que els graus d'aquests dos polinomis són iguals, es dedueix que $\exists\, \lambda \in \mathbb{Q}(i)^*$ tal que

$$x^d P_\beta(1/x) = \lambda Q_\beta(x) \tag{4.25}$$

Ara aprofitem resultats anteriors per a determinar λ. En particular, si avaluem (4.18) a $z = \frac{\varpi}{2}$ i fem servir (4.19), trobem

$$i^\epsilon = i^\epsilon \frac{P_\beta(1)}{Q_\beta(1)}$$

per la qual cosa $P_\beta(1) = Q_\beta(1) \neq 0$. Si ara avaluem (4.25) per a $x = 1$, trobem que $\lambda = 1$, de manera que $x^d P_\beta(1/x) = Q_\beta(x)$, com volíem demostrar.

Pas 6: Irreductibilitat de $P_\sigma(x)$. Sigui $\sigma \in \mathbb{Z}[i]$ primer senar. N'hi ha prou amb veure que $P_\sigma(x) = x^d + a_1 x^{d-1} + ... + a_d \in \mathbb{Z}[i][x]$, on cada a_k és divisible entre σ, per a $k \in \{1, ..., d\}$ i $a_d = i^{-\epsilon}\sigma$ perquè el fet que $P_\sigma(x)$ sigui irreductible sobre $\mathbb{Q}(i)$ en serà conseqüència directa pel criteri d'Eisenstein. Com que β és senar, ja sabem que

$$\phi(\beta z) = i^\epsilon \phi(z) \frac{\phi(z)^{4d} + a_1\phi(z)^{4d-4} + ... + a_d}{1 + a_1\phi(z)^4 + ... + a_d\phi(z)^{4d}} \tag{4.26}$$

on els coeficients $a_1, ..., a_d \in \mathbb{Z}[i]$ depenen de β. Per una banda, ens interessa expressar la següent funció racional com a sèrie de potències.

$$h(x) := i^\epsilon \frac{x^d + a_1(\beta)x^{d-1} + ... + a_d(\beta)}{1 + a_1(\beta)x + ... + a_d(\beta)x^d} \tag{4.27}$$

Notem que és una funció analítica a $x = 0$ perquè el denominador no s'anul·la per aquest valor. Així doncs, admet l'expansió en sèrie de potències

$$h(x) = \sum_{k=0}^{\infty} b_k(\beta) x^k \tag{4.28}$$

Es pot veure que $b_k(\beta) \in \mathbb{Z}[i], \forall k \in \mathbb{N}$. Es pot demostrar inductivament tenint en compte que $b_0(\beta) = h(0) = i^\epsilon \in \mathbb{Z}[i]$ i que els coeficients $a_1, ..., a_d \in \mathbb{Z}[i]$. Fent servir aquesta sèrie de potències, podem reescriure (4.26) com

$$\phi(\beta z) = \sum_{k=0}^{\infty} b_k(\beta) \phi(z)^{4k+1} \tag{4.29}$$

Per altra banda, fixem-nos que també podem expressar $\phi(z)$ com a sèrie de potències ja que és analítica a $z = 0$. Posem $\phi(z) = \sum_{k=0}^{\infty} c_k z^k$. Recordant les relacions $\phi'(z)^2 = 1 - \phi(z)^4$ i $\phi''(z) = -2\phi(z)^3$, és fàcil demostrar inductivament que, per tota $n \in \mathbb{N}$, existeix $G_n \in \mathbb{Z}[x]$ tal que

$$\phi^{(n)}(z) = \begin{cases} G_n(\phi(z))\phi'(z), & n = 2k+1 \\ G_n(\phi(z)), & n = 2k \end{cases} \tag{4.30}$$

amb $k \in \mathbb{N}$, i que els coeficients $c_k \in \mathbb{Q}$ perquè G_n té coeficients a $\mathbb{Z}$. Més concretament, com que $\phi(iz) = i\phi(z)$, fent servir el desenvolupament en sèrie de potències de Taylor, podem escriure

$$\phi(z) = \sum_{j=0}^{\infty} c_j z^{4j+1}, \quad c_j = \frac{G_{4j+1}(0)}{(4j+1)!} \tag{4.31}$$

perquè $\phi'(0) = 1$. Com que $G_n \in \mathbb{Z}[x]$, tenim que $c_j \in \mathbb{Q}, \forall j \in \mathbb{N}$. En particular, es pot comprovar que $G_1(x) = 1$, $G_5(x) = -12(1 - 10x^4)$ i $G_9(x) = 3024(1 - 10x^4 + 30x^8)$. De manera que els primers coeficients són $c_0 = G_1(0) = 1$, $c_1 = \frac{G_5(0)}{5!} = -\frac{1}{10}$ i $c_2 = \frac{G_9(0)}{9!} = \frac{1}{120}$. Així doncs, podem substituir z per βz a (4.31), obtenim

$$\phi(\beta z) = \sum_{j=0}^{\infty} c_j (\beta z)^{4j+1} = \beta z + c_1 \beta^5 z^5 + c_2 \beta^9 z^9 + ... \tag{4.32}$$

Havent vist això, ara volem relacionar explícitament els coeficients $b_k(\beta)$ amb β per a demostrar que β divideix $b_0(\beta), ..., b_{d-1}(\beta)$ quan β és senar. Després relacionarem els coeficients $a_1(\beta), ..., a_d(\beta)$ amb els $b_0(\beta), ..., b_{d-1}(\beta)$ per a concloure que β divideix $a_1(\beta), ..., a_{d-1}(\beta)$.

Substituïm (4.31) i (4.32) a (4.29) i, comparant termes de mateix grau, trobem

$$\begin{aligned} b_0(\beta) &= \beta \\ b_1(\beta) &= \beta c_1(\beta^4 - 1) \\ b_2(\beta) &= \beta(c_2\beta^8 - 5c_1^2\beta^4 + 5c_1^2 - c_2) \end{aligned} \tag{4.33}$$

Com que $c_j \in \mathbb{Q}$, es demostra en general que existeix $S_k \in \mathbb{Q}[x]$ tal que $b_k(\beta) = \beta S_k(\beta)$ amb $\mathrm{gr}(S_k) = 4k$, per a tot $\beta \in \mathbb{Z}[i]$ senar. Aquesta relació sembla implicar que b_k és un múltiple de β per tot $k \in \mathbb{N}$. El problema és que $S_k \in \mathbb{Q}[x]$ no necessàriament té coeficients enters. Sigui $s_k \in \mathbb{Z} \setminus \{0\}$ el mínim comú múltiple dels denominadors dels

coeficients de $S_k(x)$. Clarament, $S_k(x) = \frac{1}{s_k} T_k(x)$, amb $T_k \in \mathbb{Z}[x]$. Notem que ± 1 són els únics enters que divideixen alhora s_k i els coeficients de $T_k(x)$. Amb això, podem afirmar

$$s_k b_k(\beta) = \beta T_k(\beta), \quad \beta \in \mathbb{Z}[i] \text{ } senar \tag{4.34}$$

Com que $b_k(\beta) \in \mathbb{Z}[i]$, si un $\alpha \in \mathbb{Z}[i]$ primer senar divideix s_k, aleshores α també divideix $\beta T_k(\beta)$. Llavors

$$\beta T_k(\beta) \equiv 0 \pmod{\alpha}, \quad \beta \in \mathbb{Z}[i] \text{ } senar \tag{4.35}$$

Atès que α és senar, per la demostració del lema 4.14, sabem que els elements de $\mathbb{Z}[i]/\alpha\mathbb{Z}[i]$ són de la forma $[\beta]$, amb β senar. Per tant, (4.35) implica que el polinomi $xT_k(x)$ mòdul α és un polinomi amb almenys $|\mathbb{Z}[i]/\alpha\mathbb{Z}[i]|$ arrels. Tenint en compte també que α divideix s_k, la definició de s_k comporta que $xP_k(x)$ mòdul α és un polinomi no trivial de grau com a molt $4k+1$, la qual cosa indica que té com a molt $4k+1$ arrels.

Aquestes dues observacions permeten afirmar que $N(\alpha) = |\mathbb{Z}[i]/\alpha\mathbb{Z}[i]| \leq 4k+1$. Per tant, $\alpha | s_k \Rightarrow N(\alpha) \leq 4k+1, \forall \alpha \in \mathbb{Z}[i]$ primer senar. Fixem ara β enter gaussià senar. Si $N(\beta) > 4k+1$, llavors $\beta \nmid s_k$. Fixem-nos, però que $N(\beta) > 4k+1 \iff k < (N(\beta)-1)/4 = d$. Per tant, $\beta \nmid s_k$ per a $k \in \{0, ..., d-1\}$. Com que β és primer, (4.34) implica que β divideix $b_k(\beta)$ per a $k \in \{0, ..., d-1\}$.

Ja per acabar, expressem els coeficients $a_1(\beta), ..., a_d(\beta)$ en termes dels $b_0(\beta), ..., b_{d-1}(\beta)$. Si escrivim (4.29) en la forma

$$i^\epsilon \left(x^d + a_1(\beta)x^{d-1} + ... + a_d(\beta) \right) = \left(1 + a_1(\beta)x + ... + a_d(\beta)x^d \right) \left(\sum_{k=0}^{\infty} b_k(\beta)x^k \right)$$

i desenvolupem la part de la dreta, només cal comparar termes per a trobar

$$\begin{aligned}
a_d(\beta) &= i^{-\epsilon} b_0(\beta) \\
a_{d-1}(\beta) &= i^{-\epsilon} \left[a_1(\beta)b_0(\beta) + b_1(\beta) \right] \\
a_{d-2}(\beta) &= i^{-\epsilon} \left[a_2(\beta)b_0(\beta) + a_1(\beta)b_1(\beta) + b_2(\beta) \right] \\
&\vdots \\
a_1(\beta) &= i^{-\epsilon} \left[a_{d-1}(\beta)b_0(\beta) + a_{d-2}(\beta)b_1(\beta) + ... + b_{d-1}(\beta) \right]
\end{aligned} \tag{4.36}$$

Com que hem vist que $b_0(\beta), ..., b_{d-1}(\beta)$ són divisibles entre β i $a_j(\beta) \in \mathbb{Z}[i]$, trobem que β divideix $a_0(\beta), ..., a_d$ ja que $i^{-\epsilon}$ és una unitat. Recordem que a (4.33) hem vist que $b_0(\beta) = \beta$. Consegüentment, la primera equació de (4.36) implica que $a_d(\beta) = i^{-\epsilon}\beta$. Això completa la nostra demostració. □

Definició 4.20. *De manera anàloga a la definició 3.5, per a $\beta \in \mathbb{Z}[i]$ senar, definim polinomi de β-divisió el polinomi $D_\beta(x) := xP_\beta(x^4) \in \mathbb{Z}[i][x]$.*

5 Cossos lemnatòmics

En aquesta secció s'introdueix una teoria algebraica d'extensió de cossos centrada en la lemniscata que busca establir un paral·lelisme amb la construcció dels cossos ciclotòmics en el cas de la circumferència. Així com en el cas de la circumferència es construeixen extensions de $\mathbb{Q}$ a partir de les arrels n-èsimes de la unitat, aquí es pretén trobar una caracterització anàloga a partir dels punts de divisió de la lemniscata. L'objectiu d'aquesta secció és, doncs, estudiar els grups de Galois de les extensions lemnatòmiques. És a partir d'aquesta caracterització que podrem determinar la constructibilitat dels polígons regulars sobre la lemniscata. Per a fer-ho, s'empraran dues estratègies diferents, que anomenarem *natural* i *alternativa* respectivament.

5.1 Plantejament natural

Així com les extensions ciclotòmics n-èsimes sorgeixen d'adjuntar les arrels n-èsimes de la unitat ζ_n a $\mathbb{Q}$, en aquest apartat construirem les extensions lemnatòmiques a partir d'adjuntar els punts de n-divisió de la lemniscata, $\phi(\frac{2\varpi}{n})$ amb a $n \in \mathbb{Z}_+$, a $\mathbb{Q}(i)$. Aquest enfocament s'ha denotat com a *natural* en aquest treball ja que deriva exclusivament de consideracions geomètriques. Un cop s'hagin caracteritzat adequadament aquestes extensions, es procedirà a examinar diverses nocions de constructibilitat amb regle i compàs que ens permetran determinar finalment quins polígons són construïbles sobre la lemniscata. Aquest apartat es nodreix principalment d'idees presentades a [4] i [14].

5.1.1 Extensions lemnatòmiques

Definició 5.1. *Sigui $n \in \mathbb{Z}_+$. S'anomena cos lemnatòmic n-èsim el cos de descomposició del polinomi $D_n(x)$ sobre $\mathbb{Q}(i)$.*

Notació 2. *D'ara endavant, denotarem per n un nombre natural senar i escriurem $K = \mathbb{Q}(i)$ i $L = K(\phi(\frac{\varpi}{n})) = \mathbb{Q}(i, \phi(\frac{\varpi}{n}))$.*

Lema 5.2. *Donat $\beta \in \mathbb{Z}[i]$ senar, $\frac{\varpi}{n} \in \frac{1}{\beta}\mathcal{L}$ és un β-generador de torsió.*

Demostració. Com que n és senar, sabem que $n(1+i) \in \mathbb{Z}[i]$ és parell. Per tant, podem escriure $n(1+i) = \beta[u(1+i)+v]$ per alguns $u, v \in \mathbb{Z}[i]$. Si multipliquem aquesta expressió per $\delta_\beta = \frac{(1+i)\varpi}{\beta}$ trobem que $\frac{(1+i)\varpi}{\beta} - v\frac{\varpi}{n} = (1+i)u\varpi$, la qual cosa és equivalent a $v\frac{\varpi}{n} \equiv \delta_\beta \pmod{\mathcal{L}}$. Per l'observació 4.18, tenim que $\frac{\varpi}{n}$ és un β-generador de torsió. □

Teorema 5.3. *Siguin $\beta \in \mathbb{Z}[i]$ i $n \in \mathbb{N}$ senars, $K = \mathbb{Q}(i)$ i $L = \mathbb{Q}(i, \phi(\frac{\varpi}{n}))$.*

(1) L/K és una extensió de Galois.

(2) Per qualsevol $\sigma \in Gal(L/K)$, existeix un únic $[\alpha] \in (\mathbb{Z}[i]/n\mathbb{Z}[i])^*$ tal que $\sigma(\phi(\delta)) = \phi(\alpha\delta)$, per qualsevol β-generador de torsió δ. En particular, l'aplicació que envia $\sigma \mapsto [\alpha]$ defineix l'isomorfisme $Gal(L/K) \cong (\mathbb{Z}[i]/n\mathbb{Z}[i])^*$.

(3) En particular, $Gal(L/K)$ és abelià.

Demostració. Com que $\frac{\varpi}{n}$ és un β-generador de torsió, pel teorema 4.19, sabem que el polinomi de β-divisió $D_\beta(x) = xP_\beta(x^4)$ té arrels $\phi(\alpha\frac{\varpi}{n})$, amb $\alpha \in \mathbb{Z}[i]$ senar, i la demostració del lema 4.14 implica que, per a cada arrel, l'element $\alpha \in \mathbb{Z}[i]$ associat és únic mòdul $n\mathbb{Z}[i]$. Ja que, per a cada arrel, α és senar, la fórmula de multiplicació complexa per a $\phi(\alpha z)$ vista al teorema 4.19 posa de manifest que $\phi(\alpha\frac{\varpi}{n})$ és una funció racional en $\phi(\frac{\varpi}{n})$ amb coeficients a $\mathbb{Q}(i)$. Per consegüent, $D_\beta(x)$ descompon totalment a $L = \mathbb{Q}(i, \phi(\frac{\varpi}{n}))$. Aleshores, com que una de les arrels és simplement $\phi(\frac{\varpi}{n})$, sabem que L és cos de descomposició de $D_\beta(x)$ sobre $K = \mathbb{Q}(i)$. Així doncs, queda demostrat que L/K és una extensió de Galois.

Sigui $\sigma \in \mathrm{Gal}(L/K)$. Aleshores $\sigma(\phi(\frac{\varpi}{n}))$ és una arrel de $D_\beta(x)$. Per tant, existeix $\alpha \in \mathbb{Z}[i]$ senar tal que

$$\sigma\left(\phi\left(\frac{\varpi}{n}\right)\right) = \phi\left(\alpha\frac{\varpi}{n}\right) \tag{5.1}$$

Hem argumentat prèviament que α és únic mòdul $n\mathbb{Z}[i]$. Vegem que α és coprimer a n. Sigui m l'ordre de $\sigma \in \mathrm{Gal}(L/K)$. Aleshores, iterant (5.1) trobem

$$\phi\left(\frac{\varpi}{n}\right) = \sigma^m\left(\phi\left(\frac{\varpi}{n}\right)\right) = \phi\left(\alpha^m\frac{\varpi}{n}\right)$$

Per unicitat, $1 \equiv \alpha^m \pmod{n}$. D'aquí veiem que α i n són coprimers a $\mathbb{Z}[i]$. Com a conseqüència, l'aplicació $\mathrm{Gal}(L/K) \to (\mathbb{Z}[i]/\beta\mathbb{Z}[i])^*$ que envia $\sigma \mapsto [\alpha]$ està ben definida. Siguin $\sigma, \tau \in \mathrm{Gal}(L/K)$ tals que tenen imatges $\alpha, \gamma \in (\mathbb{Z}[i]/n\mathbb{Z}[i])^*$ respectivament. Per (5.1), veiem que $\sigma\tau(\phi(\frac{\varpi}{n})) = \phi(\alpha\gamma\frac{\varpi}{n})$, és a dir, l'aplicació defineix un morfisme de grups. Clarament és un morfisme exhaustiu. Per a veure que és injectiu, considerem que $[\alpha] = [\gamma]$ a $(\mathbb{Z}[i]/n\mathbb{Z}[i])^*$. Aleshores, $\alpha = \gamma + (a+bi)n$, on $(a+bi)$ ha de ser senar ja que α, γ i n són senars. Si invoquem la proposició 4.1, obtenim

$$\sigma\left(\phi\left(\frac{\varpi}{n}\right)\right) = \phi\left(\alpha\frac{\varpi}{n}\right) = \phi\left(\gamma\frac{\varpi}{n}\right) = \tau\left(\phi\left(\frac{\varpi}{n}\right)\right)$$

Això demostra que el morfisme de grups considerat és, en efecte, un isomorfisme ja que $\phi(\frac{\varpi}{n})$ genera L sobre K. Finalment, observem que $\mathrm{Gal}(L/K)$ és un grup abelià perquè $(\mathbb{Z}[i]/n\mathbb{Z}[i])^*$ ho és. □

Observació 5.4. Una pregunta apropiada seria per què definim les extensions lemnatòmiques sobre $\mathbb{Q}(i)$ i no sobre $\mathbb{Q}$. Una raó és que l'extensió $\mathbb{Q}(\phi(\frac{\varpi}{n}))/\mathbb{Q}$ no és galoisiana. En particular, l'extensió $\mathbb{Q}(\phi(\frac{\varpi}{n}))/\mathbb{Q}$ en general no és normal ja que el polinomi de n-divisió $D_n(x) \in \mathbb{Z}[x] \subset \mathbb{Q}[x]$, del qual sabem que una de les seves arrels és $\phi(\frac{\varpi}{n})$, no descomposa totalment sobre $\mathbb{Q}(\phi(\frac{\varpi}{n}))/\mathbb{Q}$ però sí sobre $L = \mathbb{Q}(i, \phi(\frac{\varpi}{n}))$. A l'Observació 5.30 del *Plantejament alternatiu* (subsecció 5.2) es proporciona una altra argumentació sobre el perquè d'aquesta construcció.

Corol·lari 5.5. *Les coordenades dels punts de n-divisió de la lemniscata es poden expressar per radicals sobre $\mathbb{Q}$.*

Demostració. Aquest resultat és conseqüència directa del fet que $\mathrm{Gal}(L/K)$ sigui abelià perquè sabem que els grups abelians són resolubles. Això implica que els polinomis $D_\beta(x)$ són resolubles per radicals. Pel teorema 4.19, sabem que les arrels de $D_\beta(x)$ són els punts de n-divisió de la lemniscata. Aleshores queda demostrat que les coordenades d'aquests punts es poden expressar per radicals sobre $\mathbb{Q}$. □

5.1.2 Construccions amb regle i compàs

Recordem que un nombre complex α és construïble amb regle i compàs si, i només si, α pertany a un cos L que és extensió finita de $\mathbb{Q}$ amb $[L:\mathbb{Q}]$ potència de 2.

Proposició 5.6. *Sigui P un punt de la lemniscata i r la distància de P a l'origen. Llavors P és construïble amb regle i compàs si, i només si, r és construïble.*

Demostració. Sigui $P=(x,y)$. Per la definició dels punts de la lemniscata (2.1) i de la distància polar r, es verifica

$$\begin{cases} r^4 = x^2 - y^2 \\ r^2 = x^2 + y^2 \end{cases}$$

la qual cosa ens condueix a expressar les coordenades dels punts de la lemniscata com

$$x = \pm\sqrt{\frac{1}{2}\left(r^2 + r^4\right)}, \qquad y = \pm\sqrt{\frac{1}{2}\left(r^2 - r^4\right)} \tag{5.2}$$

Ja que els nombres contruïbles formen un subcòs de $\mathbb{C}$ tancat sota arrels quadrades, veiem que x i y són construïbles quan r és construïble. El recíproc també es compleix perquè si x, y són construïbles, immediatament tenim que $r=\sqrt{x^2+y^2}$ és construïble. □

Lema 5.7. *Sigui $n \in \mathbb{N}$ tal que $\phi(\frac{2\varpi}{n})$ és construïble. Aleshores els punts de n-divisió de la lemniscata són construïbles amb regle i compàs.*

Demostració. En virtut de la proposició 5.6, n'hi ha prou amb veure que $\phi(m\frac{2\varpi}{n})$ és construïble per cada $m \in \mathbb{Z}$. El cas $m=0$ és trivial i com que ϕ és una funció senar, ens limitarem a demostrar-ho pel cas $m>0$. En particular, els casos $n \in \{1,2\}$ són trivials, així que considerarem $n>2$. Observem que si $\phi(\frac{2\varpi}{n})$ és construïble, llavors $\phi'(\frac{2\varpi}{n})$ també ho és perquè $\phi'(x)^2 = 1-\phi(x)^2$. Gràcies al teorema 3.4, sabem que $\phi(m\frac{2\varpi}{n})$ és una funció racional de $\phi(\frac{2\varpi}{n})$ i $\phi'(\frac{2\varpi}{n})$ amb coeficients a $\mathbb{Z}$ per a $n>2$. Això demostra que $\phi(m\frac{2\varpi}{n})$ és construïble per tot $m \in \mathbb{Z}$. □

Lema 5.8. *Siguin $n, m \in \mathbb{N}$ tals que $\phi(\frac{2\varpi}{n})$ i $\phi(\frac{2\varpi}{m})$ són construïbles. Llavors $\phi(\frac{2\varpi}{N})$ és construïble amb $N = mcm(n,m)$.*

Demostració. Sigui $d \in \mathbb{Z}$ el màxim comú divisor entre n i m. Llavors $d = \frac{nm}{N}$. Clarament existeixen $\mu, \nu \in \mathbb{Z}$ tals que $\mu m + \nu n = d$. Per tant,

$$\frac{2\varpi}{N} = \frac{2\varpi}{nm}d = \frac{2\varpi}{nm}(\mu m + \nu n) = \mu\frac{2\varpi}{n} + \nu\frac{2\varpi}{m}$$

Pel lema anterior, $\phi(\mu\frac{2\varpi}{n})$ i $\phi(\nu\frac{2\varpi}{m})$ són construïbles, així com també ho són les respectives derivades. Aleshores, invocant el teorema 3.2, podem expressar $\phi(\frac{2\varpi}{N}) = \phi(\mu\frac{2\varpi}{n} + \nu\frac{2\varpi}{m})$ com a funció racional en ϕ i ϕ' avaluades en $\mu\frac{2\varpi}{n}$ i $\nu\frac{2\varpi}{m}$ amb coeficients enters. Notem que aquesta funció racional està ben definida perquè el denominador $1+\phi(\mu\frac{2\varpi}{n})^2\phi(\nu\frac{2\varpi}{m})^2$ és no nul. □

Teorema 5.9. *Sigui $n \in \mathbb{Z}_+$. Són equivalents:*

(i) Els punts de n-divisió de la lemniscata es poden construir amb regle i compàs.

(ii) $\phi(\frac{2\varpi}{n})$ és construïble.

(iii) $n = 2^s$, amb $s \in \mathbb{N}$, o bé $n = 2^s p_1 \dots p_r$, amb $s \in \mathbb{N}, r \in \mathbb{Z}_+$ i $p_i, 1 \leq i \leq r$, primers de Fermat diferents.

Demostració. La implicació $(i) \Rightarrow (ii)$ és conseqüència de la proposició 5.6. La implicació recíproca $(i) \Leftarrow (ii)$ és resultat del lema 5.7. Vegem la implicació $(ii) \Leftarrow (iii)$. Suposem que $n = 2^s p_1 ... p_r$ tal com s'indica a l'enunciat. Pel lema 5.8, $\phi(\frac{2\varpi}{n})$ serà construïble si $\phi(\frac{2\varpi}{2^s}), \phi(\frac{2\varpi}{p_1}), ..., \phi(\frac{2\varpi}{p_r})$ són construïbles. Per a comprovar que $\phi(\frac{2\varpi}{2^s})$ és construïble per tot $s \in \mathbb{Z}$, n'hi ha prou amb demostrar que si $\phi(z)$ és construïble, aleshores $\phi(\frac{z}{2})$ també ho és. Si considerem la fórmula de duplicació (3.20) amb $a = \phi(z)$ i $b = \phi(\frac{z}{2})$, tenim

$$a^2 = \left(\frac{2b\,\phi'(\frac{z}{2})}{1+b^4} \right)^2 = \frac{4b^2(1-b^4)}{(1+b^4)^2} \tag{5.3}$$

on s'ha fet servir que $\phi'(\frac{z}{2})^2 = 1 - \phi(\frac{z}{2})^4 = 1 - b^4$. Sigui $c \in \mathbb{C}$ tal que

$$c^2 = \frac{2ib^2}{1-b^4} \tag{5.4}$$

Aleshores l'expressió (5.3) es pot expressar com

$$\frac{-2ic^2}{1-c^4} = \frac{-2i\frac{2ib^2}{1-b^4}}{1-\left(\frac{2ib^2}{1-b^4}\right)^2} = \frac{4b^2(1-b^4)}{(1+b^4)^2} = a^2 \tag{5.5}$$

Si solucionem (5.5) per c^2, trobem que c^2 és construïble perquè a ho és per hipòtesi. I llavors resolent (5.4), trobem que b és construïble. Demostrem ara que $\phi(\frac{2\varpi}{p})$ és construïble, amb p primer de Fermat, i.e. $p = 2^{2^t} + 1$, per algun $t \in \mathbb{Z}$. Hem vist que $\phi(\frac{2\varpi}{p})$ és construïble quan $\phi(\frac{\varpi}{p})$ ho és. Pel teorema 5.3, l'extensió de Galois $K = \mathbb{Q}(i) \subset \mathbb{Q}(i, \phi(\frac{\varpi}{p})) = L$ verifica

$$\mathrm{Gal}(L/K) \cong F \subseteq (\mathbb{Z}[i]/p\mathbb{Z}[i])^*$$

on F és un subgrup de $(\mathbb{Z}[i]/p\mathbb{Z}[i])^*$. Com que L/K és una extensió de Galois, pel teorema d'Artin, $|\mathrm{Gal}(L/K)| = [L : K]$. Aleshores, per tal que $\phi(\frac{\varpi}{p})$ sigui construïble, cal que $|(\mathbb{Z}[i]/p\mathbb{Z}[i])^*| = [L : K] = 2^m$, per alguna $m \in \mathbb{Z}_+$. Demostrem, doncs, que això passa per tot p primer de Fermat. Per a $p = 3$, tenim que $\mathbb{Z}[i]/3\mathbb{Z}[i] = \{0, 1, 2, i, 2i, i+1, i+2, 2i+1, 2i+2\}$. Com que l'únic element que no té invers a $\mathbb{Z}[i]/3\mathbb{Z}[i]$ és el zero, afirmem que $|(\mathbb{Z}[i]/3\mathbb{Z}[i])^*| = 8 = 2^3$. Si $p > 3$, llavors $t \geq 1$, de manera que

$$p = 2^{2^t} + 1 = \left(2^{2^{t-1}} + i\right)\left(2^{2^{t-1}} - i\right) = \beta\bar{\beta} \tag{5.6}$$

on $\beta, \bar{\beta}$ són primers no associats de $\mathbb{Z}[i]$ de norma p. Fent servir el teorema xinès del residu en els enters de Gauss i el lema 4.15, podem aprofitar l'expressió (5.6) per a escriure

$$\mathbb{Z}[i]/p\mathbb{Z}[i] = \mathbb{Z}[i]/\beta\bar{\beta}\mathbb{Z}[i] \cong \mathbb{Z}[i]/\beta\mathbb{Z}[i] \times \mathbb{Z}[i]/\bar{\beta}\mathbb{Z}[i] \cong \mathbb{F}_p \times \mathbb{F}_p \tag{5.7}$$

Aleshores

$$|(\mathbb{Z}[i]/p\mathbb{Z}[i])^*| = |\mathbb{F}_p^* \times \mathbb{F}_p^*| = (p-1)^2 = 2^{2^{t+1}} \tag{5.8}$$

Això demostra que, per tot p primer de Fermat, $|(\mathbb{Z}[i]/p\mathbb{Z}[i])^*| = 2^m$, per alguna $m \in \mathbb{Z}$. Per tant, queda vist $(ii) \Leftarrow (iii)$.

Només queda per veure $(ii) \Rightarrow (iii)$. Sigui $n \in \mathbb{Z}_+$ tal que $\phi(\frac{2\varpi}{n})$ és construïble. Assumim que $n > 1$ perquè altrament el teorema és trivial. Fent servir les fórmules d'addició com abans, n'hi ha prou amb considerar que $\phi(\frac{\varpi}{n})$ és construïble amb n senar. Sigui p un primer que divideixi n. Clarament p és senar perquè n ho és. Sigui $\delta \in \mathbb{Z}[i]$ primer tal que $p = \delta$ si $p \equiv 3 \pmod 4$ i $p = \delta\bar{\delta}$ si $p \equiv 1 \pmod 4$. Llavors, $n/\delta \in \mathbb{Z}[i]$ és senar (perquè n i δ ho són) i $\frac{\varpi}{\delta}$ és un múltiple senar de $\frac{\varpi}{n}$. Fent servir el teorema 4.19, trobem

$$\phi\left(\frac{\varpi}{\delta}\right) \in \mathbb{Q}\left(i, \phi\left(\frac{\varpi}{n}\right)\right) \tag{5.9}$$

En concret, com que i i $\phi(\frac{\varpi}{n})$ són construïbles, $\phi(\frac{\varpi}{\delta})$ també ho és. Això indica que el grau del polinomi mínim de $\phi(\frac{\varpi}{\delta})$ sobre $\mathbb{Q}$ ha ser potència de 2. Per la fórmula dels graus d'extensions de cossos, trobem que el polinomi mínim de $\phi(\frac{\varpi}{\delta})$ sobre $\mathbb{Q}$ també ha ser potència de 2.

El teorema 4.19 implica que $\phi(\frac{\varpi}{\delta})$ és arrel de $D_\delta = xP_\delta(x^4)$. Com que clarament $\phi(\frac{\varpi}{\delta}) \neq 0$, sabem que $\phi(\frac{\varpi}{\delta})$ és arrel de $P_\delta(x^4)$. Pel mateix teorema, $P_\delta(x^4)$ té grau $N(\delta) - 1$ i és irreductible sobre $\mathbb{Q}(i)$. Per tant, el polinomi mínim de $\phi(\frac{\varpi}{\delta})$ sobre $\mathbb{Q}(i)$ té grau $N(\delta) - 1$. Per una banda, quan $p = \delta$ per $p \equiv 3 \pmod 4$, tenim $N(\delta) - 1 = p^2 - 1 = (p+1)(p-1)$. Consegüentment, $p^2 - 1$ és potència de 2 si, i només si, $p = 3$ (que és un nombre primer de Fermat). Per altra banda, quan $p = \delta\bar{\delta}$ per $p \equiv 1 \pmod 4$, tenim que $N(\delta) - 1 = p - 1$ és potència de 2 si, i només si, p és un primer de Fermat. D'aquesta manera, queda demostrat que els únics primers que divideixen n són primers de Fermat.

Per a completar la demostració, cal veure que $p^2 \nmid n$. Suposem que existeix p primer de Fermat tal que $p^2 | n$. Aleshores existeix $\delta \in \mathbb{Z}[i]$ primer senar tal que $\delta^2 | n$. Anàlogament al raonament anterior,

$$z_0 = \phi\left(\frac{\varpi}{\delta^2}\right) \in \mathbb{Q}\left(i, \phi\left(\frac{\varpi}{n}\right)\right) \tag{5.10}$$

la qual cosa implica que $\phi\left(\frac{\varpi}{\delta^2}\right)$ és construïble. És per això que el grau del polinomi mínim de $\phi\left(\frac{\varpi}{\delta^2}\right)$ sobre $\mathbb{Q}(i)$ ha de ser una potència de 2. Arribarem a contradicció en veure que el grau del polinomi mínim en qüestió és $N(\delta)(N(\delta) - 1)$ perquè $N(\delta)$ és o bé p o bé p^2. Com que δ és senar, el teorema 4.19 implica que

$$\phi\left(\frac{\varpi}{\delta}\right) = \phi\left(\delta\frac{\varpi}{\delta^2}\right) = i^\epsilon z_0 \frac{P_\delta(z_0^4)}{Q_\delta(z_0^4)} \tag{5.11}$$

Atès que $\phi(\frac{\varpi}{\delta})$ és arrel de $P_\delta(x^4)$, l'expressió (5.11) ens permet escriure

$$0 = P_\delta\left(\left(\phi\left(\frac{\varpi}{\delta}\right)\right)^4\right) = P_\delta\left(z_0^4 \frac{P_\delta(z_0^4)^4}{Q_\delta(z_0^4)^4}\right) \tag{5.12}$$

Si escrivim $P_\delta(x) = x^d + a_1 x^{d-1} + ... + a_d$ amb $d = (N(\delta) - 1)/4$, l'equació (5.12) indica que z_0 és arrel de

$$\tilde{P}(x) = x^{4d} P_\delta(x^4)^{4d} + a_1 x^{4d-4} P_\delta(x^4)^{4d-4} Q_\delta(x^4)^4 + ... + a_d Q_\delta(x^4)^{4d} \in \mathbb{Z}[i][x] \tag{5.13}$$

Aquest polinomi té grau $4d(4d+1) = (N(\delta) - 1)N(\delta)$ ja que $P_\delta(x), Q_\delta(x) \in \mathbb{Z}[i][x]$ tenen grau d. Al teorema 4.19 també s'ha vist que δ divideix $a_1, ..., a_d$. Per tant, $P_\delta(x) \equiv x^d \pmod \delta$. Aleshores

$$\tilde{P}(x) \equiv x^{N(\delta)(N(\delta)-1)} \pmod \delta$$

Com que $Q_\delta(0) = 1$, tenim $\tilde{P}(0) = a_d Q_\delta(0) = a_d$. Al teorema 4.19 és demostra que a_d no és divisible entre δ^2. Per tant, pel criteri d'Eisenstein, $\tilde{P}(x)$ és irreductible sobre $\mathbb{Q}(i)$. Així doncs, el polinomi mínim de z_0 sobre $\mathbb{Q}(i)$ té grau $N(\delta)(N(\delta)-1)$. Amb això, queda demostrat aquest teorema. □

Observació 5.10. Els únics primers de Fermat que es coneixen són els cinc primers: $3, 5, 17, 257$ i 65537. Pel teorema 5.9, doncs, els primers n tals que els punts de n-divisió de la lemniscata es poden construir amb regle i compàs (amb $n < 100$) són 1, 2, 3, 4, 5, 6, 8, 10, 12, 15, 16, 17, 20, 24, 30, 32, 34, 40, 48, 51, 60, 64, 68, 80, 85, 96.

$1 = 2^0$	$3 = 2^0 \cdot 3$	$5 = 2^0 \cdot 5$	$15 = 2^0 \cdot 3 \cdot 5$	$17 = 2^0 \cdot 17$	$51 = 2^0 \cdot 3 \cdot 17$
$2 = 2^1$	$6 = 2^1 \cdot 3$	$10 = 2^1 \cdot 5$	$30 = 2^1 \cdot 3 \cdot 5$	$34 = 2^1 \cdot 17$	
$4 = 2^2$	$12 = 2^2 \cdot 3$	$20 = 2^2 \cdot 5$	$60 = 2^2 \cdot 3 \cdot 5$	$68 = 2^2 \cdot 17$	
$8 = 2^3$	$24 = 2^3 \cdot 3$	$40 = 2^3 \cdot 5$			
$16 = 2^4$	$48 = 2^4 \cdot 3$	$80 = 2^4 \cdot 5$			
$32 = 2^5$	$96 = 2^5 \cdot 3$				
$64 = 2^6$					$85 = 2^0 \cdot 5 \cdot 17$

5.2 Plantejament alternatiu

En aquest apartat es presenta una construcció *alternativa* de les extensions lemnatòmiques. En aquest cas, es construiexen a partir d'adjuntar els β-punts de divisió de la lemniscata, $\phi(\frac{2\varpi}{\beta})$ amb a $\beta \in \mathbb{Z}[i]$ senar, a $\mathbb{Q}(i)$. L'origen d'aquest enfocament ja no és purament geomètric sinó que respon al vincle subjacent que existeix amb el camp de les funcions el·líptiques.
En primer lloc, doncs, es donaran algunes nocions bàsiques de funcions el·líptiques que ens permetran adonar-nos que, en efecte, ϕ és una funció el·líptica. Posteriorment, s'introduiran la funció $\wp$ de Weierstrass i el concepte de corba el·líptica, que combinats ens permetran justificar el perquè d'aquesta construcció alternativa de les extensions lemnatòmiques. Els primers apartats d'aquesta subsecció es fonamenten principalment en les idees exposades en els capítols més elementals de [17], [18], [19] i [20]. La vinculació algebraica d'aquests conceptes amb el tema del nostre treball s'inspira en [11] i [14]. Finalment, aconseguirem definir els *polinomis lemnatòmics* Λ_β, que garantiran la factorització de D_β sobre $\mathbb{Q}(i)$ i en demostrarem la seva irreductibilitat sobre $\mathbb{Q}(i)$.

5.2.1 Fonaments de funcions el·líptiques

Definició 5.11. *Entenem per xarxa en el pla complex $\mathbb{C}$ un subgrup que és lliure de dimensió 2 com a $\mathbb{Z}$-mòdul i que genera $\mathbb{C}$ sobre els reals.*

Notació 3. *Sigui $\{\omega_1, \omega_2\}$ una base de la xarxa $\mathcal{L}$ sobre $\mathbb{Z}$. Llavors escrivim $\mathcal{L} = [\omega_1, \omega_2]$.*

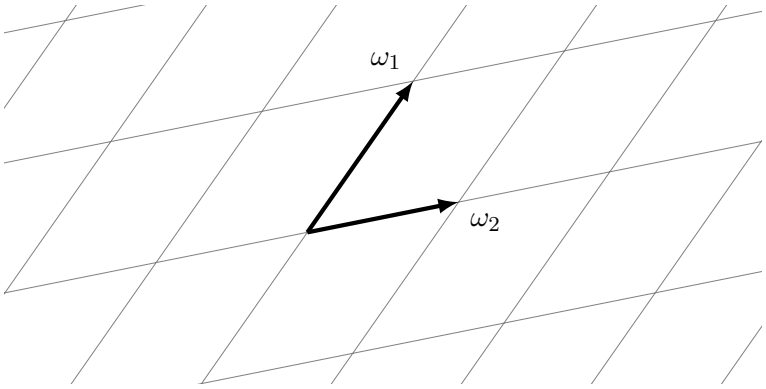

Figura 4: Xarxa generada pels vectors ω_1 i ω_2.

Observació 5.12. Assumim $Im\left(\frac{\omega_1}{\omega_2}\right) > 0$, i.e. $\frac{\omega_1}{\omega_2}$ viu al semiplà superior $\{x+iy, y > 0\}$.

Definició 5.13. *Una funció el·líptica respecte de $\mathcal{L}$ és una funció meromorfa a $\mathbb{C}$ que és $\mathcal{L}$-periòdica, i.e.*

$$f(z+\omega) = f(z), \quad \forall z \in \mathbb{C}, \omega \in \mathcal{L}$$

Habitualment, els elements $\omega \in \mathcal{L}$ que verifiquen aquesta condició s'anomenen períodes.

Observació 5.14. f $\mathcal{L}$-periòdica, amb $\mathcal{L} = [\omega_1, \omega_2] \iff f(z+\omega_1) = f(z) = f(z+\omega_2)$

Observació 5.15. La proposició 4.1 i el teorema 4.2 indiquen que les funcions ϕ i ϕ' són funcions meromorfes i de xarxa periòdica $\mathcal{L} = \mathbb{Z}(1+i)\varpi + \mathbb{Z}(1-i)\varpi$. Per tant, podem afirmar que són funcions el·líptiques respecte de $\mathcal{L} = \mathbb{Z}(1+i)\varpi + \mathbb{Z}(1-i)\varpi$.

Definició 5.16. *Sigui $\mathcal{L} = [\omega_1, \omega_2]$ i $\alpha \in \mathbb{C}$. Definim paral·lelogram fonamental el conjunt de punts de la forma $\alpha + t_1\omega_1 + t_2\omega_2$, amb $t_i \in [0,1], i \in \{1,2\}$.*

Teorema 5.17. *Sigui P el paral·lelogram fonamental de $\mathcal{L}$ i suposem que la funció el·líptica f no té pols a la frontera ∂P. Aleshores, la suma de tots els residus de f a P és 0.*

Demostració. En virtut del teorema dels residus,

$$2\pi i \sum_{a_i \in P} Res(f, a_i) = \int_{\partial P} f(z)dz = 0$$

perquè, en ser f $\mathcal{L}$-periòdica, es cancel·len els costats oposats. □

Observació 5.18. Notem que una funció el·líptica es pot concebre com una funció meromorfa al tor complex $\mathbb{C}/\mathcal{L}$. Així doncs, una funció el·líptica entera (i.e. sense pols) ha de ser constant en virtut del teorema de Liouville perquè $\mathbb{C}/\mathcal{L}$ és isomorf al tor complex, que és un compacte. Per tant, una funció el·líptica no trivial ha de tenir, com a mínim, 2 pols al tor.

5.2.2 Funció $\wp$ de Weierstrass

En aquest apartat veurem que l'existència de funcions el·líptiques es pot demostrar a partir de definir una nova funció que anomenem funció $\wp$ de Weierstrass.

Definició 5.19. *La funció $\wp$ de Weierstrass associada a una xarxa $\mathcal{L}$ es defineix com*

$$\wp(z) = \frac{1}{z^2} + \sum_{\omega \in \mathcal{L}'} \left[\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right]$$

on la suma (infinita) recorre el conjunt dels períodes no nuls de $\mathcal{L}$ denotat per $\mathcal{L}'$.

Observació 5.20. El segon terme del sumatori ens assegura que la suma és convergent. D'aquesta manera, la funció $\wp$ és meromorfa i només té pols d'ordre 2 als punts de la xarxa $\omega \in \mathcal{L}'$.

Proposició 5.21. *La funció $\wp$ de Weierstrass verifica les següents propietats:*

(i) $\wp(-z) = \wp(z)$

(ii) $\wp'(z) = -2\sum_{\omega \in \mathcal{L}} \frac{1}{(z-\omega)^3}$

(iii) $\wp'(-z) = -\wp'(z)$

(iv) Si $\mathcal{L} = [\omega_1, \omega_2]$, llavors $\wp$ i $\wp'$ són periòdiques en ω_1 i ω_2.

Demostració. La propietat (i) és immediata perquè la suma de $\wp$ recorre tant els valors positius com els valors negatius de la xarxa. La propietat (ii) es troba diferenciant els termes de la definició de $\wp$ (ara la suma de $\wp'$ recorre tots els valors $\omega \in \mathcal{L}$). De l'expressió trobada de $\wp'$, és immediat comprovar la propietat (iii). Vegem l'última propietat. La periodicitat de $\wp'$ és immediata per la propietat (ii). Aleshores, com que $\wp'$ és la derivada

de $\wp$, sabem que han d'existir constants C_i tals que $\wp(z+\omega_i) = \wp(z)+C_i$, per a $i \in \{1,2\}$. Si prenem $z = -\omega_i/2$ (que no és cap pol de $\wp$), obtenim

$$\wp\left(\frac{\omega_i}{2}\right) = \wp\left(-\frac{\omega_i}{2}\right) + C_i$$

Per la propietat (i), veiem que $C_i = 0, i \in \{1,2\}$. Per tant, $\wp$ és periòdica en ω_1, ω_2. □

Teorema 5.22. *El conjunt de les funcions el·líptiques (respecte d'una xarxa $\mathcal{L}$) forma un cos generat per $\wp$ i $\wp'$ sobre el cos dels nombres complexos.*

Demostració. Sigui f una funció el·líptica. Aleshores podem escriure f com a suma d'una funció el·líptica parella i una de senar:

$$f(z) = \frac{f(z)+f(-z)}{2} + \frac{f(z)-f(-z)}{2}$$

Si f és una funció senar, llavors el producte $f\wp'$ és parell. Per tant, n'hi ha prou amb veure que $\mathbb{C}(\wp)$ és el cos de les funcions el·líptiques parelles, i.e. si f és parella, aleshores f és una funció racional de $\wp$. Vegem-ho.
Suposem que f és parella i que té un zero d'ordre m en algun punt p. Aleshores f també té un zero de mateix ordre a $-p$ perquè $f^{(k)}(p) = (-1)^k f^{(k)}(-p)$, pel fet de ser parella. Similarment pels pols. Si $p \equiv -p \pmod{\mathcal{L}}$, llavors l'asserció anterior es compleix en un sentit més fort afirmant que f té un zero (o pol) d'ordre parell a p. Comprovem-ho:
Si $p \equiv -p \pmod{\mathcal{L}}$, aleshores $2p \equiv 0 \pmod{\mathcal{L}}$. Existeixen exactament quatre punts a $\mathcal{L}$ amb aquesta propietat: $\{0, \frac{\omega_1}{2}, \frac{\omega_2}{2}, \frac{\omega_1+\omega_2}{2}\}$. Tenint en compte que si f és parella, llavors f' és senar (i.e. $f'(-x) = -f'(x)$), com que $p \equiv -p \pmod{\mathcal{L}}$, tenim $f'(p) = 0$. De manera que f té un zero d'ordre almenys 2.

- Si $p \not\equiv 0 \pmod{\mathcal{L}}$, l'argument anterior prova que la funció $g(z) := \wp(z) - \wp(p)$ també té un zero d'almenys ordre 2 (i, per tant, d'ordre exactament 2 perquè $\wp$ només té un pol d'ordre 2 al tor). Consegüentment, $f(p)/g(p)$ és parella, el·líptica i holomorfa a p.
  - Si $f(p)/g(p) \neq 0$, llavors $ord_p f = 2$.
  - Si $f(p)/g(p) = 0$, aleshores f/g té un zero d'ordre almenys 2 a p i podem repetir l'argument.
- Si $p \equiv 0 \pmod{\mathcal{L}}$, en aquest cas definim la funció $g = \frac{1}{\wp}$ i argumentem de manera anàloga.

Havent demostrat això, considerem una família de punts p_i, $i \in \{1, ..., r\}$, que conté un representant de cada classe $(p, -p) \pmod{\mathcal{L}}$ on f té un pol o un zero diferent a la classe de $\mathcal{L}$. Sigui

$$m_i = \begin{cases} ord_{p_i} f & , \quad 2p_i \not\equiv 0 \pmod{\mathcal{L}} \\ \frac{1}{2} ord_{p_i} f & , \quad 2p_i \equiv 0 \pmod{\mathcal{L}} \end{cases}$$

Hem vist que, per a $a \in \mathbb{C}, a \not\equiv 0 \pmod{\mathcal{L}}$, la funció $\wp(z) - \wp(a)$ té un zero d'ordre 2 a a si, i només si, $2a \equiv 0 \pmod{\mathcal{L}}$ i té dos zeros diferents d'ordre 1 a a i $-a$ altrament. Així doncs, $\forall z \not\equiv 0 \pmod{\mathcal{L}}$ la funció

$$\prod_{i=1}^{r} [\wp(z) - \wp(p_i)]^{m_i}$$

té el mateix ordre a z que a f. El quocient del productori anterior entre f és aleshores una funció el·líptica sense zeros ni pols, és a dir, una constant. □

Observació 5.23. El que ve a dir el teorema 5.22 és que tota funció el·líptica respecte de $\mathcal{L}$ és una funció racional del $\wp(z)$ i $\wp'(z)$. En particular, recordant l'observació 5.15, podem afirmar que les funcions ϕ i ϕ' són funcions racionals de $\wp$ i $\wp'$. En particular, analitzant els zeros i pols, es troba que

$$\boxed{\phi(z) = -2\frac{\wp(z)}{\wp'(z)}\,, \qquad \phi'(z) = \frac{4\wp(z)^2 - 1}{4\wp(z)^2 + 1}}$$

Proposició 5.24. *El desenvolupament en sèrie de potències de $\wp$ és*

$$\wp(z) = \frac{1}{z^2} + \sum_{n=1}^{\infty}(2n+1)s_{n+2}(\mathcal{L})z^{2n}, \quad s_k(\mathcal{L}) := \sum_{\omega\neq 0}\frac{1}{\omega^k}$$

Demostració.

$$\wp(z) = \frac{1}{z^2} + \sum_{\omega\in\mathcal{L}'}\left[\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}\right] = \frac{1}{z^2} + \sum_{\omega\in\mathcal{L}'}\left[\frac{1}{\omega^2}\left(1 + \frac{z}{\omega} + \frac{z^2}{\omega^2} + ...\right)^2 - \frac{1}{\omega^2}\right] =$$

$$= \frac{1}{z^2} + \sum_{\omega\in\mathcal{L}'}\left[\frac{1}{\omega^2}\left(\frac{z}{\omega} + \frac{z^2}{\omega^2} + ...\right)^2\right] = \frac{1}{z^2} + \sum_{\omega\in\mathcal{L}'}\sum_{m=1}^{\infty}\frac{1}{\omega^2}(m+1)\left(\frac{z}{\omega}\right)^m =$$

$$= \frac{1}{z^2} + \sum_{m=1}^{\infty}\left(\sum_{\omega\neq 0}\frac{m+1}{\omega^{m+2}}\right)z^m = \frac{1}{z^2} + \sum_{n=1}^{\infty}(2n+1)s_{n+2}(\mathcal{L})z^{2n}, \quad s_k(\mathcal{L}) := \sum_{\omega\neq 0}\frac{1}{\omega^k}$$

□

5.2.3 Corbes el·líptiques

Definició 5.25. *Sigui $\mathcal{L}$ una xarxa. La corba el·líptica associada a $\mathcal{L}$ es defineix com $E_{\mathcal{L}} = \mathbb{C}/\mathcal{L}$. La relació d'equivalència que determina aquest conjunt quocient estableix que dos nombres $z, z' \in \mathbb{C}$ són equivalents si, i només si, $z - z' \in \mathcal{L}$.*

Proposició 5.26. *Considerem la xarxa $\mathcal{L} = \mathbb{Z}(1+i)\varpi + \mathbb{Z}(1-i)\varpi$. Els punts $(\wp(z), \wp'(z))$, amb $z \in \mathbb{C}$, verifiquen l'equació de la corba el·líptica associada a $\mathcal{L}$ és $Y^2 = 4X^3 + X$. Aquesta corba sovint s'anomena equació de Weierstrass i denotem per E el conjunt de punts sobre aquesta corba.*

Demostració. A partir del desenvolupament en sèrie de potències de $\wp$ vist a la proposició 5.24 i de la corresponent expressió derivada, es pot comprovar que

$$\wp'(z)^2 = 4\wp(z)^3 - g_2(\mathcal{L})\wp(z) - g_3(\mathcal{L})$$

on $g_2(\mathcal{L}) := 60s_4(\mathcal{L})$ i $g_3(\mathcal{L}) := 140s_6(\mathcal{L})$ (es pot consultar les pàgines 436-437 de [16] per a veure'n la deducció). En particular, a [11] es demostra amb tot detall que $g_2(\mathcal{L}') = \frac{1}{4}$ i $g_3(\mathcal{L}') = 0$, on $\mathcal{L}' = \mathbb{Z}2\varpi + \mathbb{Z}2\varpi i$. Fixem-nos que

$$\mathcal{L}' = \mathbb{Z}(1+1)\varpi + \mathbb{Z}(1+2i-1)\varpi = (1+i)[\mathbb{Z}(1-i)\varpi + \mathbb{Z}(1+i)\varpi] = (1+i)\mathcal{L}$$

Per tant,

$$\frac{1}{4} = g_2(\mathcal{L}') = g_2((1+i)\mathcal{L}) = \frac{1}{(1+i)^4} g_2(\mathcal{L}) = -\frac{1}{4} g_2(\mathcal{L}) \tag{5.14}$$

Clarament, doncs, $g_2(\mathcal{L}) = -1$ i $g_3(\mathcal{L}) = 0$. Això demostra que, en efecte, els punts $(\wp(z), \wp'(z))$ verifiquen l'equació de Weierstrass $Y^2 = 4X^3 + X$. □

Definició 5.27. *Siguin C_1 i C_2 dues corbes algebraiques (i.e. els conjunts de zeros de dues equacions polinòmiques) definides sobre un cos K. Una transformació birracional entre C_1 i C_2 és un parell de funcions racionals $f : C_1 \to C_2$ i $g : C_2 \to C_1$ tals que f i g són inverses l'una de l'altra quan es restringeixen als seus respectius dominis.*

Proposició 5.28. *Les corbes $C_1 = \{Y^2 = 4X^3 + X\}$ i $C_2 = \{y^2 = 1 - x^4\}$ estan relacionades per la transformació birracional $\psi : C_1 \to C_2$ definida per*

$$(X, Y) \mapsto (x, y) = \left(-2\frac{X}{Y}, \frac{4X^2 - 1}{4X^2 + 1}\right)$$

Demostració. Per una banda, a la proposició 5.26 hem vist que $\wp$ i $\wp'$ parametritzen la corba $Y^2 = 4X^3 + X$. Per altra banda, recordem per la proposició 3.1 que $\phi'(z)^2 = 1 - \phi(z)^4$, és a dir, que ϕ i ϕ' parametritzen la corba $y^2 = 1 - x^4$. Si invoquem la relació entre ϕ, ϕ' i $\wp, \wp'$ de l'observació 5.23, trobem directament el resultat de l'enunciat. □

5.2.4 Extensions lemnatòmiques a partir de funcions el·líptiques

Després d'aquesta exposició sintètica sobre les funcions i corbes el·líptiques, ja podem introduir la construcció alternativa de les extensions lemnatòmiques.

Definició 5.29. *Sigui $\beta \in \mathbb{Z}[i]$. S'anomena cos lemnatòmic β-èsim el cos de descomposició del polinomi $D_\beta(x)$ sobre $\mathbb{Q}(i)$.*

Observació 5.30. Ens preguntem per què definim les extensions lemnatòmiques sobre $\mathbb{Q}(i)$ i no sobre $\mathbb{Q}$. Es pot consultar a [20] que les corbes el·líptiques defineixen estructures de grups. En particular, podem considerar endomorfismes que enviïn els punts de la corba a altres punts de la mateixa corba, tot preservant-ne l'estructura de grup. Observem que, sobre la corba el·líptica $E : \{y^2 = x^3 + x\}$, podem definir l'endomorfisme $\xi : E \to E$ (sovint referit com a *multiplicació complexa*) que verifica $\xi(x, y) = (-x, iy)$. Això és fàcil de comprovar perquè $(iy)^2 = -y^2 = -(x^3 + x) = (-x)^3 + (-x)$, és a dir que per tot $(x, y) \in E$ tenim que $(-x, iy) \in E$. Sigui $K/\mathbb{Q}$ una extensió de Galois tal que $i \in K$ i $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$. Sigui $E(K) = \{(x, y) \in E : x, y \in K\}$ el conjunt de punts sobre la corba E amb coordenades a K. Per tot punt $P \in E(K)$, tenim dues maneres d'obtenir un altre punt a $E(K)$. Una podria ser aplicar l'endomorfisme $\xi : E \to E$ a P i l'altra seria aplicar σ sobre P. La pregunta evident seria si $\sigma(\xi(P)) = \xi(\sigma(P)), \forall P \in E(K)$. Fent servir les definicions trobem

$$\sigma(\xi(P)) = \sigma(-x, iy) = (\sigma(-x), \sigma(iy)) = (-\sigma(x), \sigma(i)\sigma(y))$$

$$\xi(\sigma(P)) = \xi(\sigma(x), \sigma(y)) = (-\sigma(x), i\sigma(y))$$

Així doncs, les accions de ξ i σ commuten sobre $E(K)$ sempre que $\sigma(i) = i$. En altres paraules, commuten si $\sigma \in \mathrm{Gal}(K/\mathbb{Q}(i))$. És per aquesta raó que és convenient estudiar les extensions lemnatòmiques sobre $\mathbb{Q}(i)$ més que sobre $\mathbb{Q}$.

Proposició 5.31. *Sigui $\beta \in \mathbb{Z}[i]$ senar i δ un β-generador de torsió. Aleshores*

$$\mathbb{Q}\left(i, \phi\left(\frac{2\varpi}{\beta}\right)\right) = \mathbb{Q}\left(i, \phi(\delta)\right) = \mathbb{Q}\left(\phi(\delta), \phi'(\delta)\right) = \mathbb{Q}\left(\wp(\delta), \wp'(\delta)\right) = \mathbb{Q}\left(i, E[\beta]\right)$$

on $\mathbb{Q}\left(i, E[\beta]\right)$ és el cos obtingut d'adjuntar a $\mathbb{Q}(i)$ les coordenades dels β-punts de torsió de E.

Demostració. En primer lloc, demostrem que $\frac{2\varpi}{\beta}$ és generador de torsió. Com que β és senar, sabem que $u\beta + v(1+i) = 1$ per alguns $u, v \in \mathbb{Z}[i]$. Si multipliquem aquesta expressió per $\delta_\beta = \frac{(1+i)\varpi}{\beta}$ trobem que $\frac{(1+i)\varpi}{\beta} - v\frac{2\varpi}{\beta} = (1+i)u\varpi$, la qual cosa és equivalent a $v\frac{2\varpi}{\beta} \equiv \delta_\beta \pmod{\mathcal{L}}$. Per l'observació 4.18, tenim que $\frac{2\varpi}{\beta}$ és un β-generador de torsió.

Siguin $\delta, \tilde{\delta}$ dos β-generadors de torsió. Per l'observació 4.18, $\delta \equiv \alpha\tilde{\delta} \pmod{\mathcal{L}}$ per algun $\alpha \in (\mathbb{Z}[i]/\beta\mathbb{Z}[i])^*$, on podem assumir que α és senar perquè β ho és (si α és senar, triem $\alpha + \beta$). Llavors, $\phi(\delta) = \phi(\alpha\tilde{\delta})$ i $\phi(\alpha\tilde{\delta}) \in \mathbb{Q}\left(i, \phi(\delta)\right)$ pel teorema 4.19. Triant $\tilde{\delta} = \frac{2\varpi}{\beta}$, queda demostrada la primera igualtat.
La segona igualtat és immediata per la llei d'addició vista a la proposició 4.1. La tercera igualtat es verifica per l'existència de la transformació birracional vista a la proposició 5.23. Finalment, la darrera igualtat es compleix perquè $(\wp(\delta), \wp'(\delta)) \in E[\beta]$ genera $E[\beta]$ com a $\mathbb{Z}[i]$-mòdul. □

Teorema 5.32. *Sigui $\beta \in \mathbb{Z}[i]$ senar, $K = \mathbb{Q}(i)$ i $\tilde{L} = \mathbb{Q}(i, \phi(\frac{2\varpi}{\beta}))$. Per a cada $\sigma \in Gal(\tilde{L}/K)$, existeix un únic $\alpha \in (\mathbb{Z}[i]/\beta\mathbb{Z}[i])^*$ tal que $\sigma(\phi(\delta)) = \phi(\alpha\delta)$ per qualsevol β-generador de torsió δ. A més, l'aplicació $\sigma \mapsto [\alpha]$ defineix l'isomorfisme*

$$Gal(\tilde{L}/K) \cong (\mathbb{Z}[i]/\beta\mathbb{Z}[i])^*$$

Demostració. Els arguments usats per a demostar el teorema 5.3 serveixen per a justificar la injecció

$$\mathrm{Gal}(\tilde{L}/K) \hookrightarrow (\mathbb{Z}[i]/\beta\mathbb{Z}[i])^* \tag{5.15}$$

Fent ús de la teoria de cossos de classe de raig de [18], podem esciure $\mathfrak{L} = \mathbb{Q}\left(i, \wp\left(\delta_{2(1+i)\beta}\right)^2\right)$ que és el cos de classe de raig[3] de $\mathbb{Q}(i)$ pel mòdul $2(1+i)\beta$. Com que $\mathbb{Z}[i]$ és un domini d'ideals principals, $\mathbb{Z}[i]^* = \{\pm 1, \pm i\}$ i β és senar, l'aplicació d'Artin i el teorema xinès del residu impliquen que

$$\mathrm{Gal}(\mathfrak{L}/K) \cong (\mathbb{Z}[i]/2(1+i)\beta\mathbb{Z}[i])^*/\mathbb{Z}[i]^* \cong (\mathbb{Z}[i]/\beta\mathbb{Z}[i])^*$$

Fent servir l'observació 5.23, també tenim

$$\mathfrak{L} = \mathbb{Q}\left(i, \wp'\left(\delta_{2(1+i)\beta}\right)^2\right) = \mathbb{Q}\left(i, \phi'\left(\frac{\varpi}{2\beta}\right)\right)$$

[3] Un cos de nombres algebraics $\mathcal{K}$ és una extensió finita de $\mathbb{Q}$. El propòsit principal de la teoria de cossos de classe és descriure totes les extensions finites de $\mathcal{K}$. Per exemple, quan $\mathcal{K} = \mathbb{Q}$, el teorema de Kronecker-Weber afirma que tota extensió abeliana de $\mathbb{Q}$ és un subcòs de l'extensió ciclotòmica $\mathbb{Q}(\zeta_n)$, per algun $n \in \mathbb{Z}_+$. De manera similar, tota extensió abeliana de $\mathbb{Q}(i)$ és un subcòs de l'extensió lemnatòmica $L = \mathbb{Q}(i, \phi(\frac{\varpi}{n}))$ per algun $n \in \mathbb{Z}_+$. Per a saber-ne més sobre teoria de cossos de classe i l'aplicació d'Artin, es pot consultar [18] i [21].

Derivant la llei d'addició 4.1 per a $\phi(z-\frac{\varpi}{2})$ trobem la identitat

$$\phi'\left(z-\frac{\varpi}{2}\right)=2\frac{\phi(z)}{1+\phi(z)^2} \tag{5.16}$$

Com que β és senar, existeix $\gamma\in\mathbb{Z}[i]$ tal que $2(1+i)\gamma-\beta=i^\epsilon$. Aleshores, $\gamma\delta_\beta-\frac{\varpi}{2}=i^\epsilon\frac{\varpi}{2\beta}$. Fent servir $\phi'(iz)=\phi'(z)$ i (5.16), obtenim

$$\phi'\left(\frac{\varpi}{2\beta}\right)=\phi'\left(i^\epsilon\frac{\varpi}{2\beta}\right)=\phi'\left(\gamma\delta_\beta-\frac{\varpi}{2}\right)=2\frac{\phi(\gamma\delta_\beta)}{1+\phi(\gamma\delta_\beta)^2}\in\mathbb{Q}\left(i,\phi(\delta_\beta)\right)=\tilde{L}$$

Per això, $K=\mathbb{Q}(i)\subseteq\mathfrak{L}\subseteq\tilde{L}$, de manera que $|\mathrm{Gal}(\tilde{L}/K)|\geq|\mathrm{Gal}(\mathfrak{L}/K)|=|(\mathbb{Z}[i]/\beta\mathbb{Z}[i])^*|$ Com que (5.15) és una injecció, trobem que $\mathfrak{L}=\tilde{L}$. Per tant, trobem l'isomorfisme que buscàvem. □

5.2.5 Polinomis lemnatòmics

Definició 5.33. *Sigui $\beta\in\mathbb{Z}[i]$ senar. Fixat un β-generador de torsió $\delta_\beta=\frac{(1+i)\varpi}{\beta}$, definim polinomi lemnatòmic β-èsim com*

$$\Lambda_\beta(x):=\prod_{[\alpha]\in(\mathbb{Z}[i]/\beta\mathbb{Z}[i])^*}(x-\phi(\alpha\delta_\beta))$$

Observació 5.34. (a) Notem que la definició dels polinomis lemnatòmics no depèn de la tria del β-generador de torsió δ_β. En particular, si recordem l'observació 4.18 és immediat reconèixer que les arrels de Λ_β són tots els $\phi(\delta)$ amb δ recorrent tots els β-generadors de torsió equivalents a la xarxa.

(b) Siguin β i β' dos enters de Gauss associats. Aleshores $\Lambda_\beta=\Lambda'_\beta$ ja que Λ_β només depèn de l'ideal generat per β.

(c) Per la definició de polinomi lemnatòmic β-èsim, és clar que $\Lambda_\beta(x)$ és mònic.

(d) Per la geometria de la lemniscata, és evident que la divisió en 1 segment de mateixa longitud d'arc és trivial. És a dir, el polinomi lemnatòmics 1-èsim només té l'arrel 0. D'aquesta manera, $\Lambda_1(x)=x$.

Lema 5.35. *Siguin $\beta\in\mathbb{Z}[i]$ senar i Λ_β un polinomi lemnatòmic β-èsim. Llavors $\Lambda_\beta\in\mathbb{Z}[i][x]$ és un polinomi mònic de grau $|\,(\mathbb{Z}[i]/\beta\mathbb{Z}[i])^*\,|$.*

Demostració. Siguin $K=\mathbb{Q}(i)$ i $\tilde{L}=\mathbb{Q}(i,\phi(\frac{2\varpi}{\beta}))$. N'hi ha prou amb veure $\Lambda_\beta(x)\in\mathbb{Z}[i][x]$. Pel teorema 5.32, les arrels de Λ_β permuten sota l'acció de $\mathrm{Gal}(L/K)$ i, per tant, els coeficients de Λ_β viuen a $\mathbb{Q}(i)$. Les arrels de Λ_β són enters algebraics (i.e. arrels d'un polinomi mònic de coeficients enters) ja que també són arrels del polinomi mònic de β-divisió $D_\beta=xP_\beta(x^4)\in\mathbb{Z}[i]$. Per tant, $\Lambda_\beta(x)\in\mathbb{Z}[i][x]$. □

Observació 5.36. De mateixa manera que els polinomis ciclotòmics garanteixen la factorització de x^n-1 sobre $\mathbb{Q}$, els polinomis lemnatòmics són els factors irreductibles de D_β sobre $\mathbb{Q}(i)$.

Proposició 5.37. *Sigui $\beta \in \mathbb{Z}[i]$ senar i $D_\beta(x)$ el polinomi de β-divisió associat a β. Aleshores*

$$D_\beta(x) = \prod_{\gamma|\beta} \Lambda_\gamma(x)$$

on el productori recorre tots els divisors normalitzats γ de β.

Demostració. Pel teorema 4.19, les arrels de D_β són $\phi(\alpha\delta_\beta)$ amb $[\alpha] \in \mathbb{Z}[i]/\beta\mathbb{Z}[i]$. Per tant,

$$D_\beta(x) = \prod_{[\alpha]\in\mathbb{Z}[i]/\beta\mathbb{Z}[i]} (x - \phi(\alpha\delta_\beta)) \tag{5.17}$$

Fent servir la noció de màxim comú divisor en l'anell d'enters de Gauss vista a la definició 4.10, sabem que tot nombre $\alpha \in \mathbb{Z}[i]$ dóna un divisor $\gamma = mcd(\alpha, \beta)$ de β. Ja que diferents valors de η poden donar el mateix divisor γ, podem reorganitzar la factorització de (5.17) de manera que

$$D_\beta(x) = \prod_{\gamma|\beta} \prod_{\substack{[\alpha]\in\mathbb{Z}[i]/\beta\mathbb{Z}[i] \\ \gamma=mcd(\alpha,\beta)}} (x - \phi(\alpha\delta_\beta)) \tag{5.18}$$

Per a un divisor γ de β, la part corresponent de factorització és

$$\prod_{\substack{[\alpha]\in\mathbb{Z}[i]/\beta\mathbb{Z}[i] \\ \gamma=mcd(\alpha,\beta)}} (x - \phi(\alpha\delta_\beta)) \tag{5.19}$$

Observem que $\gamma = mcd(\alpha, \beta)$ implica que existeix $\eta \in \mathbb{Z}[i]$ tal que $\alpha = \eta\gamma$ i $\beta = \gamma\frac{\beta}{\gamma}$, de manera que $mcd(\eta, \frac{\beta}{\gamma}) = 1$. Fixem-nos que llavors tenim dos $\frac{\beta}{\gamma}$-generadors de torsió: $\delta_{\gamma\frac{\beta}{\gamma}}$ i $\delta_{\frac{\beta}{\gamma}}$ (el primer ho és perquè δ_β ho és i el segon es pot demostrar de manera anàloga a com es veu a la proposició 5.31). Per l'observació 4.18, llavors, podem reescriure (5.19) com

$$\prod_{\substack{[\eta\gamma]\in\mathbb{Z}[i]/\left(\gamma\frac{\beta}{\gamma}\right)\mathbb{Z}[i] \\ mcd\left(\eta,\frac{\beta}{\gamma}\right)=1}} \left(x - \phi\left(\eta\gamma\delta_{\gamma\frac{\beta}{\gamma}}\right)\right) = \prod_{\substack{[\eta]\in\left(\mathbb{Z}[i]/\frac{\beta}{\gamma}\mathbb{Z}[i]\right)^* \\ mcd\left(\eta,\frac{\beta}{\gamma}\right)=1}} \left(x - \phi\left(\eta\delta_{\frac{\beta}{\gamma}}\right)\right) \tag{5.20}$$

Anem a entendre aquesta igualtat. Per tal que la classe $[\eta\gamma] \in \mathbb{Z}[i]/\left(\gamma\frac{\beta}{\gamma}\right)\mathbb{Z}[i]$ fos la classe del zero, tindríem que $\gamma\frac{\beta}{\gamma}$ hauria de dividir $\eta\gamma$, però això no pot ser perquè $mcd(\eta, \frac{\beta}{\gamma}) = 1$. Així doncs totes les classes $[\eta\gamma]$ són no nul·les i, per tant, podem identificar-les amb les classes $[\eta] \in \left(\mathbb{Z}[i]/\frac{\beta}{\gamma}\mathbb{Z}[i]\right)^*$. Havent vist això, fixem-nos que (5.20) coincideix amb la definició 5.33 de polinomi lemnatòmic $\frac{\beta}{\gamma}$-èsim. Per tant, la factorització (5.18) es pot reescriure com

$$D_\beta(x) = \prod_{\gamma|\beta} \Lambda_{\frac{\beta}{\gamma}}(x)$$

com que el producte recorre tots els divisors de β i els nombres $\frac{\beta}{\gamma}$ també són divisors de β, podem reetiquetar els índexos i trobem el resultat de la proposició. □

Determinem, ara, el terme constant de Λ_β.

Proposició 5.38. *Sigui $\beta \in \mathbb{Z}[i]$ senar i no unitat. Llavors*

$$\Lambda_\beta(0) = \begin{cases} \pi, & \beta = \alpha\pi^k \\ 1, & altrament \end{cases}$$

on $\alpha \in \mathbb{Z}[i]^*, k \in \mathbb{Z}_+$ i $\pi \in \mathbb{Z}[i]$ és un element primer.

Demostració. Assumim que β és senar i normalitzat. Ja que $\phi'(0) = 1$, podem aplicar la regla de l'Hôpital i el teorema 4.19 per trobar

$$\beta = \lim_{x\to 0} \frac{\phi(\beta x)}{\phi(x)} = \lim_{x\to 0} \frac{P_\beta(\phi(x)^4)}{Q_\beta(\phi(x)^4)} = \frac{P_\beta(0)}{Q_\beta(0)} = P_\beta(0) \tag{5.21}$$

Sigui π un enter de Gauss primer senar normalitzat. Si $\beta = \pi$, llavors la proposició 5.37 implica que $P_\pi(x^4) = \Lambda_\pi(x)$ perquè $\Lambda_1(x) = x$. Fent servir (5.21), trobem $\Lambda_\pi(0) = P_\pi(0) = \pi$. Si $\beta = \pi^k$, procedim per inducció. Suposem que per tot $k \in \{1, ..., n\}$ tenim $\Lambda_{\pi^k}(0) = \pi$. Aleshores, per la proposició 5.37 i per la hipòtesi d'inducció

$$\pi^{n+1} = P_{\pi^{n+1}}(0) = \prod_{k=1}^{n+1} \Lambda_{\pi^k}(0) = \pi^n \Lambda_{\pi^{n+1}}(0)$$

Concloem, doncs, que $\Lambda_{\pi^{n+1}}(0) = \pi$. Suposem que β no es pot expressar com a potència d'un primer. De nou, per la proposició 5.37, tenim

$$\beta = P_\beta(0) = \prod_{\substack{\gamma|\beta, \gamma\neq 1 \\ \gamma\, normalitzat}} \Lambda_\gamma(0) \tag{5.22}$$

Cada potència de primers π^k que divideix β, on π és un primer normalitzat, hem vist que contribueix π al producte (5.22). Consegüentment, els divisors potències de primers de β contribueixen un factor β a (5.22). Per tant

$$\prod_{\substack{\gamma|\beta, \gamma\neq 1 \gamma\neq\pi^k \\ \gamma\, normalitzat}} \Lambda_\gamma(0) = 1$$

Fent servir aquest resultat, podem demostrar inductivament que $\Lambda_\beta(0) = 1$ quan β no és potència d'un primer. □

Lema 5.39 (Lema de Gauss)**.** *Sigui D un domini de factorització única i K el seu cos de fraccions. Llavors tot polinomi primitiu $P(x) \in D[x]$ és irreductible a $D[x]$ si, i només si, també és irreductible a $K[x]$.*

Teorema 5.40. *Sigui $\beta \in \mathbb{Z}[i]$ senar. Aleshores el polinomi lemnatòmic Λ_β és irreductible sobre $\mathbb{Q}(i)$.*

Demostració. Un factor irreductible $\lambda(x)$ de $\Lambda_\beta(x)$ a $\mathbb{Q}(i)[x]$ pertany a $\mathbb{Z}[i][x]$ en virtut del lema de Gauss. Com que $\Lambda_\beta(x)$ és mònic, podem considerar que $\lambda(x)$ també ho és. Les arrels de $\lambda(x)$ són de la forma $\phi(\alpha_i\delta_\beta)$ amb $\alpha_i \in \mathbb{Z}[i]$ i $mcd(\alpha_i, \beta) = 1$, per a $i \in \{1, ..., r\}$ on $r \in \mathbb{Z}_+$. Fixat $\pi \in \mathbb{Z}[i]$ primer senar, considerem el polinomi

$$\lambda_\pi(x) = \prod_{i=1}^{r} (x - \phi(\pi\alpha_i\delta_\beta))$$

En vista del teorema 4.19, podem afirmar que el polinomi $D_\beta(x) = xP_\beta(x^4)$ és separable perquè les seves arrels en el seu cos de descomposició són totes diferents. Aleshores podem dir que $\Lambda_\beta(x)$ és separable sobre $\mathbb{Q}(i)$ i, d'aquí, que és separable mòdul qualsevol primer de $\mathbb{Z}[i]$ que no divideixi el discriminant $\Delta(\Lambda_\beta) \neq 0$. Considerem que $\pi \in \mathbb{Z}[i]$ verifica:

(a) $\pi \equiv 1 \pmod{2(1+i)}$

(b) Λ_β és separable mòdul π

(c) $mcd(\beta, \pi) = 1$

En primer lloc, vegem que $\lambda_\pi(x) \in \mathbb{Z}[i][x]$. Sigui $\sigma \in \mathrm{Gal}(\tilde{L}/K)$ i considerem l'arrel $\phi(\pi\alpha_i\delta_\beta)$ de $\lambda_\pi(x)$. Com que $\alpha_i\delta_\beta$ i $\pi\alpha_i\delta_\beta$ són β-generadors de torsió, el teorema 5.32 implica que existeix $\gamma \in \mathbb{Z}[i]$ coprimer a β tal que

$$\sigma(\phi(\alpha_i\delta_\beta)) = \phi(\gamma\alpha_i\delta_\beta)\,, \qquad \sigma(\phi(\pi\alpha_i\delta_\beta)) = \phi(\pi\gamma\alpha_i\delta_\beta) \tag{5.23}$$

Com que $\phi(\alpha_i\delta_\beta)$ és una arrel de $\lambda(x) \in \mathbb{Z}[i][x]$, la part de la esquerra de (5.23) indica que $\phi(\gamma\alpha_i\delta_\beta)$ també ho és. Aleshores $\phi(\pi\gamma\alpha_i\delta_\beta)$ és arrel de $\lambda_\pi(x)$ per definició. La part dreta de (5.23) indica que aquesta arrel correspon a $\sigma(\phi(\pi\alpha_i\delta_\beta))$. Per tant σ permuta les arrels de $\lambda_\pi(x)$ i llavors $\lambda_\pi(x) \in \mathbb{Z}[i][x]$.
Ara volem demostrar que

$$(a), (b), (c) \Rightarrow \lambda(x) = \lambda_\pi(x) \tag{5.24}$$

Suposem que (5.24) és fals. Sabem que $\lambda(x)$ i $\lambda_\pi(x)$ són mònics, que tenen el mateix grau i que $\lambda(x)$ és irreductible per hipòtesi. Així doncs, suposar que $\lambda(x) \neq \lambda_\pi(x)$ és equivalent a considerar que $\lambda(x)$ i $\lambda_\pi(x)$ són coprimers. Com que les arrels de $\lambda_\pi(x)$ també són arrels de $\Lambda_\beta(x)$, existeix un polinomi mònic $h(x) \in \mathbb{Z}[i][x]$ tal que $\Lambda_\beta(x) = \lambda(x)\lambda_\pi(x)h(x)$. Estudiem les arrels de $\lambda_\pi(x)$ mòdul π. Pel teorema 4.19, tenim

$$\begin{aligned} P_\pi(x^4) &= x^{N(\pi)-1} + a_1 x^{N(\pi)-5} + \cdots + a_{(N(\beta)-1)/4} \\ Q_\pi(x^4) &= a_{(N(\beta)-1)/4} x^{N(\pi)-1} + \cdots + a_1 x + 1 \end{aligned} \tag{5.25}$$

on π divideix tots els $a_i, i \in \{1, \ldots, (N(\beta)-1)/4\}$. Siguin $\mathcal{O}$ l'anell d'enters de $\tilde{L}$ i $\mathfrak{B}$ un ideal primer de $\mathcal{O}$ que divideix $\pi\mathcal{O}$ i suposem que $\phi(\alpha_i\delta_\beta)$ és una arrel de $\lambda(x)$. Aleshores, a $\tilde{L}$

$$\phi(\pi\alpha_i\delta_\beta) = \phi(\alpha_i\delta_\beta)\frac{P_\pi(\phi(\alpha_i\delta_\beta)^4)}{Q_\pi(\phi(\alpha_i\delta_\beta)^4)}$$

Per (5.25), podem reduir aquesta expressió a

$$\phi(\pi\alpha_i\delta_\beta) = \phi(\alpha_i\delta_\beta)^{N(\alpha)} \pmod{\mathfrak{B}}. \tag{5.26}$$

Sigui

$$\tilde{\lambda}_\pi(x) = \prod_{i=1}^{r} \left(x - \phi(\alpha_i\delta_\beta)^{N(\pi)}\right)$$

De manera anàloga a com s'ha fet per a $\lambda_\pi(x)$ es pot argumentar que $\tilde{\lambda}_\pi(x) \in \mathbb{Z}[i][x]$. Per una banda, fent servir (5.26) trobem que $\lambda_\pi(x)$ i $\tilde{\lambda}_\pi(x)$ tenen les mateixes arrels a $\mathcal{O}/\mathfrak{B}$ i, per tant, $\lambda_\pi \equiv \tilde{\lambda}_\pi \pmod{\pi\mathbb{Z}[i][x]}$. Per altra banda, ja que $\tilde{\lambda}_\pi(x)$ s'obté a partir de $\lambda(x)$ elevant les seves arrels a la $N(\pi)$, tenim $\tilde{\lambda}_\pi \equiv \lambda \pmod{\pi\mathbb{Z}[i][x]}$. Combinant ambdues congruències, trobem que $\lambda_\pi \equiv \lambda \pmod{\pi\mathbb{Z}[i][x]}$. Per tant,

$$\Lambda_\beta(x) \equiv \lambda(x)\lambda_\pi(x)h(x) \equiv \lambda(x)^2 h(x) \pmod{\pi\mathbb{Z}[i][x]}$$

la qual cosa és equivalent a dir que $\Lambda_\beta(x)$ no és separable mòdul π. Això contradiu la nostra tria de π i, doncs, queda demostrat (5.24).

Considerem una arrel $\phi(\alpha_i\delta_\beta)$ de $\lambda(x)$. Sigui η el producte de tots els primers senars que divideixen $\Delta(\Lambda_\beta)$ però que no divideixen β. Si $\phi(\gamma\delta_\beta)$ és una arrel qualsevol de $\Lambda_\beta(x)$, el teorema xinès del residu implica que existeix $\omega \in \mathbb{Z}[i]$ tal que

$$\omega \equiv \gamma\alpha_i^{-1} \pmod{\beta}, \qquad \omega \equiv 1 \pmod{2(1+i)}, \qquad \omega \equiv 1 \pmod{\eta}$$

Consegüentment, ω és senar i podem factoritzar $\omega = \pi_1 \dots \pi_k$, per a π_i primers senars normalitzats coprimers a $\beta\Delta(\Lambda_\beta)$, $i \in \{1, \dots, k\}$. Iterant (5.24) trobem $\lambda(x) = \lambda_{\pi_1}(x) = \lambda_{\pi_1\pi_2}(x) = \cdots = \lambda_{\pi_1\dots\pi_k}(x)$. D'aquí,

$$\phi(\gamma\delta_\beta) = \phi(\gamma\alpha_i^{-1}\alpha_i\delta_\beta) = \phi(\omega\alpha_i\delta_\beta) = \phi(\pi_1 \dots \pi_k\alpha_i\delta_\beta)$$

és una arrel de $\lambda_{\pi_1\dots\pi_k}(x) = \lambda(x)$. Així doncs, $\Lambda_\beta(x)$ i λ tenen les mateixes arrels. Com que tots dos polinomis són mònics i separables, necessàriament han de ser el mateix. Concloem, doncs, que $\Lambda_\beta(x)$ és irreductible sobre $\mathbb{Q}(i)$. □

Havent provat que el polinomi lemnatòmic β-èsim és irreductible (fins ara, amb β senar), podem ampliar la noció de polinomi lemnatòmic pel cas β parell. Fixem-nos que la definició 5.33 considera exclusivament el cas β senar. Així doncs, de manera convenient, definim polinomi lemnatòmic β-èsim, per a $\beta \in \mathbb{Z}[i]$ parell, com

$$\Lambda_\beta(x) = \operatorname{Irr}\left(\phi\left(\frac{2\varpi}{\beta}\right), \mathbb{Q}(i)\right)$$

Observació 5.41. Tal com veurem a les construccions de l'hexàgon regular i del decàgon regular a les seccions A.4 i A.6 de l'Annex A, si $n \in \mathbb{Z}_+$ és senar, el polinomi lemnatòmic $2n$-èsim és el mateix que el polinomi lemnatòmic n-èsim.

6 Conclusions

La lemniscata és una corba parametritzada per $(x^2+y^2)^2 = x^2 - y^2$ o, equivalentment, per $r^2 = \cos(2\theta)$ en coordenades polars. La seva longitud d'arc és doncs

$$s(r) = \int_0^r \frac{dx}{\sqrt{1-x^4}}$$

S'ha demostrat que la longitud d'arc de la lemniscata verifica la següent llei d'addició

$$s(u) + s(v) = s(r), \quad r = \frac{u\sqrt{1-v^4} + v\sqrt{1-u^4}}{1+u^2v^2}$$

A partir de la longitud d'arc de la corba en el primer quadrant, es defineix una constant ϖ com $\varpi/2 = \int_0^1 dx/\sqrt{1-x^4}$ per analogia amb $\pi/2 = \int_0^1 dx/\sqrt{1-x^2}$ en el cas de la circumferència. Així doncs, la constant ϖ assumeix el mateix rol que la constant π en la configuració circular. De manera convenient, es considera la funció inversa ϕ

$$s(r) = \int_0^r \frac{dx}{\sqrt{1-x^4}} \iff r = \phi(s)$$

Aquesta funció no només es pot estendre a tot $\mathbb{R}$, sinó que es pot veure en el seu sentit més ampli com una funció el·líptica, és a dir, una funció meromorfa en el pla complex i doblement periòdica respecte de la xarxa $\mathcal{L} = \mathbb{Z}(1+i)\varpi + \mathbb{Z}(1-i)\varpi$. La consideració d'aquesta funció inversa ϕ esdevé altament convenient per a divisió de la lemniscata en segments de mateixa longitud d'arc. Geomètricament, els valors $\phi(m\frac{2\varpi}{n})$, $m \in \{0, ..., n-1\}$ representen les distàncies respecte de l'origen dels punts de n-divisió de la corba que, com a tals, formen el polígon regular n-èsim sobre la lemniscata. Un resultat elemental però important vist en aquest treball és que tot punt qualsevol de la lemniscata és construïble amb regle i compàs si, i només si, la seva distància a l'origen també ho és. I precisament es troba que els punts de n-divisió de la lemniscata són les arrels d'un polinomis de $\mathbb{Z}[x]$ que reben el nom de polinomis de divisió, $D_n(x)$.

Com que l'objectiu principal d'aquest treball era determinar quins polígons regulars són construïbles amb regle i compàs sobre la lemniscata, s'ha estudiat la teoria de Galois sobre aquests polinomis. Concretament, s'ha computat el grup de Galois

$$\mathrm{Gal}\left(\mathbb{Q}\left(i, \phi\left(\frac{2\varpi}{n}\right)\right)/\mathbb{Q}(i)\right) \tag{6.1}$$

amb $n \in \mathbb{Z}_+$ senar. L'ordre del grup (6.1) determina si és possible dividir la lemniscata amb regle i compàs o no. El nostre resultat principal és l'isomorfisme

$$\mathrm{Gal}\left(\mathbb{Q}\left(i, \phi\left(\frac{2\varpi}{n}\right)\right)/\mathbb{Q}(i)\right) \cong (\mathbb{Z}[i]/n\mathbb{Z}[i])^* \tag{6.2}$$

Per a demostrar aquest fet, s'han emprat dues estratègies diferents. Per una banda, la primera s'ha fonamentat en la construcció d'extensions lemnatòmiques (per analogia amb les extensions ciclotòmiques de la circumferència) segons

$$K = \mathbb{Q}(i) \subset \mathbb{Q}\left(i, \phi\left(\frac{2\varpi}{n}\right)\right) = L$$

Aquest enfocament s'ha batejat en aquest treball com a *natural*, atès que sorgeix d'adjuntar les divisions enteres de la longitud d'arc de la lemniscata. El fet que aquestes

extensions es construeixin a partir de $\mathbb{Q}(i)$ s'explica a través del fet que els punts de la funció ϕ es poden caracteritzar a través d'una corba el·líptica $E : \{y^2 = x^3 + x\}$ que admet multiplicació complexa $(x, y) \mapsto (-x, iy)$. Per altra banda, també s'ha estudiat les extensions de Galois construïdes a partir de

$$K = \mathbb{Q}(i) \subset \mathbb{Q}\left(i, \phi\left(\frac{2\varpi}{\beta}\right)\right) = \tilde{L}$$

on $\beta \in \mathbb{Z}[i]$ és coprimer a $1+i$ (diem que β és senar). Aquest segon enfocament *alternatiu* ve a ser una generalització del cas anterior. En particular, per a caracteritzar aquest grup cal recórrer a conceptes del camp de les funcions el·líptiques i corbes el·líptiques i d'altres més sofisticats com la teoria de cossos de classe. En aquest segon cas, però, trobem l'isomorfisme anàleg a (6.2)

$$\mathrm{Gal}\left(\mathbb{Q}\left(i, \phi\left(\frac{2\varpi}{\beta}\right)\right)/\mathbb{Q}(i)\right) \cong (\mathbb{Z}[i]/\beta\mathbb{Z}[i])^*$$

la qual cosa posa de manifest la compatibilitat entre ambdós plantejaments. Havent vist això, i imposant que l'ordre del grup de Galois de l'extensió lemnatòmica n-èsima tingui ordre potència de 2, s'ha demostrat que els punts de n-divisió de la lemniscata es poden construir amb regle i compàs si, i només si, $n = 2^s$, amb $s \in \mathbb{N}$, o bé $n = 2^s p_1 \dots p_r$, amb $s \in \mathbb{N}, r \in \mathbb{Z}_+$ i $p_i, 1 \leq i \leq r$, primers de Fermat diferents.

Si recordem la condició de constructibilitat dels polígons regulars n-èsims sobre la circumferència, veiem que tenim la mateixa restricció per a n. Aquesta coincidència s'explica a través del fet que els grups de Galois de les extensions algebraiques involucrades, les ciclotòmiques i les lemnatòmiques, són isomorfs a grups multiplicatius de quocients sobre els anells $\mathbb{Z}$ i $\mathbb{Z}[i]$ respectivament.

Finalment, i per a completar l'analogia amb la teoria de cossos ciclotòmics, s'han definit els polinomis lemnatòmics β-èsims $\Lambda_\beta \in \mathbb{Z}[i][x]$, amb $\beta \in \mathbb{Z}[i]$, que garanteixen la factorització de $D_\beta(x) \in \mathbb{Z}[x]$. Precisament, s'ha determinat que el grau dels polinomis lemnatòmics β-èsims és $|\,(\mathbb{Z}[i]/\beta\mathbb{Z}[i])^*\,|$ quan β és senar i que són irreductibles sobre $\mathbb{Q}(i)$.

Com a colofó, aquest treball presenta la construcció pas a pas de les primeres construccions possibles amb regle i compàs de polígons regulars sobre la lemniscata (per a $n \leq 12$) i s'hi exposen els detalls algebraics involucrats.

A Construcció amb regle i compàs de polígons regulars a la lemniscata

Les principals construccions amb regle i compàs de polígons sobre la lemniscata presentades en aquesta secció són derivades de [22]. Altres nocions sobre construccions amb regle i compàs que han permès detallar tots els traçats han estat consultades a [23].

A.1 Triangle equilàter

Per a calcular $D_3(x)$ partim de (3.19) amb $u = 2x$ i $v = x$

$$\phi(2x + x) + \phi(2x - x) = \frac{2\phi(2x)\phi'(x)}{1 + \phi(2x)^2\phi(x)^2}$$

Desenvolupant termes arribem a

$$\phi(3x) = \phi(x)\frac{\phi(x)^8 + 6\phi(x)^4 - 3}{1 + 6\phi(x)^4 - 3\phi(x)^8} \tag{A.1}$$

Així doncs, és clar que $D_3(x) = -x^9 - 6x^5 + 3x$. En virtut de la proposició 5.37, sabem que $D_3(x) = \Lambda_3(x)\Lambda_1(x)$. Per tant, com que $\Lambda_1(x) = x$, el 3-polinomi lemnatòmic és

$$\boxed{\Lambda_3(x) = -x^8 - 6x^4 + 3}$$

Fent el canvi de variable $t = x^4$, trobem que $t = -3 \pm 2\sqrt{3}$. Recordem que les arrels dels polinomis lemnatòmics són els radis $\phi(2\varpi k/n), k \in \{1, ..., n-1\}$, de manera que necessàriament $t > 0$. Aleshores restringim les solucions trobades a $t = -3 + 2\sqrt{3}$. Desfent el canvi de variables i recordant l'equació polar de la lemniscata (que ens serveix per a trobar l'azimut dels radis trobats), concloem que les arrels de $\Lambda_3(x)$ són

$$x = \sqrt[4]{2\sqrt{3} - 3} \approx 0.8253787244...$$

$$\cos(2\theta) = \sqrt{-3 + 2\sqrt{3}} \Rightarrow \sin(2\theta) = 1 - \sqrt{3}$$

Es pot construir el triangle equilàter a la lemniscata de la següent manera:

(1) Traçar un cercle de radi 1 centrat a l'origen O.

(2) Traçar una línia horitzontal a distància $\sqrt{3} - 1$ per sota de l'eix d'abscisses. Per a fer-ho, es poden seguir els següents passos (es corresponen a la part superior esquerra de la Figura 5):

- Traçar dues rectes verticals a distància 1 de l'origen.
- Construir un hexàgon regular entre les dues rectes verticals de manera que l'aresta superior de l'hexàgon estigui continguda a l'eix d'abscisses. L'hexàgon dibuixat té alçada $\sqrt{3}$ (entenent per alçada el doble de l'apotema).
- Traçar un cercle unitari centrat a la intersecció de l'aresta inferior de l'hexàgon amb l'eix d'ordenades.
- Traçar una recta horitzontal paral·lela a l'eix d'abscisses a partir del punt de tall superior d'aquest darrer cercle unitari amb l'eix d'ordenades.

(3) Intersectar aquesta recta amb el cercle unitari original per a tenir un punt A (part inferior esquerra de la Figura 5).

(4) Dibuixar la bisectriu de l'angle $\angle AOB$, on B és el punt d'intersecció de la lemniscata amb el cercle unitari original (amb $x > 0$). Per a fer-ho, es poden seguir els següents passos (es corresponen a la part superior dreta de la Figura 5):

- Dibuixar dos cercles unitaris centrats als punts A i B respectivament.
- Traçar una recta que vagi de l'origen al punt d'intersecció d'aquests dos cercles unitaris auxiliars per a bisectar l'angle $\angle AOB$.

(5) La línia bisectriu intersecta la lemniscata en tres punts diferents, que són els vèrtexos del triangle regular que buscàvem (part inferior dreta de la Figura 5).

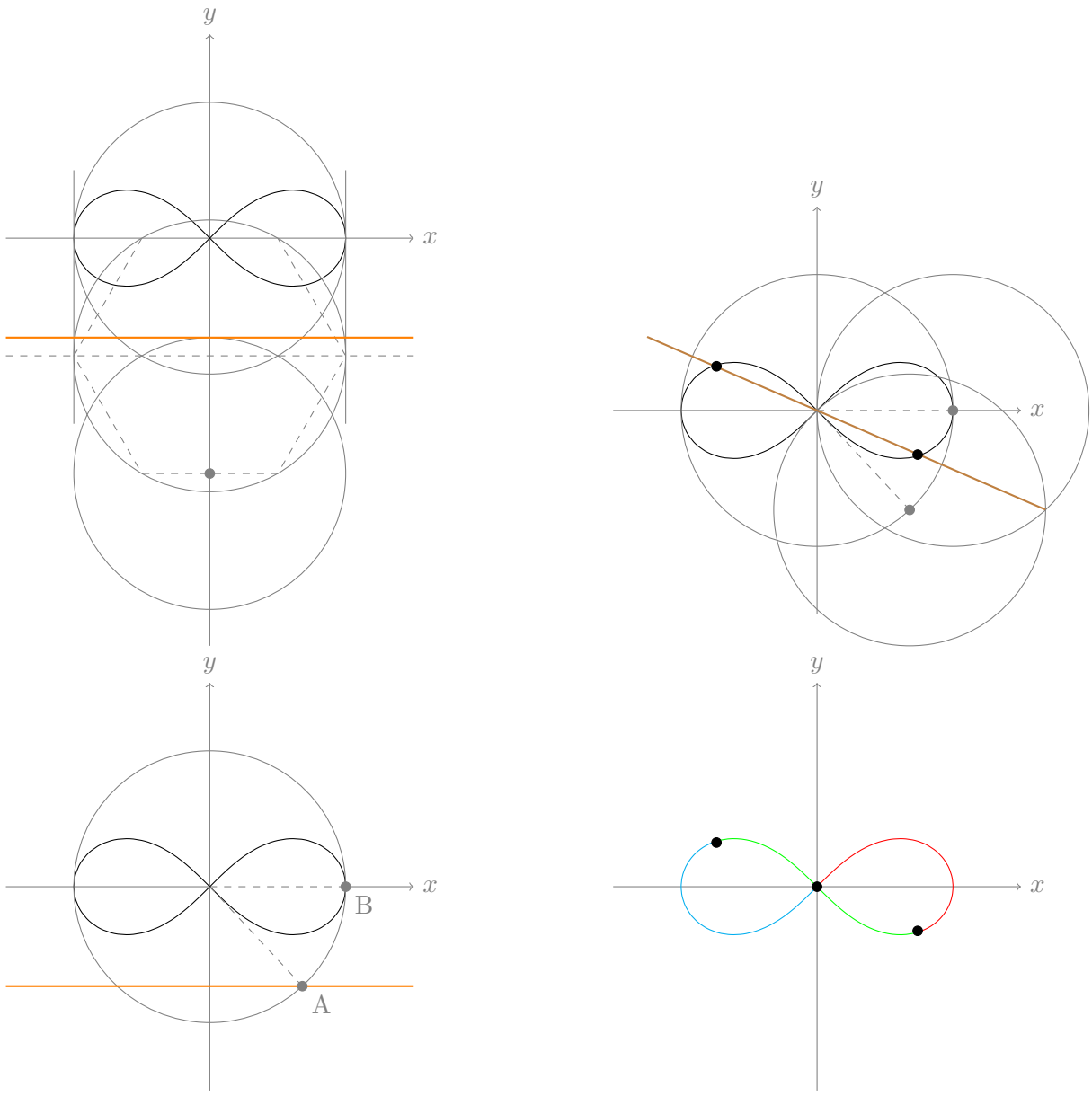

Figura 5: Construcció amb regle i compàs del triangle equilàter a la lemniscata.

A.2 Quadrat

Dividim ara la lemniscata en quatre trossos de longitud $\frac{2\varpi}{4} = \frac{\varpi}{2}$. Per a fer-ho, invoquem la relació (3.20) i trobem

$$0 = \phi(\varpi) = \phi\left(\frac{\varpi}{2} + \frac{\varpi}{2}\right) = \frac{2\phi\left(\frac{\varpi}{2}\right)\sqrt{1-\phi\left(\frac{\varpi}{2}\right)^4}}{1+\phi\left(\frac{\varpi}{2}\right)^4}$$

Això indica que $\phi(\frac{\varpi}{2})$ anul·la $x\sqrt{1-x^4}$. En particular, com que $\phi(\frac{\varpi}{2}) = 1$, notem que podem concretar que $\phi(\frac{\varpi}{2})$ anul·la $x-1$. Ja que el polinomi $x-1$ és irreductible, podem afirmar que

$$\boxed{\Lambda_4(x) = x - 1}$$

La Figura 6 presenta la construcció del quadrat a la lemniscata, una construcció que resulta immediata atesa la simetria que presenta la corba.

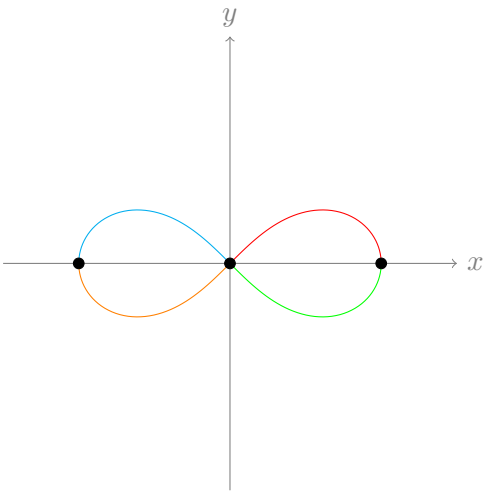

Figura 6: Construcció amb regle i compàs del quadrat a la lemniscata.

A.3 Pentàgon regular

Per a calcular $D_5(x)$ partim de (3.19) amb $u = 3x$ i $v = 2x$

$$\phi(3x+2x) + \phi(3x-2x) = \frac{2\phi(3x)\phi'(2x)}{1+\phi(3x)^2\phi(2x)^2} \tag{A.2}$$

Desenvolupant termes arribem a

$$\phi(5x) = \phi(x)\frac{\phi(x)^{24} + 50\phi(x)^{20} - 125\phi(x)^{16} + 300\phi(x)^{12} - 105\phi(x)^8 - 62\phi(x)^4 + 5}{1 + 50\phi(x)^4 - 125\phi(x)^8 + 300\phi(x)^{12} - 105\phi(x)^{16} - 62\phi(x)^{20} + 5\phi(x)^{24}}$$

Per tant, $D_5(x) = x^{25} + 50x^{21} - 125x^{17} + 300x^{13} - 105x^9 - 62x^5 + 5x$. Precisament, aquest polinomi factoritza com

$$D_5(x) = x(x^8 - 2x^4 + 5)(x^{16} + 52x^{12} - 26x^8 - 12x^4 + 1)$$

Com abans, $D_5(x) = \Lambda_5(x)\Lambda_{2+i}(x)\Lambda_{2-i}(x)\Lambda_1(x)$. Així doncs, ens disposem a calcular $\Lambda_{2+i}(x)$ i $\Lambda_{2-i}(x)$. En virtut de (4.4) podem trobar

$$\phi((2+i)x) = \phi(x)\frac{(2+i) - i\phi(x)^4}{1-(1-2i)\phi(x)^4}\,, \qquad \phi((2-i)x) = \phi(x)\frac{(2-i) + i\phi(x)^4}{1-(1+2i)\phi(x)^4}$$

Aleshores, com que tant $(2+i)$ com $(2-i)$ són senars i primers, és clar que $D_{2\pm i}(x) = x\left[(2\pm i) \mp ix^4\right]$ i $D_{2\pm i}(x) = \Lambda_{2\pm i}(x)\Lambda_1(x)$. Consegüentment, $\Lambda_{2\pm i}(x) = (2\pm i) \mp ix^4$. Fixem-nos que

$$\Lambda_{2+i}(x)\Lambda_{2-i}(x) = \left[(2+i) - ix^4\right]\left[(2-i) + ix^4\right] = x^8 - 2x^4 + 5$$

Podem afirmar, doncs, que el 5-polinomi lemnatòmic és

$$\boxed{\Lambda_5(x) = x^{16} + 52x^{12} - 26x^8 - 12x^4 + 1}$$

Apliquem el canvi de variable $t = x^4$ i obtenim $\Lambda(t) = t^4 + 52t^3 - 26t^2 - 12t + 1$. Aquest polinomi en t té arrels

$$\left.\begin{array}{l} t_1 = -13 + 6\sqrt{5} + 2\sqrt{85 - 38\sqrt{5}} > 0 \\ t_2 = -13 + 6\sqrt{5} - 2\sqrt{85 - 38\sqrt{5}} > 0 \\ t_3 = -13 - 6\sqrt{5} + 2\sqrt{85 + 38\sqrt{5}} < 0 \\ t_4 = -13 - 6\sqrt{5} - 2\sqrt{85 + 38\sqrt{5}} < 0 \end{array}\right\} \Rightarrow \left.\begin{array}{l} x_1 = \sqrt[4]{-13 + 6\sqrt{5} + 2\sqrt{85 - 38\sqrt{5}}} \\ x_2 = \sqrt[4]{-13 + 6\sqrt{5} - 2\sqrt{85 - 38\sqrt{5}}} \end{array}\right\}$$

En concret, els radis són $x_1 \approx 0.933517817393730...$ i $x_2 \approx 0.520470271379642...$ Si recuperem, de nou, l'expressió polar de la lemniscata, $r^2 = \cos(2\theta)$, trobem que els azimuts $\sin(\theta_1), \sin(\theta_2)$ dels radis trobats són arrels del polinomi $y^2 - 2(2-\sqrt{5})y + 2(2-\sqrt{5})$. Per una raó de conveniència, reescalem aquest polinomi per l'invers de $2(2-\sqrt{5})$ obtenim l'equació quadràtica

$$-(1/2+\varphi)y^2 - y + 1 = 0$$

on $\varphi = (1+\sqrt{5})/2$ és la raó àuria. Clarament, aquesta equació té les mateixes arrels que l'anterior. A continuació, es detalla una possible construcció amb regle i compàs del pentàgon regular a la lemniscata:

(1) Traçar un cercle de radi 1 centrat a l'origen.

(2) Dibuixar els punts $A = (-\frac{1}{2} - \varphi)$ i $B = (1, -1)$. Com que el punt $C = (1, 0)$ divideix de forma àuria el segment AO, es poden seguir els següents passos:

   - Marcar el punts $C = (0, 1)$ donat pel cercle unitari.
   - Traçar el segment que uneix el punt mig del segment CO, que denotem per C', amb D.
   - Traçar el cercle centrat a C que té per radi la longitud del segment $C'D$. La intersecció d'aquest cercle amb el semieix negatiu d'abscisses determina A.

(3) Dibuixar el cercle que té per diàmetre el segment que uneix els punts A i B. Notem que aquest cercle passa també per (1,0).

(4) Intersectar el cercle que uneix A i B amb l'eix d'ordenades. Els punts resultants els anomenem E i F.

(5) Traçar les línies paral·leles a AE i AF que passen per C per a obtenir els punts G i H. Aquests punts verifiquen $OG = \sin(2\theta_1)$ i $OH = \sin(2\theta_2)$.

(6) N'hi ha prou amb bisecar els angles $2\sin(2\theta_i)$, $i \in \{1, 2\}$, per a trobar els dos primers vèrtexos del pentàgon. Els altres dos vèrtexos són els punts simètrics respecte de l'origen.

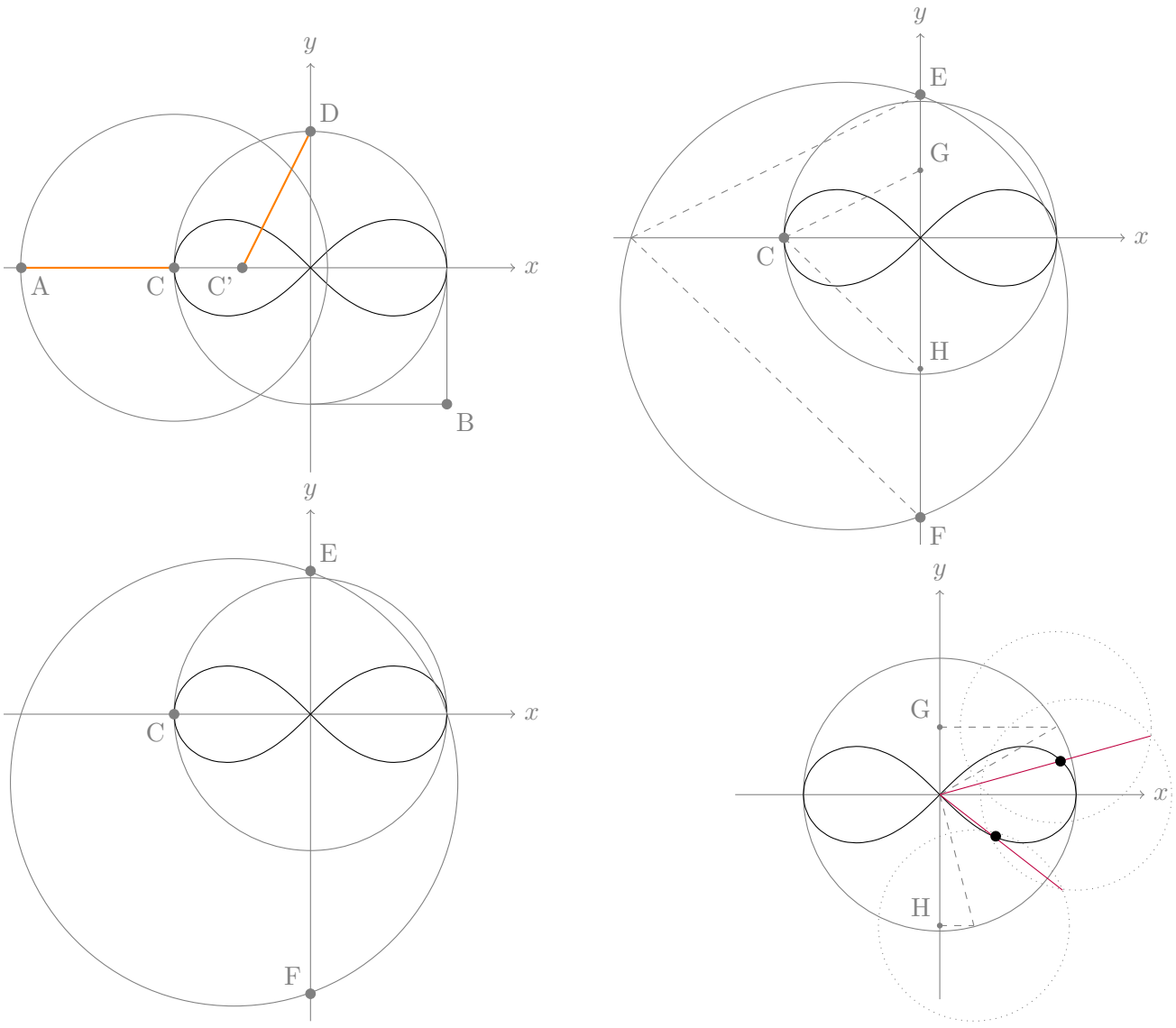

Figura 7: Construcció amb regle i compàs del pentàgon regular a la lemniscata.

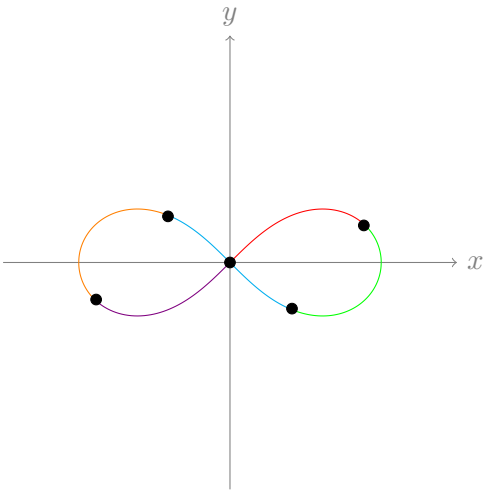

Figura 8: Pentàgon regular a la lemniscata

A.4 Hexàgon regular

Dividim ara la lemniscata en sis segments de longitud d'arc $\frac{2\varpi}{6} = \frac{\varpi}{3}$. En primer lloc, remarquem que la constructibilitat de $\phi(\frac{\varpi}{3})$ està assegurada gràcies a la fórmula de duplicació (3.20). Recordem la construcció del triangle equilàter A.1. Atesa la simetria que presenta la lemniscata, fixem-nos que la divisió de la corba en tres segments de longitud d'arc $\frac{2\varpi}{3}$ presenta la següent dualitat:

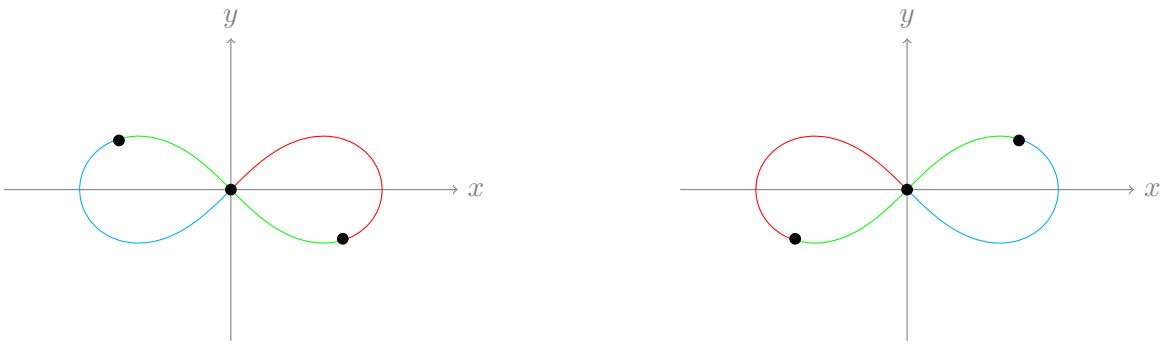

Figura 9: Simetria del triangle equilàter sobre la lemniscata.

La simetria de la Figura 9 evidencia que els punts de 6-divisió de la lemniscata surten de superposar les dues possibilitats de 3-divisió començant a l'origen: una recorrent la corba en sentit horari i l'altra, en sentit antihorari. És a dir, $\phi(\frac{\varpi}{3}) = \phi(\frac{2\varpi}{3})$. Per la definició de $\Lambda_6(x) = \text{Irr}\left(\phi\left(\frac{\varpi}{3}\right), \mathbb{Q}(i)\right)$ veiem clarament que $\Lambda_6(x) = \Lambda_3(x)$. I, per tant,

$$\boxed{\Lambda_6(x) = -x^8 - 6x^4 + 3}$$

La construcció amb regle i compàs de l'hexàgon regular a la lemniscata és immediata a partir de la construcció del triangle equilàter vista a A.1. En particular, n'hi ha prou amb trobar la intersecció de la lemniscata amb un cercle centrat a l'origen que passi pels vèrtexos del triangle equilàter. D'aquesta manera, es poden trobar els vèrtexos que falten per a tenir l'hexàgon regular. La Figura 10 il·lustra aquesta construcció.

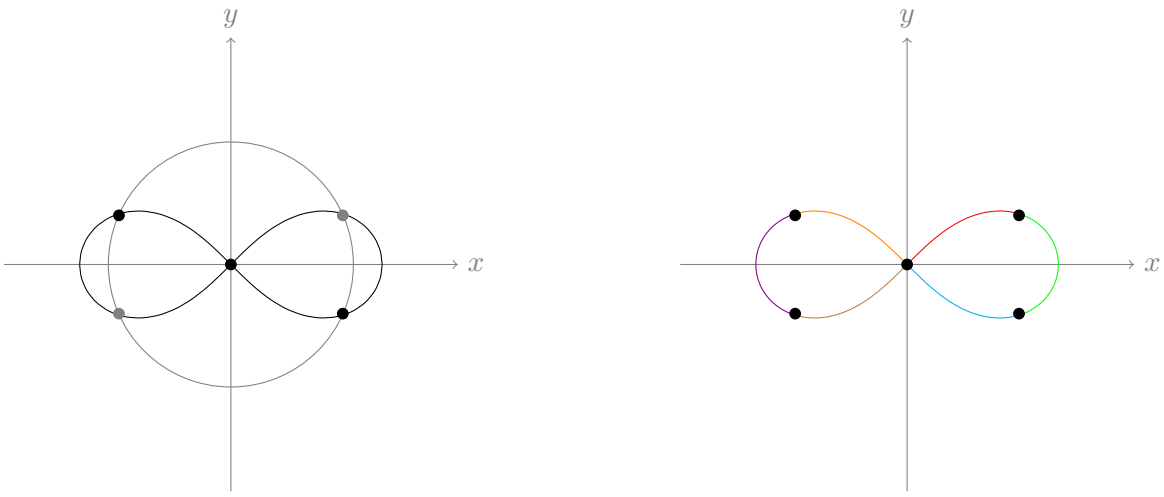

Figura 10: Construcció amb regle i compàs de l'hexàgon regular a la lemniscata.

A.5 Octàgon regular

Dividim ara la lemniscata en vuit trossos de longitud $\frac{2\varpi}{8} = \frac{\varpi}{4}$. Com que $\phi(\frac{\varpi}{2}) = 1$, la llei d'addició vista al Corol·lari 3.3 ens permet escriure

$$1 = \phi\left(\frac{\varpi}{2}\right) = \phi\left(\frac{\varpi}{4} + \frac{\varpi}{4}\right) = \frac{2\phi\left(\frac{\varpi}{4}\right)\sqrt{1-\phi\left(\frac{\varpi}{4}\right)^4}}{1+\phi\left(\frac{\varpi}{4}\right)^4} \tag{A.3}$$

D'aquesta manera, és immediat de comprovar que $\phi\left(\frac{\varpi}{4}\right)$ és arrel del polinomi $x^8 + 4x^6 + 2x^4 - 4x^2 + 1$. Aquest polinomi factoritza com $(x^4 + 2x^2 - 1)^2$, llavors

$$\boxed{\Lambda_8(x) = x^4 + 2x^2 - 1}$$

Si apliquem el canvi de variable $t = x^2$, es pot reescriure com $\Lambda_8(t) = t^2 + 2t - 1$. Aquest polinomi té les següents arrels:

$$\left.\begin{array}{l} t_1 = \sqrt{2} - 1 > 0 \\ t_2 = -\sqrt{2} - 1 < 0 \end{array}\right\} \Rightarrow x = \sqrt{\sqrt{2} - 1} \approx 0.6435942529...$$

Aquesta és l'única arrel que ens interessa perquè la distància polar $\phi\left(\frac{\varpi}{4}\right) \in \mathbb{R}_+$. Si recuperem l'equació polar de la lemniscata, trobem que els azimuts d'aquestes noves arrels verifiquen $\cos(2\theta) = \sqrt{2} - 1$. Tot seguit es detalla una possible construcció amb regle i compàs de l'octàgon regular a la lemniscata (la Figura 11 n'il·lustra els passos):

(1) Es parteix de la construcció del quadrat vista a A.2.

(2) Traçar dos cercles centrat a l'origen O, un de radi 1 i l'altre de radi $\sqrt{2}$. Sigui A la intersecció del cercle més gran amb el semieix positiu d'abscisses.

(3) Marcar el punt mig del segment OA, denotat per A'.

(4) Traçar un cercle unitari centrat a A'.

(5) Traçar un segment vertical que parteixi del punt $B = (1, 0)$ i arribi a la intersecció amb el cercle unitari centrat a A', que denotem per C.

(6) Dibuixar un cercle centrat a l'origen tal que el seu radi coincideixi amb la longitud del segment BC. La intersecció d'aquest cercle amb la lemniscata proporciona dos dels vèrtex que falten per a construir l'octàgon. Els altres dos vèrtexos són els punts simètrics respecte de l'origen.

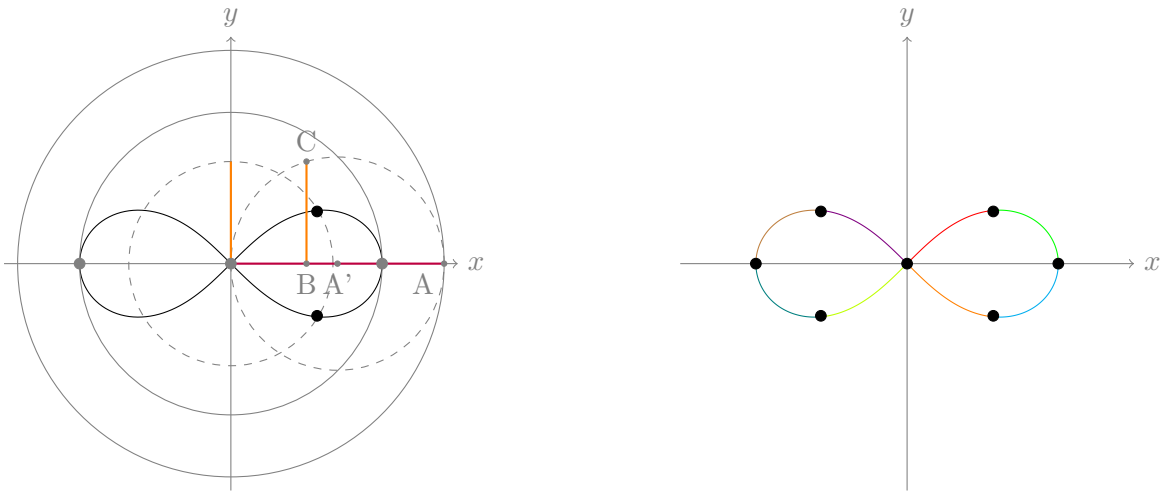

Figura 11: Construcció amb regle i compàs de l'octàgon a la lemniscata.

A.6 Decàgon regular

Dividim ara la lemniscata en deu segments de longitud d'arc $\frac{2\varpi}{10} = \frac{\varpi}{5}$. En primer lloc, remarquem que la constructibilitat de $\phi(\frac{\varpi}{5})$ està assegurada gràcies a la fórmula de duplicació (3.20). Recordem la construcció del pentàgon regular A.3. Atesa la simetria que presenta la lemniscata, fixem-nos que la divisió de la corba en cinc segments de longitud d'arc $\frac{2\varpi}{3}$ presenta la següent dualitat:

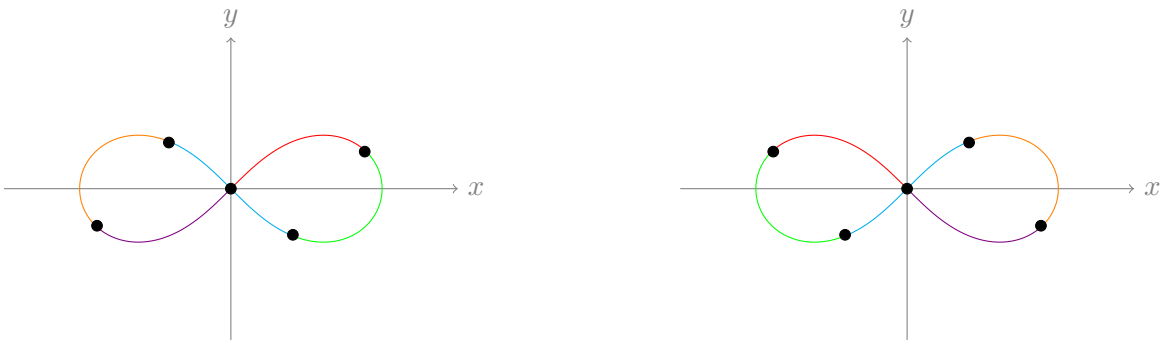

Figura 12: Simetria del pentàgon regular sobre la lemniscata.

La simetria de la Figura 12 evidencia que els punts de 10-divisió de la lemniscata surten de superposar les dues possibilitats de 5-divisió començant a l'origen: una recorrent la corba en sentit horari i l'altra, en sentit antihorari. És a dir, $\phi(\frac{\varpi}{5}) = \phi(\frac{2\varpi}{5})$. Per la definició de $\Lambda_{10}(x) = \operatorname{Irr}\left(\phi\left(\frac{\varpi}{5}\right), \mathbb{Q}(i)\right)$ veiem clarament que $\Lambda_{10}(x) = \Lambda_5(x)$. I, per tant,

$$\boxed{\Lambda_{10}(x) = x^{16} + 52x^{12} - 26x^8 - 12x^4 + 1}$$

La construcció amb regle i compàs del decàgon regular a la lemniscata és immediata a partir de la construcció del pentàgon regular vista a l'apartat A.3. En particular, n'hi ha prou amb trobar la intersecció de la lemniscata amb els cercles centrats a l'origen que passin respectivament pels vèrtexos del pentàgon regular.

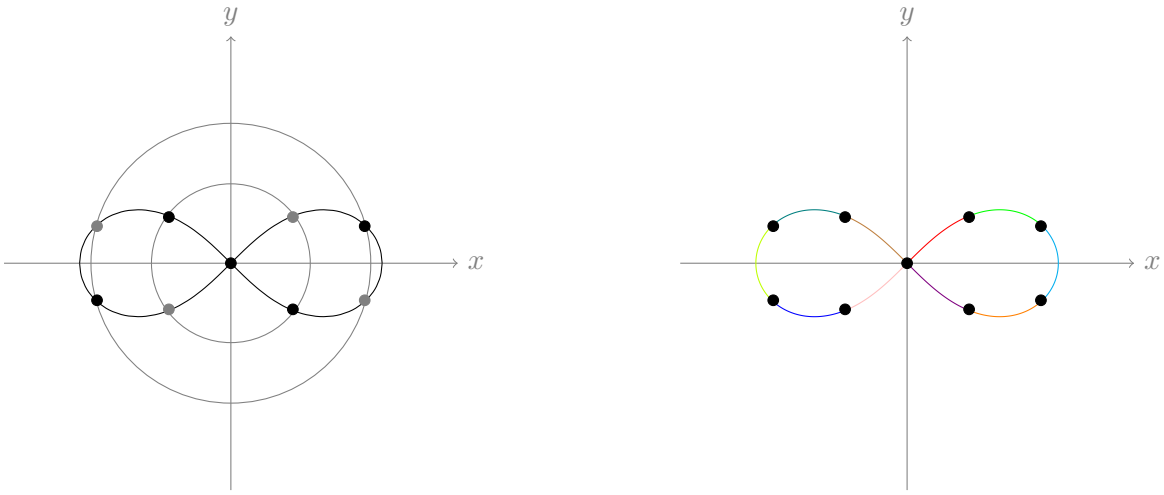

Figura 13: Construcció amb regle i compàs del decàgon regular a la lemniscata.

A.7 Dodecàgon regular

Dividim ara la lemniscata en dotze segments de longitud d'arc $\frac{2\varpi}{12} = \frac{\varpi}{6}$. Com que $\phi(\frac{\varpi}{3}) = \sqrt[4]{2\sqrt{3}-3}$, la llei d'addició vista al Corol·lari 3.3 ens permet escriure

$$\sqrt[4]{2\sqrt{3}-3} = \phi\left(\frac{\varpi}{3}\right) = \phi\left(\frac{\varpi}{6}+\frac{\varpi}{6}\right) = \frac{2\phi\left(\frac{\varpi}{6}\right)\sqrt{1-\phi\left(\frac{\varpi}{6}\right)^4}}{1+\phi\left(\frac{\varpi}{6}\right)^4} \tag{A.4}$$

D'aquesta manera, es pot comprovar que $\phi\left(\frac{\varpi}{6}\right)$ és arrel del polinomi

$$-3x^{32}+72x^{28}+364x^{24}-1288x^{20}+942x^{16}-1288x^{12}+364x^8+72x^4-3$$

Precisament, aquest polinomi factoritza com

$$-(x^4-2x^3-2x+1)(x^4+2x^3+2x+1)(x^8+6x^4-3)(x^8+4x^6-6x^4+4x^2+1)(3x^8-6x^4-1)$$

Sabem que $\phi(\frac{\varpi}{6})$ ha d'anul·lar algun d'aquest factors. Recordem que $\phi(\frac{\varpi}{6}) \in \mathbb{R}_+$ i que $\phi(\frac{\varpi}{6}) \leq 1$ per estar dins de la lemniscata. Veiem que l'únic factor que té una arrel real positiva més petita que 1 és el primer. Com que aquest polinomi és irreductible, podem concloure que

$$\boxed{\Lambda_{12}(x) = x^4-2x^3-2x+1}$$

Les úniques arrels reals que té aquest polinomi són

$$\left.\begin{array}{l} x_1 = \frac{1}{2}\left(1+\sqrt{3}+\sqrt[4]{12}\right) > 1 \\ x_2 = \frac{1}{2}\left(1+\sqrt{3}-\sqrt[4]{12}\right) < 1 \end{array}\right\} \Rightarrow x = \frac{1}{2}\left(1+\sqrt{3}-\sqrt[4]{12}\right) \approx 0.4354205447...$$

Tot seguit es detalla una possible construcció amb regle i compàs del dodecàgon regular a la lemniscata (la Figura 14 n'il·lustra els passos):

(1) Es parteix de la construcció de l'hexàgon regular vista a A.4.

(2) S'afegeixen els punts de 4-divisió vistos a A.2.

(3) Construir un segment de longitud $\sqrt{12}$. Per a fer-ho es poden seguir els següent passos (no estan representats gràficament a la Figura 14 perquè són molt elementals):

- Traçar tres cercles centrats a l'origen O: el primer, de radi 1, el segon, de radi 2, i el tercer, de radi 3.
- Dibuixar el segment que uneix els punts (2,0) i (0,1). Aquest segment té longitud $\sqrt{3}$.
- Transportar aquest segment a l'eix d'ordenades de manera que es pugui dibuixar un segment d'extrems $(0,\sqrt{3})$ i (3,0). Aquest segment té longitud $\sqrt{12}$.

(4) Construir un segment de longitud $\sqrt[4]{12}$. Per a fer-ho es poden seguir els següent passos (no estan representats gràficament a la Figura 14 perquè són anàlegs a passos vistos anteriorment):

- Traçar el segment d'extrems $O = (0,0)$ i $A = (1+\sqrt{12}, 0)$.

- Dibuixar el punt mig M del segment OA i la semicircumferència del semiplà superior amb diàmetre OA.
- Traçar la vertical pel punt $I = (1, 0)$ i marcar B el punt de tall amb la semicircumferència, que efectivament és $\sqrt[4]{12}$.

(5) Construir el segment PQ on $P = (1 + \sqrt{3}, 0)$ i $Q = (\sqrt[4]{12}, 0)$.

(6) Marcar el punt R del semieix positiu d'abscisses tal que el segment OR tingui la mateixa longitud que el PQ.

(7) Traçar la mediatriu del segment OR per a trobar-ne el punt mig, N.

(8) Dibuixar un cercle de radi la longitud del segment ON. La intersecció d'aquest cercle amb la lemniscata són els vèrtex que ens faltaven per a completar el dodecàgon regular.

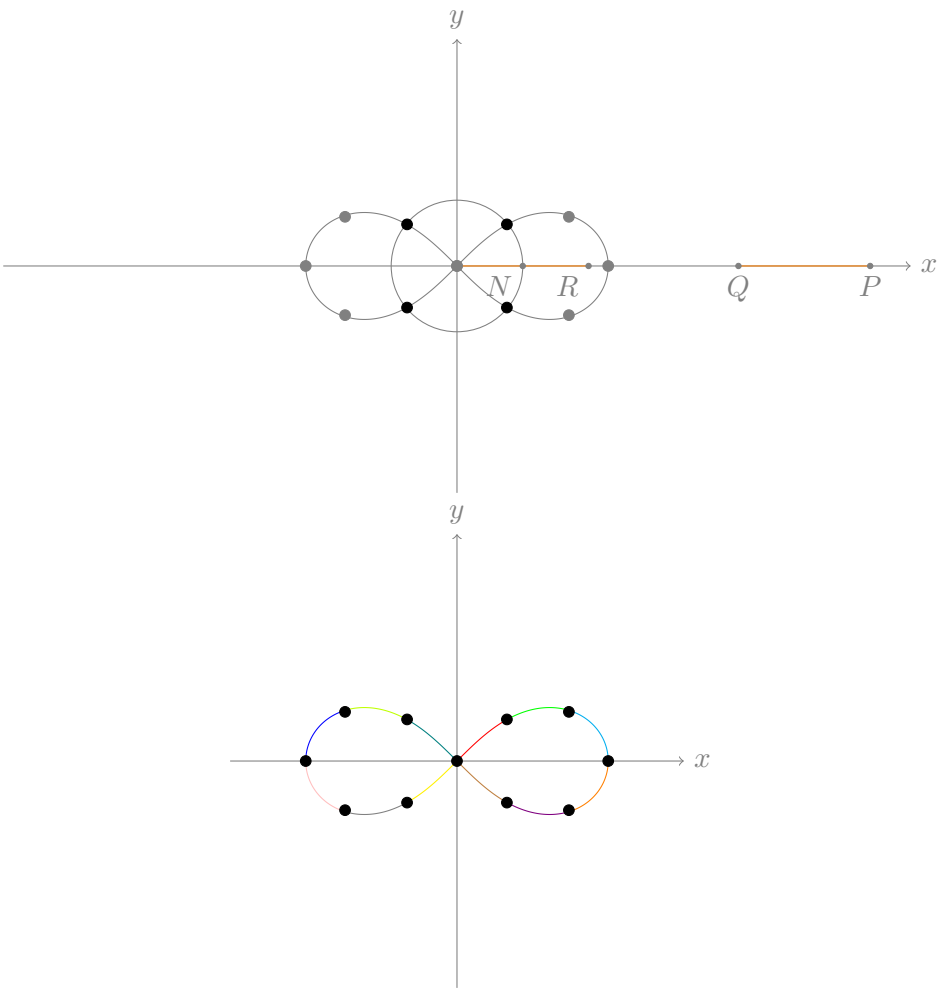

Figura 14: Construcció amb regle i compàs del dodecàgon regular sobre la lemniscata.

Referències

[1] Morrow, G.R.: *Proclus: A commentary on the first book of Euclid's Elements*, Princeton University Press, 1970.

[2] Karataş, M.: *A Multi Foci Closed Curve: Cassini Oval, Its Properties and Applications*, Doğuş Üniversitesi Dergisi, 14 (2): pp.231-248, 2013.

[3] Usunáriz, U., Usunáriz, P.: *Diccionario biográfico de matemáticos*, 2012

[4] Cox, D.A.: *Galois Theory*, 2a edició, John Wiley & Sons: pp.463-514, 2012.

[5] Cox, D.: *The arithmetic-geometric mean of Gauss*, L'Enseignement Mathématique 30, 1984.

[6] Ayoub, R.: *The lemniscate and Fagnano's contributions to elliptic integrals*, Arch. Hist. Exact Sci, 29: pp.131-149, 1984.

[7] Gauss, C.F.: *Werke: Elegantiores Integralis* $\int \frac{dx}{\sqrt{1-x^4}}$ *Proprietates*, Königlichen Gesellschaft der Wissenschaften zu Göttingen, 2a edició: pp.404-412, 1876.

[8] Wells, Jr., R. O., Wells, R. O.: *Elliptic Functions. Differential and Complex Geometry: Origins, Abstractions and Embeddings*, Springer: pp.97-112, 2017.

[9] Takagi, T.: *Über die im Bereiche der rationalen complexen Zahlen Abel'schen Zahlkörper*, The Journal of the College of Science, Imperial University of Tokyo, 19: pp.1-42, 1903.

[10] Abramowitz, M., Stegun, I.A.: *Handbook of Mathematical Functions: With Formulas, Graphs, and Mathematical Tables*, Courier Corporation, 1965.

[11] Rosen, M.: *Abel's theorem on the lemniscate*, The American Mathematical Monthly, 88(6): pp.387-395, 1981.

[12] Siegel, C.L.: *Topics in Complex Function Theory, Vol. 1: Elliptic Functions and Uniformization Theory*, John Wiley & Sons: pp.1-9, 1969.

[13] Lemmermeyer, F.: *Reciprocity laws: from Euler to Eisenstein*, Springer Science & Business Media: pp.239-244, 2013.

[14] Cox, D.A., Hyde T.: *The Galois theory of the lemniscate*, Journal of Number Theory 135: pp.43-59, 2014.

[15] Marsden, J.E., Hoffman M.J., Marsden, T.: *Basic complex analysis*, 3a edició, Macmillan, 1999.

[16] Whittaker, E. T., Watson, G. N. A.: *Course in Modern Analysis*, 4a edició, Cambridge University Press, 1990.

[17] Lang, S.: *Elliptic functions*, 2a edició, New York: Springer-Verlag, 1987.

[18] Silverman, J.H.: *Advanced Topics in the Arithmetic of Elliptic Curves*, 2a edició, Springer-Verlag, 1994.

[19] Prasolov, V., Solovyev, Y.: *Elliptic functions and elliptic integrals*, Vol. 170. American Mathematical Soc., 1997.

[20] Silverman, J.H., Tate, J.: *Rational Points on Elliptic Curves*, 2a edició, New York: Springer-Verlag, 1992.

[21] Lang, S.: *Algebraic number theory*, 2a edició, Addison-Wesley Educational Publishers Inc., 1971.

[22] Gómez-Molleda, M.A., Lario, J.C.: *Ruler and Compass Constructions of the Equilateral Triangle and Pentagon in the Lemniscate Curve*, Math Intelligencer, 41: pp.17–21, 2019.

[23] Crespo, T.: *Equacions Algebraiques. Curs 2021-22*, Universitat de Barcelona, Departament de Matemàtiques, 2021.