Construccions amb regla i compàs a la lemniscata

David Galindo Chacón

Juliol 1999

Índex

‘*De même j’enverrai a M. Gergonne un grand mémoire sur les fonctions elliptiques* [..]. *Entre autres choses il traite de la division de l’arc de la lemniscate. Tu verras comme c’est de gentil.*’

Niels Henrick Abel

Capítol 1

Introducció

En aquest capítol s'exposen breument els fets més rellevants a la gènesi de les construccions amb regla i compàs a la lemniscata que són tractades al present treball, així com l'enfocament que hem donat a aquest estudi.

1.1 Nota històrica

L'any 1694 **Jakob Bernoulli** publicà l'article '*Constructio Curvae Accesus & Recessus aequabilis a puncto dato, mediante rectificatione Curvae Elasticae*', el qual féu que la lemniscata comencés a ser coneguda per la comunitat matemàtica de l'època. Per aquest motiu de vegades rep el nom de *lemniscata de Bernoulli*. Però va ser un matemàtic italià, el comte **Fagnano** (1682-1766), el primer que en va descobrir propietats importants. Va trobar que la bisecció i trisecció d'un arc de lemniscata constituïen un problema algebraic.

El 1796, el jove **Gauss** prova que es pot construir amb regla i compàs el polígon regular de 17 costats. Més tard supera aquest resultat demostrant que el N-àgon regular és construïble amb regla i compàs si *i només si* N és de la forma $N = 2^n p_1 \cdots p_k$, on els p_i són primers de Fermat diferents dos a dos. Gauss s'interessa també per la N-divisió a la lemniscata, i en particular prova que l'equació relacionada amb el cas particular de N=5 és resoluble per radicals, encara que aquest resultat mai va ser publicat. Però, en la seva obra *Disquisitiones Arithmeticae* (1801), afirma que els mètodes que ha emprat per a la N-divisió al cercle '*no només es poden aplicar a les funcions circulars, sinó, amb èxit semblant, a moltes altres funcions transcendents,*

per exemple, a les que depenen de la integral $\int \frac{dx}{\sqrt{1-x^4}}$ *...'.*

Aquesta petita remarca aconseguí captar l'atenció d'**Abel**. Així, va investigar l'equació per a la N-divisió de la lemniscata, i va demostrar que era possible la divisió amb regla i compàs per als mateixos valors de N que en el cas del cercle (1826). Abel valorava aquest teorema com un dels seus resultats més importants. Aquests estudis van esdevenir els fonaments de la *teoria de les funcions el·líptiques*.

Més recentment (1981), **Rosen** ha publicat una prova actualitzada d'aquest resultat, fent servir la teoria de Galois i la teoria de corbes el·líptiques amb multiplicació complexa, recursos que a l'època d'Abel tot just s'estaven desenvolupant. A més a més Rosen demostra també el recíproc, és a dir, que si la lemniscata és divisible en N parts iguals amb regla i compàs, aleshores $N = 2^n p_1 \cdots p_k$, on els p_i són primers de Fermat diferents dos a dos.

1.2 Objectius i pre-requisits

El primer objectiu que ens proposem en aquest treball és entendre i explicar la prova del teorema d'**Abel-Rosen**. Per això ens cal recopilar un variat recull de resultats matemàtics, així com mostrar les seves interrelacions. Assumirem que el lector està familiaritzat amb la teoria de Galois, que té nocions de geometria algebraica i de funcions de variable complexa, i que coneix la prova per als N-àgons regulars a la circumferència. Un altre objectiu és realitzar la construcció efectiva d'alguns polígons regulars lemniscàtics. En particular, farem la construcció dels polígons de 3, 5, 6 i 8 costats.

1.3 Fonts bibliogràfiques

Han estat diverses les referències bibliogràfiques que hem utilitzat. A continuació senyalem les que més ajut ens han proporcionat.

[Abel] L. Sylow i S. Lie. *Oeuvres complètes du Niels Henrik Abel.* Christianna, 1881.

[Ber] P. Radelet-de-Grave. *Die Streitschriften von Jacob und Johann Bernoulli.* Birkhäuser Verlag, 1991.

[Cox] D. A. Cox. *Primes of the form $x^2 + ny^2$.* Pure and Applied Mathematics. Wiley & Sons Inc., 1989.

[Fen] M. H. Fenrick. *Introduction to the Galois correspondence.* Birkhäuser Boston, 1992.

[Gauss] C. F. Gauss. *Disquisicions aritmètiques.* Traducció al català a càrrec de Griselda Pascual. SCM. Barcelona, 1996.

[Kli] M. Kline. *El pensamiento matemático de la Antigüedad a nuestros días.* Alianza Editorial. Madrid, 1992.

[Hur] A. Hurwitz. *Über die Entwicklungskoeffizienten der lemniscatischen Funktionen,* Matematische Werke vol. 2, p. 342-373. Birkhäuser Verlag, Basel und Sttutgart, 1962.

[Pra] V. Prasolov, Y. Soloyvev. *Elliptic functions and Elliptic Integrals.* Translations of Math. Monographs **70**. AMS, 1997.

[Ros] M. Rosen. *Abel's theorem on the lemniscate.* Amer. Math. Monthly **88** (1981), p. 387-395.

[Sch] N. Schappacher. *Some milestones of lemniscatomy,* extret de *Algebraic geometry.* Marcel Dekker Inc., New York, 1997.

[Sie] C. L. Siegel. *Complex Function Theory.* John Wiley & Sons, 1988.

[Ste] I. Stewart. *Galois Theory.* Chapman and Hall Mathematics, 1989.

[Wal] M. Waldschmidt. *Nombres transcendants.* Springer-Verlag Berlin · Heidelberg, 1974.

També hem fet ús de la informació que es troba a les pàgines de la *World Wide Web*:

[1] www.museo.unimo.it/labmat/lemn.htm

[2] www.best.com/%7Exah/SpecialPlaneCurves-dir

[3] www.mathsoft.com/asolve/constant/gauss/gauss.html .

Capítol 2

Construccions amb regla i compàs

En aquest capítol estudiem les construccions amb regla i compàs. L'objectiu és fer una recopilació tant de les tècniques emprades com dels resultats teòrics que permeten tractar els problemes de regla i compàs. Aquests problemes són clàssics en l'estudi de la geometria. Hom vol determinar quins punts o objectes, normalment del pla, són construïbles usant només aquests dos instruments, i en el cas que això sigui possible, trobar un procediment per efectuar la construcció. Però, perquè s'admet només l'ús d'aquests dos instruments? La resposta la trobem a l'època en què sorgeix l'interès per aquest problema, a l'Antiga Grècia. Per als grecs, la línia recta i la circumferència eren les figures bàsiques, que es traduïen físicament a la regla i el compàs. Per aquesta raó jutjaven que les construccions amb aquests elements eren les més preferibles des del punt de vista estètic, i d'aquí ve que Euclides als *Elements* només considerés les que es poden realitzar amb regla i compàs. Així, es van proposar construir els polígons regulars amb regla i compàs, problema que és equivalent a dividir la longitud de la circumferència en parts iguals. Van aconseguir construir els polígons de costats $n = 3, 4, 5, 15$, corresponents al triangle equilàter, quadrat, pentàgon, i pentadecàgon, a més de tots aquells que s'obtenen en doblar repetidament el nombre de costats anteriors. Però no van saber-ne construir cap altre, ni tampoc determinar si això era possible.

Després de l'època grega, aquests problemes van resorgir al segle XVI, quan es va començar a desenvolupar l'àlgebra a Occident. Aquest nou llenguatge proporcionava noves tècniques per la resolució del problema. Finalment, el tractament d'aquestes qüestions ha acabat a mans de la matemàtica

global –amb especial èmfasi a l'esfera de la Geometria Algebraica, la Teoria de Nombres i la Teoria de funcions de variable complexa.

2.1 Construccions elementals

Les operacions admisibles en les construccions amb regla i compàs són les següents:

(i) Traçar la recta que uneix dos punts (regla).

(ii) Traçar la circumferència amb centre i radi donats (compàs).

(iii) Intersecció de dues rectes (regla).

(iv) Intersecció d'una recta amb una circumferència (regla i compàs).

(v) Intersecció de dues circumferències (compàs).

Es parteix d'un segment donat, que es pren com a unitat de referència. Aleshores, un punt del pla es diu construïble amb regla i compàs si es pot obtenir a partir del segment unitat mitjançant una seqüència (finita) de les construccions elementals esmentades abans. Aleshores la qüestió que es planteja consisteix a saber resoldre el problema següent.

Problema. Determinar tots els punts del pla construïbles amb regla i compàs.

A continuació fem un breu llistat de construccions elementals:

- Rectes paral·leles i perpendiculars a una de donada;
- Bisectriu d'un angle;
- Suma, diferència, producte, i divisió de segments;
- L'arrel quadrada d'un segment.

2.2 Criteris de constructibilitat

En aquesta secció recordem la traducció dels problemes geomètrics de constructibilitat amb regla i compàs al llenguatge algebraic. Posem de manifest el benefici obtingut procedint així atesa la caracterització en termes algebraics dels punts que són construïbles. Tanmateix recordem uns criteris que ens permetran decidir amb certa facilitat sobre la constructibilitat de punts.

Construïm una recta ℓ perpendicular al segment unitat per un dels seus extrems. Identifiquem aquest extrem com l'origen del sistema de referència amb eixos la recta ℓ i la recta que suporta el segment unitat. Aleshores tot punt P del pla queda determinat unívocament per les seves coordenades cartesianes (x, y), essent x i y nombres reals. Alternativament, podem interpretar els punts del pla com a nombres complexos fent $P = x + i\,y$ (veure figura 2.1). Plantejat en aquests termes el problema que ens ocupa es redueix a determinar tots els parells (x, y) corresponents a punts del pla construïbles amb regla i compàs. Equivalentment, determinar tots els nombres complexos $x + i\,y$ construïbles amb regla i compàs.

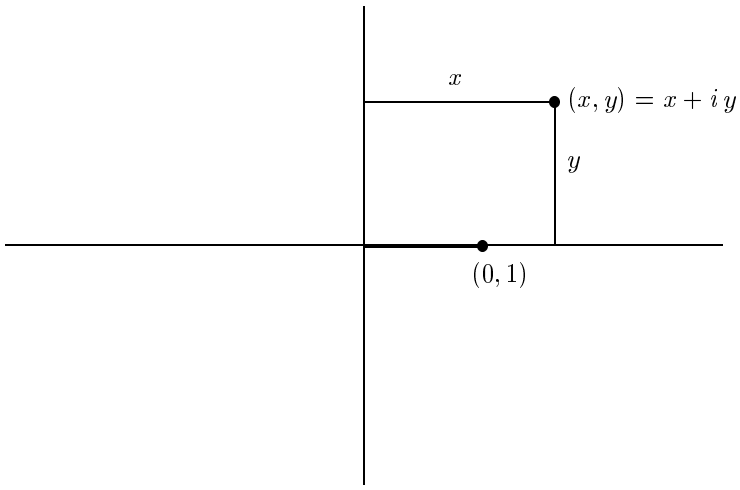

Figura 2.1: Interpretació algebraica de les construccions amb regla i compàs

És clar que un punt (x, y) és construïble si i només si els segments x i y

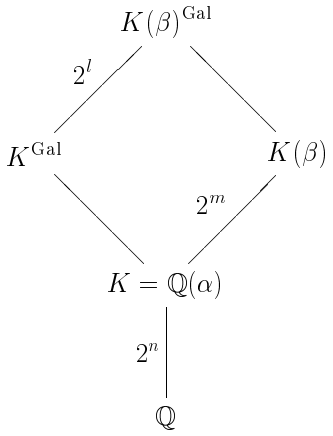

Figura 2.2: Prova del criteri 3

són construïbles, és a dir, si ho són las seves coordenades cartesianes. Els criteris següents ens permetran decidir si un nombre complex α és construïble utilitzant eines purament algebraiques.

Criteri 1. Si α és construïble, aleshores $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2^m$ per algun m enter.

El recíproc no és cert en general. En efecte, sigui α una arrel del polinomi irreductible $x^4 + 6x - 2$. Per tant $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$ i es té que α no és construïble. Per a obtenir una condició suficient cal que l'extensió de cossos $\mathbb{Q}(\alpha)/\mathbb{Q}$ sigui normal. Més concretament,

Criteri 2. Sigui $\alpha \in \overline{\mathbb{Q}}$. Posem $K = \mathbb{Q}(\alpha)$ i K^{Gal} la clausura algebraica de K dins $\overline{\mathbb{Q}}$. Aleshores α és construïble si i només si $[K^{\mathrm{Gal}} : \mathbb{Q}] = 2^m$ per $m \in \mathbb{N}$.

Criteri 3. Sigui α construïble i sigui $K = \mathbb{Q}(\alpha)$. Si $\beta \in \mathbb{C}$ és tal que l'extensió $K(\beta)/K$ és normal i $[K(\beta) : K] = 2^m$ per $m \in \mathbb{N}$, aleshores β és construïble.

El criteri 3 és conseqüència dels anteriors, com es pot observar al gràfic següent. `este no pirula, Xavi`

Per a una prova d'aquests criteris es pot consultar [Fen], capítol 4.1 . Per il·lustrar la seva utilitat fem menció dels tres problemes clàssics sobre les construccions amb regla i compàs: la trisecció de l'angle, la duplicació del cub i la quadratura del cercle.

- En general no es pot trisecar un angle qualsevol amb regla i compàs. Posem-ne un exemple. Com que $\cos(\frac{\pi}{3}) = \frac{1}{2}$, l'angle $\frac{\pi}{3}$ és construïble. Vegem, però, que $\alpha = \frac{\pi}{9}$ no ho és. En efecte, usant relacions trigonomètriques tenim que

$$\frac{1}{2} = \cos(3\alpha) = 4\cos^3(\alpha) - 3\cos(\alpha) \ ,$$

  i per tant $\cos(\alpha)$ és arrel del polinomi irreductible $f(x) = 8x^3 - 6x - 1 \in \mathbb{Q}[x]$. Tenim aleshores que $[\mathbb{Q}(\cos(\alpha)) : \mathbb{Q}] = 3$ i per tant, pel criteri 1 de constructibilitat, l'angle α no és construïble.

- El problema de la duplicació del cub consisteix en construir amb regla i compàs un cub que tingui el doble de volum que un de donat. Suposem així que tenim un cub de volum 1. Si volem construïr un altre de volum 2 serà necessari construir un segment de longitud $\sqrt[3]{2}$, o equivalentment, construir el punt $(\sqrt[3]{2}, 0)$. Però $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$ i aleshores, utilitzant el mateix criteri de constructibilitat, tenim que $\sqrt[3]{2}$ no és construïble. Per tant no és possible realitzar la duplicació del cub només amb regla i compàs.

- Recordem també que no és possible la quadratura del cercle, és a dir, trobar un quadrat de la mateixa àrea que un cercle donat. Considerem un cercle de radi 1 i vegem que no podem construir un quadrat d'àrea π. Per això hauríem de construir un segment de longitud $\sqrt{\pi}$. El nombre real $\sqrt{\pi}$ és construïble si i només si ho és el seu quadrat. Però, com que π no és algebraic sobre $\mathbb{Q}$ (resultat que va provar Lindemann en 1882), es dedueix que no és un nombre construïble.

2.3 N-àgons regulars inscrits en corbes planes

Sigui $\mathcal{C}$ un corba plana i fixem P_0, P_N dos punts de la corba, no necessàriament diferents, de manera que delimitin un arc sobre la corba. Per a cada enter positiu N, ens plantegem la qüestió següent:

Problema. És possible construir amb regla i compàs punts $P_1, \ldots, P_{N-1}$ tals que divideixin l'arc $\widehat{P_0P_N}$ en N parts iguals? És a dir, de manera que les longituds d'arcs consecutius satisfacin $\ell(P_0, P_1) = \ell(P_1, P_2) = \cdots = \ell(P_{N-1}, P_N)$.

El problema plantejat en aquests termes resulta intractable. Òbviament, la resposta dependrà en primer lloc de quina sigui la corba $\mathcal{C}$ i dels punts P_0, P_N. Després es tractarà d'esbrinar quins són els enters N admisibles. No obstant això, cal fer notar una subtilesa afegida, que consisteix en precisar si hom pot o no fer ús de les interseccions de rectes i circumferències amb la corba $\mathcal{C}$. En cas afirmatiu, a priori, tenim més opcions per a construir N-àgons sobre $\mathcal{C}$.

En qualsevol cas, en aquest treball ens restringirem a suposar que la corba $\mathcal{C}$ és la lemniscata i prenem el criteri de no fer ús de la gràfica de la lemniscata en tractar sobre la constructibilitat dels seus N-àgons. Un dels objectius que perseguim és donar una prova del següent resultat.

Teorema 2.3.1 *El N-àgon regular sobre la lemniscata és construïble amb regla i compàs si i només si $N = 2^n\, p_1 \ldots p_r$, on p_i són primers de Fermat diferents.*

Podem comprovar com, sorprenentment, el resultat sobre els N-àgons regulars a la lemniscata és anàleg al cas circular. Recordem també que els primers de Fermat són els de la forma $2^{2^m} + 1$ per algun enter m i encara no se sap si n'existeixen infinits. Són primers de Fermat els corresponents als casos $m = 0, 1, 2, 3, 4$, és a dir, 3, 5, 17, 257 i 65537. Euler va descobrir que 641 divideix el nombre corresponent al cas $m = 5$, amb la qual cosa $2^{2^5} + 1$ no és primer. Fins avui no se'n coneix cap més. Podem dir, però, que no hi ha cap primer de Fermat més petit que 10^{40000} ([Ste], pàg. 170) .

Per acabar aquesta secció farem un breu recordatori d'una possible prova del cas circular, que fa ús de les extensions ciclotòmiques. Això ve motivat pel fet que la prova del cas lemniscàtic es fa de manera semblant, però amb extensions més complicades de tractar.

Teorema. (Gauss) *El N-àgon regular sobre la circumferència és construïble amb regla i compàs si i només si $N = 2^n p_1 \cdots p_r$, on els p_i són primers de Fermat diferents dos a dos.*

Sabem que el problema de construir el polígon regular de N costats és equivalent a construir els punts de N-divisió de la circumferència, la qual cosa és equivalent a construir les arrels del polinomi $X^N - 1$. Així, és suficient estudiar la constructibilitat d'una arrel N-èsima de la unitat, diem-li ξ_N. Pels criteris de constructibilitat esmentats anteriorment hem d'estudiar el grau de l'extensió de cossos $\mathbb{Q}(\xi_N)/\mathbb{Q}$, que és de Galois. Es té que $\mathrm{Gal}(\mathbb{Q}(\xi_N)/\mathbb{Q}) \simeq (\mathbb{Z}/N\mathbb{Z})^*$. Pel criteri 2 de constructibilitat arribem a la conclusió que ξ_N és construïble si i només si l'ordre de $(\mathbb{Z}/N\mathbb{Z})^*$ és una potència de 2, i això succeeix si i només si $N = 2^n p_1 \cdots p_r$, on els p_i són primers de Fermat diferents dos a dos.

Capítol 3

La lemniscata

3.1 Definicions equivalents

La **lemniscata** és el lloc geomètric dels punts del pla tals que el producte de les seves distàncies a dos punts donats, anomenats focus, és igual al quadrat de la meitat de la distància entre els focus. La lemniscata és un cas especial dels *òvals de Cassini*, que es defineixen com el lloc geomètric dels punts tals que el producte de les distàncies a dos punts donats és constant.

Siguin $F_1 = (-\frac{\sqrt{2}}{2}, 0)$ i $F_2 = (\frac{\sqrt{2}}{2}, 0)$. La equació de la lemniscata en coordenades cartesianes havent pres com a focus els punts F_1 i F_2 és

$$(x^2 + y^2)^2 = x^2 - y^2 \ . \tag{3.1}$$

A la figura 2 es representen els punts reals de la corba.

Si passem a coordenades polars, és a dir, $x = r\cos\theta$, $y = r\sin\theta$, tenim que l'equació que defineix la lemniscata és $r^2 = \cos 2\theta$. El diferencial de longitud d'arc lemniscàtic és

$$ds^2 = dx^2 + dy^2 = (\cos\theta dr - \sin\theta d\theta)^2 + (\sin\theta dr + \cos\theta r d\theta)^2 = dr^2 + r^2 d\theta^2 \ .$$

Atès que $2rdr = -2\sin 2\theta d\theta$ se segueix

$$ds^2 = dr^2 + r^2 d\theta^2 = dr^2 + \frac{r^4 dr^2}{1 - \cos^2 2\theta} = \frac{dr^2}{1 - r^4} \ .$$

Aleshores, la longitud de l'arc de lemniscata comprès entre l'origen i el punt amb mòdul r (veure figura 1) ve donada per l'expressió

$$s(r) = \int_0^r \frac{dx}{\sqrt{1 - x^4}} \ . \tag{3.2}$$

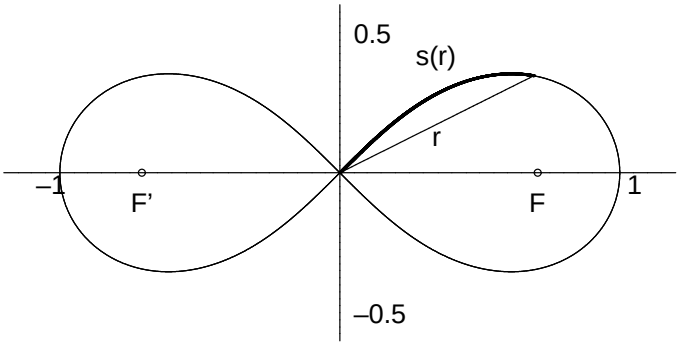

Figura 3.1: Punts reals de la lemniscata

A continuació detallem un procediment mecànic per a construir la lemniscata. Sigui $ABCD$ un antiparal·lelogram articulat de costats $AB = CD$ i tal que $CD = AD\sqrt{2}$, on els punts C i D estan fixats. Aleshores quan els punts A i B recorren respectivament les circumferències de centres D i C, es té que el punt mig M del segment AB descriu la lemniscata de Bernoulli. A la figura 3 s'il·lustra aquest mecanisme.

Vegem que en efecte M descriu la lemniscata. Tenim que $CD = AD\sqrt{2}$, o equivalentment, $CD\sqrt{2} = 2AD$ i per tant $AD = DM\sqrt{2}$. Els triangles ABD i BCD i els triangles ACD i ABC són semblants, amb la qual cosa es té que $\widehat{DAM} = \widehat{ACM}$ i $\widehat{ADM} = \widehat{MAC}$. Aleshores, els triangles MDA i MCA són semblants, i per tant, $DM : MA = MA : MC$, és a dir, $DM : MC = MA^2 = \frac{AD^2}{2} = (\frac{CD}{2})^2$.

La lemniscata també es pot definir com la intersecció d'un tor i del pla tangent al seu anell interior, on el tor és tal que el seu radi interior és igual al radi de la circumferència que el genera.

3.2 Propietats geomètriques

Tal com acabem de dir, la lemniscata és la corba algebraica plana corresponent al polinomi

$$f(x, y) = (x^2 + y^2)^2 - x^2 + y^2 \ .$$

Estudiarem tot seguit quines són les seves singularitats i de quin tipus són. Si calculem els punts singulars afins podem comprovar que només hi ha un,

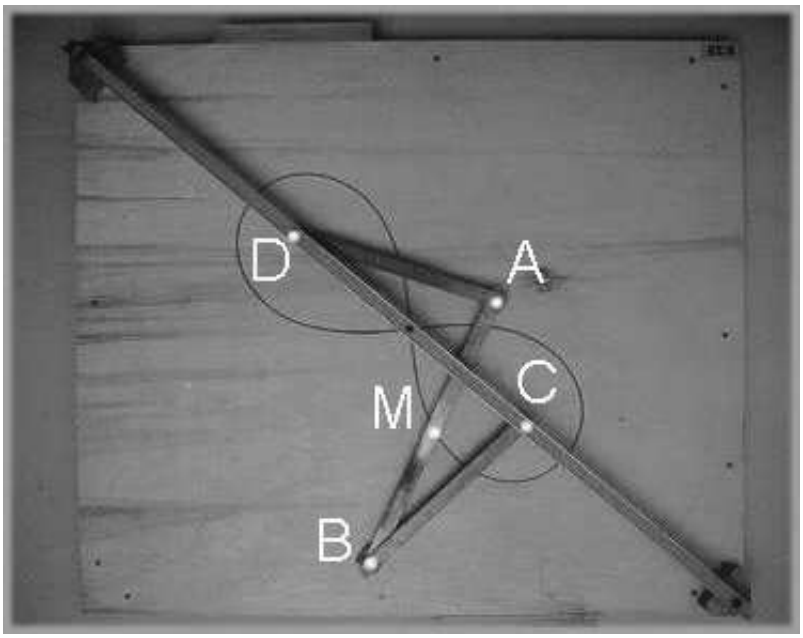

Figura 3.2: Construcció mecànica de la lemniscata

que és el $(0,0)$, amb multiplicitat 2 i rectes tangents diferents. Es tracta doncs d'un punt singular ordinari. En l'infinit la corba té dos punts, que són $[i:1:0]$ i $[-i:1:0]$, ambdós singulars, amb multiplicitat 2 i també ordinaris. Per tant, com que la corba té grau 4, i les seves singularitats són ordinàries, podem calcular el seu gènere a partir de la fórmula de Noether i concloem que és 0. Això vol dir que la lemniscata admet una parametrització racional. Per trobar-la farem servir que les relacions

$$x = \frac{\cos\theta}{1+\sin^2\theta} \quad , \quad y = \frac{\sin\theta\cos\theta}{1+\sin^2\theta} \tag{3.3}$$

són una parametrització trigonomètrica de la corba, com es pot comprovar veient que compleixen l'equació de la lemniscata. Ara, si fem el canvi $t = \tan\frac{\theta}{2}$, es compleix:

$$\sin\theta = \frac{2t}{1+t^2}$$

$$\cos\theta = \frac{1-t^2}{1+t^2} \ .$$

Si substituïm en l'expressió (3.3), obtenim

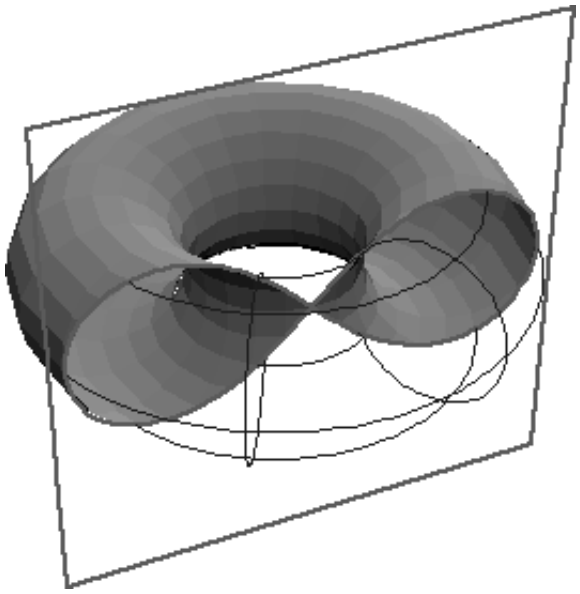

Figura 3.3: Definició de la lemniscata a partir d'un tor

$$x = \frac{1-t^4}{t^4+6t^2+1}$$

$$y = \frac{2t(1-t^2)}{t^4+6t^2+1}$$

que és el que volíem trobar. L'aplicació

$$\begin{array}{rcl} \mathbb{P}^1(\mathbb{Q}) & \longrightarrow & \text{lemniscata} \\ t & \longmapsto & \left(\dfrac{1-t^4}{t^4+6t^2+1}, \dfrac{2t(1-t^2)}{t^4+6t^2+1}\right) \\ \infty & \longmapsto & (-1,0) \end{array}$$

ens dóna els punts racionals de la lemniscata.

Capítol 4

Integrals el·líptiques

Per tal de fer N-divisions sobre corbes, resulta útil poder disposar de fórmules d'addició que permetin trobar l'arc doble, triple, ... d'un arc donat. En d'altres paraules, abans d'aprendre a dividir és convenient primer aprendre a sumar (quan això sigui possible). Un cas especialment tractable és el de les longituds d'arc que venen donades per integrals el·líptiques, atès que aquestes disposen de lleis d'addició expressables algebraicament. En les seccions següents, recordem els resultats principals de les integrals el·líptiques i les seves fórmules d'addició.

4.1 Tres espècies

Una *integral el·líptica* és una integral de la forma

$$\int R(x, \sqrt{G(x)})\, dx,$$

on $G(x)$ és un polinomi de grau 3 ó 4 sense arrels múltiples i $R(x, y)$ és una funció racional de dues variables. Se les anomena *el·líptiques* perquè apareixen en el càlcul de la longitud d'arc de l'el·lipse. Es pot veure que qualsevol integral el·líptica es pot reduir a una combinació dels tres tipus següents:

$$\int \frac{dx}{\sqrt{G(x)}}, \int \frac{x^2 dx}{\sqrt{G(x)}}, \int \frac{dx}{(x-c)\sqrt{G(x)}},$$

on $G(x) = (1-x^2)(1-k^2x^2)$. Aquestes darreres expressions es poden simplificar fent el canvi de variable $x = \sin\phi$. Aleshores les integrals abans esmentades s'expressen com segueix:

$$\int \frac{d\phi}{\sqrt{1-k^2\sin^2\phi}}\,, \int \frac{\sin^2\phi\, d\phi}{\sqrt{1-k^2\sin^2\phi}}\,, \int \frac{d\phi}{(\sin\phi - c)\sqrt{1-k^2\sin^2\phi}}\,.$$

Aquestes integrals reben el nom respectivament d'*integrals el·líptiques de primera, segona i tercera espècie*. Tots aquests resultats van ser provats per **Legendre** i es poden trobar al seu *Traité des fonctions elliptiques et des intégrales eulériennes* (1827-1832), on es recopilen un vast nombre de propietats sobre integrals el·líptiques.

4.2 Les fórmules d'addició

En aquesta secció presentem la llei d'addició per a les integrals el·líptiques de primera espècie

$$\int_0^r \frac{dx}{\sqrt{(1-x^2)(1-k^2x^2)}} = \int_0^\varphi \frac{d\phi}{\sqrt{1-k^2\sin^2\phi}} = F(\varphi)\,,$$

on $r = \sin\varphi$. Les lleis d'addició per a les integrals de segona i tercera espècie són més complicades, i no ens caldran en el present treball.

L'objectiu és trobar alguna relació entre els paràmetres φ, ψ, μ quan es es compleix la igualtat $F(\varphi) + F(\psi) = F(\mu)$. De fet veurem que $\sin\mu$ es pot expressar algebraicament en termes de $\sin\varphi$ i $\sin\psi$. Definim $\Delta(\psi) = \sqrt{1-k^2\sin^2\psi}$. Considerem l'equació diferencial

$$\frac{d\psi}{d\varphi} = -\frac{\sqrt{1-k^2\sin^2\psi}}{\sqrt{1-k^2\sin^2\varphi}}\,,$$

on entenem que ψ és funció de φ. L'equació és de variables separades, i per tant la seva integral és $F(\varphi) + F(\psi) - F(\mu) = 0$, on μ és una constant.

Demostrarem que l'expressió

$$\cos\mu = \cos\varphi\cos\psi - \sin\varphi\sin\psi\Delta(\mu) \tag{4.1}$$

també és integral de l'equació diferencial. Observem primer que en elevar al quadrat ambdós membres de la igualtat anterior s'obté

$$\cos^2\varphi + \cos^2\psi + \cos^2\mu - 2\cos\varphi\cos\psi\cos\mu + k^2\sin^2\varphi\sin^2\psi\sin^2\mu = 1 \tag{4.2}$$

i que aquesta expressió és simètrica respecte φ, ψ i μ. Aquesta simetria implica que si es compleix (4.1), aleshores també se satisfan les relacions:

$$\cos\psi = \cos\varphi\cos\mu - \sin\varphi\sin\mu\Delta(\psi) \quad (4.3)$$
$$\cos\varphi = \cos\mu\cos\psi - \sin\mu\sin\psi\Delta(\varphi)\ . \quad (4.4)$$

Per comprovar que (4.1) és integral de l'equació diferencial dividim per $\sin\varphi\sin\psi$ els dos membres de la igualtat i derivem respecte de φ considerant ψ com a funció de φ. El resultat es pot posar com

$$\frac{d\psi}{d\varphi} = -\frac{\frac{\cos\psi - \cos\mu\cos\varphi}{\sin\varphi}}{\frac{\cos\varphi - \cos\mu\cos\psi}{\sin\varphi}}\ .$$

Si fem servir les igualtats (4.3) i (4.4) s'arriba a que l'expressió anterior és equivalent a

$$\frac{d\psi}{d\varphi} = -\frac{\sqrt{1-k^2\sin^2\psi}}{\sqrt{1-k^2\sin^2\varphi}}\ ,$$

que és el que volíem veure.

Així, pel teorema d'unicitat en equacions diferencials, la igualtat $F(\varphi) + F(\psi) = F(\mu)$ implica que

$$\cos\mu = \cos\varphi\cos\psi - \sin\varphi\sin\psi\Delta(\mu)\ .$$

Per obtenir una expressió explícita, diem $x = \cos\mu$, i tenim $\sin^2\mu = 1 - x^2$. Així, la relació (4.2) es pot considerar com una equació en x i resolent-la s'obté

$$x = \cos\mu = \frac{\cos\varphi\cos\psi - \sin\psi\sin\varphi\Delta(\varphi)\Delta(\psi)}{1 - k^2\sin^2\varphi\sin^2\psi}.$$

D'aquí es dedueix també la següent expressió per $\sin\mu$:

$$\sin\mu = \frac{\sin\varphi\cos\psi\Delta(\psi) + \sin\psi\cos\varphi\Delta(\varphi)}{1 - k^2\sin^2\varphi\sin^2\psi}\ . \quad (4.5)$$

Presentem ara la llei d'addició de la integral el·líptica corresponent a la lemniscata.

4.3 Cas lemniscàtic

Examinem ara la integral el·líptica de primera espècie de mòdul $k = i$

$$\int_0^r \frac{dx}{\sqrt{(1-x^2)(1-(i^2)x^2)}} = \int_0^r \frac{dx}{\sqrt{1-x^4}} \ ,$$

que mesura la longitud d'arc de la lemniscata.
Donada la relació

$$\int_0^r \frac{dx}{\sqrt{1-x^4}} + \int_0^t \frac{dx}{\sqrt{1-x^4}} = \int_0^u \frac{dx}{\sqrt{1-x^4}}$$

vegem quin és el paràmetre u que la compleix en funció de r i t. Podem posar $r = \sin\varphi$, $t = \sin\psi$, $u = \sin\mu$, amb la qual cosa, suposant que $\varphi, \psi, \mu \in [0, \frac{\pi}{2}]$ tindrem $\cos\varphi = \sqrt{1-r^2}$, $\cos\psi = \sqrt{1-t^2}$. Aleshores, fent servir (4.5) trobem la relació

$$u = \frac{r\sqrt{1-t^4} + t\sqrt{1-r^4}}{1+r^2t^2} \ . \tag{4.6}$$

Hem obtingut per tant la llei d'addició que posseeix la integral de primera espècie $F(\varphi)$ amb mòdul $k = i$. Aquest resultat va ser descobert per **Euler** l'any 1753. El cas particular $r = t$, que correspon a doblar l'arc lemniscàtic, ja havia estat resolt per **Fagnano** 25 anys abans.

Capítol 5

Funcions el·líptiques

Suposem donada una funció sota el signe integral

$$\ell(x) = \int_{x_0}^{x} f(t)\, dt\,,$$

sense precisar quines hipòtesi requerim a les funcions $f(t)$ i $\ell(x)$. A la pràctica ens interessarà el cas en que $\ell(x)$ mesuri la longitud d'arc sobre una corba delimitat pels punts que queden determinats pel paràmetre x_0 (origen fixat) i el paràmetre x (variable).

El problema d'invertir una integral consisteix en estudiar (en cas que existeixi) la funció inversa de $\ell(x)$. És a dir, ens preguntem per l'existència i propietats d'una funció $x = p(y)$ tal que

$$y = \int_{p(y_0)=x_0}^{p(y)} f(t)\, dt\,.$$

L'interés per invertir integrals resulta obvi en el cas que ens ocupa. Donada la longitud y resultant de dividir l'arc total de la lemniscata en N parts iguals, voldrem trobar el punt $p(y)$ de la corba tal que l'arc corresponent realitza la longitud y. En el cas de la lemniscata, la funció que dóna la longitud d'arc es pot invertir i el que s'obté és una funció el·líptica.

5.1 Funcions el·líptiques

Una *ret* a $\mathbb{C}$ és el subgrup generat per dos nombres complexos (anomenats períodes) linealment independents sobre $\mathbb{R}$. Escriurem

$$\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2 \ .$$

Es diu que $f : \mathbb{C} \to \mathbb{P}^1(\mathbb{C})$ és una *funció el·líptica* respecte de la ret Λ si es compleix que f és meromorfa i $f(z) = f(z + \lambda)$ per a tot $\lambda \in \Lambda$. Es té que qualsevol nombre complex z pot expressar-se de la forma $z = a_1\omega_1 + a_2\omega_2$, amb $a_i \in \mathbb{R}$ únics. El nombre a_i es pot descomposar com la suma de la seva part entera i la seva part fraccionària, amb la qual cosa deduïm que una funció el·líptica queda completament determinada pels valors que pren a la regió

$$\{\alpha_1\omega_1 + \alpha_2\omega_2 \mid 0 \leq \alpha_1, \alpha_2 < 1\}$$

que rep el nom de *paral·lelogram fonamental* de Λ.

Donada una ret Λ, existeix una funció el·líptica notable, que s'anomena *funció de Weierstrass*, definida per

$$\wp(z) = \frac{1}{z^2} + \sum_{\lambda \in \Lambda - 0} \left(\frac{1}{(z-\lambda)^2} - \frac{1}{\lambda^2} \right) \ . \tag{5.1}$$

La seva derivada

$$\wp'(z) = -2 \sum_{\lambda \in \Lambda} \left(\frac{1}{z - \lambda} \right)^3 \tag{5.2}$$

també és una funció el·líptica respecte Λ. De les definicions es dedueix que $\wp(z)$ és una funció parell i que $\wp'(z)$ és una funció senar. La funció $\wp$ té un pol doble als elements de la ret, i no té cap altre singularitat, mentre que la funció $\wp'$ té un pol triple als elements de la ret com a úniques singularitats . Es té a més que $\wp'(z) = 0$ si i només si $z \equiv \frac{1}{2}\omega_1,\ \frac{1}{2}(\omega_1 + \omega_2),\ \frac{1}{2}\omega_2 \mod \Lambda$.

El conjunt de les funcions el·líptiques respecte una ret Λ formen un cos que denotarem per $\mathcal{M}(*)$. Es té que $\mathcal{M}(*) = \mathbb{C}(\wp, \wp')$, és a dir, que qualsevol funció el·líptica respecte una ret Λ pot expressar-se com una funció racional en $\wp$ i $\wp'$.

Una altra propietat important és que $\wp$ compleix l'equació diferencial

$$\wp'^2(z) = 4\wp(z)^3 - g_2(\Lambda)\wp(z) - g_3(\Lambda) \ ,$$

on $g_2(\Lambda) = 60 \sum_{\lambda \in \Lambda - 0} \lambda^{-4}$ i $g_3(\Lambda) = 140 \sum_{\lambda \in \Lambda - 0} \lambda^{-6}$.

Podem definir aleshores la *corba el·líptica*

$$E = \{(x, y) \in \mathbb{C}^2 \mid y^2 = 4x^3 - g_2(\Lambda)x - g_3(\Lambda)\} \cup \infty,$$

on el símbol ∞ denota el *punt de l'infinit* de la corba. Tenim per tant l'aplicació

$$\begin{array}{rccc} \phi & : & \mathbb{C}/\Lambda & \longrightarrow & E \\ & & z \neq 0 & \longmapsto & (\wp(z)\,,\, \wp'(z)) \\ & & 0 & \longmapsto & \infty \end{array}$$

que pot considerar-se com un homeomorfisme entre el tor complex $\mathbb{C}/\Lambda$ i la corba E. L'aplicació ϕ transporta l'estructura de grup abelià que $\mathbb{C}/\Lambda$ hereta de $\mathbb{C}$ a E, és a dir, si $(a, b), (c, d) \in E$ aleshores existeixen funcions f, g tals que

$$(a, b) + (c, d) = (f(a, b, c, d), g(a, b, c, d)).$$

Aquestes funcions es troben a partir de les lleis d'addició que tenen les funcions $\wp$ i $\wp'$. Recordem a continuació la llei de $\wp(z)$:

$$\wp(z_1 + z_2) = -\wp(z_1) - \wp(z_2) + \frac{1}{4}\left(\frac{\wp'(z_1) - \wp'(z_2)}{\wp(z_1) - \wp(z_2)}\right)^2 \tag{5.3}$$

per a $z_1, z_2 \notin \Lambda$ i $\wp(z_1) \neq \wp(z_2)$. Si $z_1 \equiv z_2 \bmod \Lambda$, aleshores

$$\wp(2z) = -2\wp(z) + \frac{1}{4}\left(\frac{\wp''(z)}{\wp'(z)}\right)^2 . \tag{5.4}$$

La llei d'addició de $\wp'(z)$ s'obté derivant les expressions anteriors. Així, deduïm l'existència de funcions algebraiques f_N, g_N tals que

$$N(x, y) = (x, y) + \overbrace{\cdots}^{N} + (x, y) = (f_N(x, y), g_N(x, y)).$$

Hem vist doncs que a cada ret de nombres complexos podem associar-li una corba el·líptica sobre $\mathbb{C}$. El recíproc també es compleix, resultat que es coneix com *teorema d'uniformització.*

Havíem vist que la longitud de l'arc de lemniscata comprès entre l'origen i el punt de mòdul r és $s(r) = \int_0^r \frac{dx}{\sqrt{1-x^4}}$. Volem invertir aquesta integral és

a dir, volem trobar per a quin paràmetre $\varphi(y)$, on y és una longitud d'arc donada (veure figura 6), es compleix

$$y = \int_0^{\varphi(y)} \frac{dx}{\sqrt{1-x^4}} \ .$$

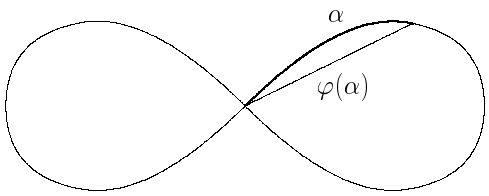

Figura 5.1: Definició de $\varphi(\alpha)$

Així, és obvi que $\varphi(s(r)) = r$. Tot seguit estudiarem les propietats més importants de la funció φ. Tenim que posseix una llei d'addició:

$$\varphi(u+v) = \frac{\varphi(u)\sqrt{1-\varphi^4(v)} + \varphi(v)\sqrt{1-\varphi^4(u)}}{1+\varphi^2(u)\varphi^2(v)} \ , \tag{5.5}$$

que es dedueix de (4.6), i amb la relació

$$ds = \frac{dr}{\sqrt{1-r^4}} = \frac{d\varphi(s)}{\sqrt{1-\varphi^4(s)}}$$

on s denota la longitud d'arc de la lemniscata, s'obté $\varphi'(s) = \sqrt{1-\varphi^4(s)}$ i per tant

$$\varphi(u+v) = \frac{\varphi(u)\varphi'(v) + \varphi'(u)\varphi(v)}{1+\varphi^2(u)\varphi^2(v)} \ . \tag{5.6}$$

Una altra propietat important de la funció φ és que $\varphi(iu) = i\varphi(u)$. Per provar-ho és suficient comprovar que fent $x = iy$ es compleix

$$\int_0^{ir} \frac{dx}{\sqrt{1-x^4}} = i\int_0^{r} \frac{dy}{\sqrt{1-y^4}}.$$

Sigui ω la longitud d'un *pètal* de la lemniscata (veure figura 4), amb la qual cosa la longitud total de la lemniscata és 2ω. Si calculem ω numèricament

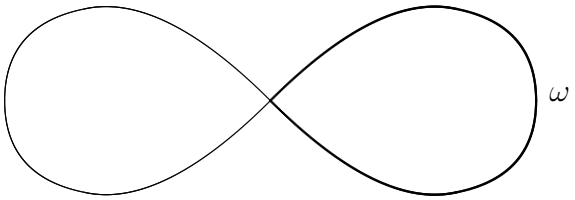

Figura 5.2: ω és la longitud d'un pètal de la lemniscata.

obtenim la següent aproximació: $\omega = 2.622057$. Es té que ω és un nombre transcendent. Una prova d'aquest resultat es pot trobar a [Wal] pàgina 91. És un resultat tècnic que utilitza mètodes de variable complexa. Sembla ser que el primer en demostrar la transcendentalitat del nombre ω va ser **Gelfond-Schneider**, matemàtic que va resoldre el 7è. problema de Hilbert, és a dir, que si α i β són nombres algebraics, $\alpha \neq 0, 1$ i $\beta \notin \mathbb{Q}$, aleshores α^β és un nombre transcendent.

Veurem que la funció φ és el·líptica respecte de la ret

$$\Lambda =< (1+i)\omega, (1-i)\omega > \ .$$

Per definició, $\varphi(\omega/2) = 1$ i, per tant, $\varphi'(\omega/2) = \sqrt{1-\varphi^4(\omega/2)} = 0$. D'altra banda, com que $\omega = \int_0^\pi \frac{d\psi}{\sqrt{1+\sin^2\psi}}$, fent $\psi = \pi$ en la igualtat $F(\varphi) + F(\psi) = F(\mu)$, de (4.5) se segueix

$$\sin\mu = \sin\varphi\cos\pi = -\sin\varphi$$

ja que $\Delta(\pi)$=1 i $\sin\pi = 0$. Per tant, si diem $u = F(\varphi)$, tenim que $\varphi(u+\omega) = -\varphi(u)$. Això implica $\varphi(u+i\omega) = -\varphi(u)$ i aleshores:

$$\begin{aligned} \varphi(u+\omega+i\omega) &= \varphi(u) \\ \varphi(u+\omega-i\omega) &= \varphi(u) \ . \end{aligned} \tag{5.7}$$

És a dir, $\omega(1+i)$, $\omega(1-i)$ són períodes de la funció φ. Per tant la funció φ queda determinada pels valors que pren en el seu paral·lelogram fonamental $R = \{\alpha_1\omega(1+i) + \alpha_2\omega(1-i) \mid 0 \leq \alpha_1, \alpha_2 < 1\}$.

Vegem ara quins són els pols i els zeros de φ. Siguin $\alpha, \beta \in \mathbb{R}$, aleshores

$$\varphi(\alpha+i\beta) = \frac{\varphi(\alpha)\varphi'(\beta) + i\varphi'(\alpha)\varphi(\beta)}{1-\varphi^2(\alpha)\varphi^2(\beta)}. \tag{5.8}$$

Com que $\varphi(\alpha)$ i $\varphi(\beta)$ són quantitats finites, aleshores $\varphi(\alpha+i\beta)=0$ només es pot complir quan $\varphi(\alpha)\varphi'(\beta)=\varphi'(\alpha)\varphi(\beta)=0$. Els zeros reals de la funció φ són de la forma $m\omega$, mentre que els zeros reals de φ' són de la forma $m+\frac{1}{2}\omega$, amb $m\in\mathbb{Z}$. Aleshores la condició $\varphi(\alpha)\varphi'(\beta)=\varphi'(\alpha)\varphi(\beta)=0$ es complirà pels nombres de la forma $m\omega+ni\omega$ o $(m+\frac{1}{2})\omega+(n+\frac{1}{2})i\omega$. És clar, però, que $\varphi(m\omega+ni\omega)=0$ per a tot $m,n\in\mathbb{Z}$ ja que, en aquest cas, $\varphi(\alpha)=\varphi(\beta)=0$ i el denominador de (5.8) és diferent de zero. El denominador, però, és nul pels nombres de la forma $(m+\frac{1}{2})\omega+(n+\frac{1}{2})i\omega$, i per tant, es té una indeterminació, que resoldrem tot seguit. Així, la relació

$$\varphi(u+\frac{\omega}{2})\varphi(u+\frac{i\omega}{2})=i\,\frac{\varphi'(u)}{1+\varphi^2(u)}\frac{\varphi'(u)}{1-\varphi^2(u)}=i$$

ens diu que si $\varphi(u+\frac{\omega}{2})=0$ aleshores $\varphi(u+\frac{i\omega}{2})=\infty$. Imposant doncs que $u+\frac{\omega}{2}$ sigui un zero de φ, s'infereix que els seus pols són de la forma $(m+\frac{1}{2})\omega+(n+\frac{1}{2})i\omega$, amb la qual cosa queda resolta la indeterminació. A partir de les expressions anteriors deduïm que els zeros i els pols de φ en el seu paral·lelogram fonamental són respectivament $\{0,\,\omega,\,i\omega,\,(1+i)\omega\}$ i $\{\frac{(1+i)\omega}{2},\,\frac{(3+i)\omega}{2},\,\frac{(1+3i)\omega}{2},\,\frac{(3+3i)\omega}{2}\}$.

De la discusió precedent deduïm que φ és una funció meromorfa, amb la qual cosa, com que també és biperiòdica, tenim que és una funció el·líptica respecte de la ret Λ. Aquest fet és un cas particular dels resultats que **Abel** va incloure a la seva obra *Recherches sur les fonctions elliptiques* (1827-1828), en què es demostra que la inversió de la integral el·líptica de primera espècie

$$\alpha=\int\frac{dx}{\sqrt{(1-c^2x^2)(1-e^2x^2)}}$$

dóna lloc a una funció $\varphi(\alpha)$ doblement periòdica a $\mathbb{C}$. Es pot dir que la teoria de les funcions el·líptiques comença amb aquesta obra d'**Abel**.

5.2 Multiplicació complexa

Recordem que en comentar la prova del teorema de **Gauss**, en què s'utilitzaven extensions ciclotòmiques, es va indicar que les extensions de cossos que sorgien al cas lemniscàtic eren més complicades de tractar. Doncs bé, per aquesta raó serà necessari aplicar un resultat sobre *multiplicació complexa*, concepte que introduirem tot seguit.

Es diu que dues corbes el·líptiques E i E' definides sobre $\mathbb{C}$ són *isomorfes*, si les seves rets respectives Λ i Λ' compleixen que $\Lambda = \alpha\Lambda'$ per algun $\alpha \in \mathbb{C}$. Podem considerar el grup d'automorfismes d'una corba el·líptica. En general, es té $\mathrm{End}(\mathbb{C}/\Lambda) = \mathbb{Z}$, però si hi ha algun altre element, es diu que la corba el·líptica $\mathbb{C}/\Lambda$ té multiplicació complexa. A més, hi ha un mètode per a construir corbes el·líptiques amb multiplicació complexa. Sigui $\mathcal{O}$ un ordre a un cos cuadràtic imaginari. Aleshores si $\mathfrak{a}$ és un ideal propi de $\mathcal{O}$ es pot pensar com una ret a $\mathbb{C}$, i es té que la corba el·líptica associada $\mathbb{C}/\mathfrak{a}$ té multiplicació complexa, ja que $\mathrm{End}(\mathbb{C}/\mathfrak{a}) = \mathcal{O}$.

Podem enunciar ara el teorema sobre multiplicació complexa necessari per a entendre la demostració d'**Abel-Rosen**.

Teorema 5.2.1 *Sigui K un cos quadràtic imaginari i sigui N un enter positiu. Es compleix que*

$$H_N = K(\jmath(\mathcal{O}_K), \tau(\frac{1}{N}; \mathcal{O}_K))$$

és el cos de classes del mòdul $N\mathcal{O}_K$, on la funció $\tau(z;\mathcal{O})$ es defineix com

$$\tau(z;\mathcal{O}) = \begin{cases} \dfrac{g_2(\mathcal{O})^2}{\Delta(\mathcal{O})}\wp(z;\mathcal{O})^2, & \text{si } g_3(\mathcal{O}) = 0\ ; \\ \dfrac{g_3(\mathcal{O})}{\Delta(\mathcal{O})}\wp(z;\mathcal{O})^3, & \text{si } g_2(\mathcal{O}) = 0\ ; \\ \dfrac{g_2(\mathcal{O})g_3(\mathcal{O})}{\Delta(\mathcal{O})}\wp(z;\mathcal{O}), & \text{altrament,} \end{cases}$$

amb $\Delta(\mathcal{O}) = g_2^3(\mathcal{O}) - 27g_3^2(\mathcal{O})$ i $\jmath(\mathcal{O}_K) = 1728\,\dfrac{g_2^3(\mathcal{O}_K)}{\Delta(\mathcal{O}_K)}$. Per tant, $\mathrm{Gal}(H_N/K) = \mathrm{Cl}(\mathcal{O})$.

Posem un exemple. Sigui $K = \mathbb{Q}(i)$ i $N = 5$. Si considerem $\mathbb{Z}[i] = \mathbb{Z} + i\mathbb{Z} = \Lambda_0$ com una ret, del fet que $i\Lambda_0 = \Lambda_0$ es dedueix que $g_3(\Lambda_0) = 0$. Aleshores tindrem

$$\Delta(\Lambda_0) = g_2^3(\Lambda_0) - 27g_3^2(\Lambda_0) = g_2^3(\Lambda_0), \quad \jmath(\Lambda_0) = 1728\frac{g_2^3(\Lambda_0)}{\Delta(\Lambda_0)} = 1728$$

i, per tant, $\tau(\frac{1}{5}, \Lambda_0) = \dfrac{\wp^2(\frac{1}{5}, \Lambda_0)}{g_2(\Lambda_0)}$. Aleshores, pel teorema 5.2.1 tenim que

$$K(\jmath(\Lambda_0), \tau(\frac{1}{5}, \Lambda_0)) = K(\frac{\wp^2(\frac{1}{5}, \Lambda_0)}{g_2(\Lambda_0)}) = H_5$$

és el cos de classes corresponent al mòdul $5\mathbb{Z}[i]$. A més, $\mathrm{Gal}(H_5/K) \simeq \mathrm{Cl}(\mathbb{Z}+5\mathbb{Z}[i])$. Per determinar $\mathrm{Cl}(\mathbb{Z}+5\mathbb{Z}[i])$ farem servir que la successió

$$\{\pm 1, \pm i\} = \mathbb{Z}[i]^* \xrightarrow{f} (\mathbb{Z}[i]/N\mathbb{Z}[i])^* \longrightarrow \mathrm{Cl}(\mathbb{Z}+N\mathbb{Z}[i]) \longrightarrow 1$$

és exacta (veure [Cox] pàgina 174), i per tant

$$(\mathbb{Z}[i]/N\mathbb{Z}[i])^*/\mathrm{Im}f \simeq \mathrm{Cl}(\mathbb{Z}+N\mathbb{Z}[i]) \ . \tag{5.9}$$

Pel cas $N = 5$ es compleix que els elements $\pm 1, \pm i$ són distints entre si a $G := (\mathbb{Z}[i]/5\mathbb{Z}[i])^*$. Es pot veure que $|G| = 16$, amb la qual cosa $\mathrm{Cl}(\mathbb{Z}+5\mathbb{Z}[i])$ és isomorf a $G/\{\pm 1, \pm i\}$ i té cardinal 4. Per tant, $[H_5 : K] = 2^2$.

Capítol 6

Polígons regulars lemniscàtics

Abans de procedir a la demostració del teorema d'Abel-Rosen presentarem els objectes que utilitzem. Treballarem amb les rets

$$\begin{aligned} \Lambda &=< 2\omega, 2i\omega > && \text{; (ret auxiliar)} \\ \Lambda_{\text{lem}} &=< (1+i)\omega, (1-i)\omega > && \text{; (ret lemniscàtica)} \\ \Lambda_0 &=< 1, i > && \text{; (ret gaussiana)} \end{aligned}$$

Es compleix $(1+i)\Lambda_{\text{lem}} = \Lambda = 2\omega\Lambda_0$, és a dir, les rets són *homotètiques*. Aquest fet implica que

$$\mathbb{C}(\wp_\Lambda, \wp'_\Lambda) \simeq \mathbb{C}(\wp_{\Lambda_{\text{lem}}}, \wp'_{\Lambda_{\text{lem}}}) \simeq \mathbb{C}(\wp_{\Lambda_0}, \wp'_{\Lambda_0}).$$

Les corbes el·líptiques que defineixen sobre $\mathbb{C}$ són isomorfes, és a dir,

$$\mathbb{C}/\Lambda \simeq \mathbb{C}/\Lambda_{\text{lem}} \simeq \mathbb{C}/\Lambda_0$$

i més endavant provarem que venen donades per les equacions

$$\begin{aligned} \mathbb{C}/\Lambda &: \; y^2 = 4x^3 - \frac{1}{4}x \\ \mathbb{C}/\Lambda_{\text{lem}} &: \; y^2 = 4x^3 + x \\ \mathbb{C}/\Lambda_0 &: \; y^2 = 4x^3 - 4\omega^4 x \ . \end{aligned}$$

Per a simplificar la notació posarem $\wp = \wp_\Lambda$, $\wp_{\text{lem}} = \wp_{\Lambda_{\text{lem}}}$, $\wp_0 = \wp_{\Lambda_0}$. Es tenen les següents relacions

$$2i\wp((1+i)z)) = \wp_{\text{lem}}(z), \qquad \wp(2\omega z) = \frac{1}{(2\omega)^2}\wp_0(z) \ . \tag{6.1}$$

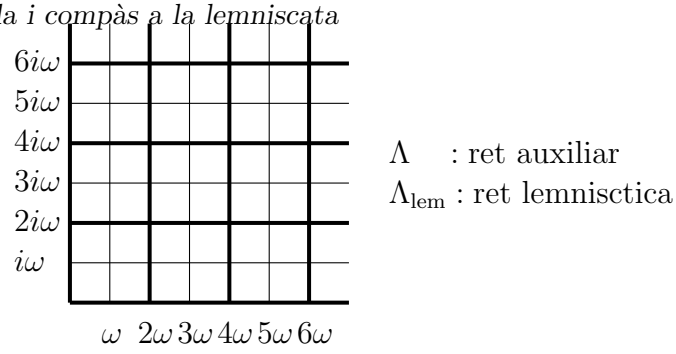

Figura 6.1: Les rets Λ i Λ_{lem}

Observem que els elements de la ret Λ també són elements de la ret Λ_{lem}, corresponent a la funció φ, com s'il·lustra a la figura 7.

A més, notem que les corbes el·líptiques abans definides tenen *multiplicació complexa*, donat que per a totes tres rets es compleix que si les multipliquem per i resten invariants.

6.1 El teorema d'Abel-Rosen

Teorema 6.1.1 *El N-àgon regular sobre la lemniscata és construïble amb regla i compàs si i només si $N = 2^n p_1 \dots p_r$, on p_i són primers de Fermat diferents.*

Primer pas. Volem dividir la lemniscata en N parts iguals. Sigui α la longitud de l'arc de lemniscata comprès entre l'origen i el punt (r, θ). Els punts que busquem són aquells pels quals $\alpha = \frac{2kw}{N}$, on $0 \leq k < N$. Suposem que podem construir els nombres $r = \varphi(\alpha)$. Atès que els punts de la lemniscata compleixen l'equació $r^2 = \cos 2\theta = 2\cos^2\theta - 1$, i per tant, $\cos\theta = \pm\sqrt{\frac{1+r^2}{2}}$, un cop tinguem r, podrem construir amb regla i compàs els nombres $r\sin\theta$ i $r\cos\theta$, amb la qual cosa obtindrem els punts $(r\cos\theta, r\sin\theta)$ sobre la lemniscata. Per tant, el problema de la N-divisió lemniscàtica amb regla i compàs es redueix ara a estudiar la constructibilitat dels nombres $\varphi(\frac{2k\omega}{N})$ per $k = 0, \dots, N-1$.

Segon pas. El nostre objectiu ara és provar que els *punts de N-torsió* de

la corba el·líptica $E \simeq \mathbb{C}/\Lambda$ són construïbles amb regla i compàs si i només si els punts de N-divisió de la lemniscata ho són. Denotarem per $E[N]$ el subgrup de E format pels punts de N-torsió. Donat que $E \simeq \mathbb{C}/\Lambda$, tenim $E[N] \simeq \frac{1}{N}\Lambda/\Lambda \simeq \Lambda/N\Lambda$, el que implica que $E[N]$ té N^2 elements. De forma explícita

$$E[N] = \{(\wp\left(\frac{2a\omega + 2bi\omega}{N}\right), \wp'\left(\frac{2a\omega + 2bi\omega}{N}\right)) \mid 0 \leq a, b < N\} \ ,$$

on al punt de l'infinit li correspon $a = b = 0$. Per exemple, els elements de $E[2]$ són $\{\infty, (e_1, 0), (e_2, 0), (e_3, 0)\}$ on

$$e_1 = \wp(\omega), \quad e_2 = \wp(i\omega), \quad e_3 = \wp((1+i)\omega) \ .$$

Observem que e_1, e_2, e_3 són les arrels de $4x^3 - \frac{1}{4}x = 0$, és a dir, $e_1 = \frac{1}{4}$, $e_2 = -\frac{1}{4}$ i $e_3 = 0$. Amb la definició de $\wp(z)$ comprovem que $\wp(iz) = -\wp(z)$ i, derivant, que $\wp'(iz) = i\wp'(z)$. Usant la fórmula d'addició es comproven les igualtats

$$\wp((1+i)z) = -\frac{i}{8}\frac{4\wp^2(z) - \frac{1}{4}}{\wp(z)} \tag{6.2}$$

$$\wp((1-i)z) = \frac{i}{8}\frac{4\wp^2(z) - \frac{1}{4}}{\wp(z)} \ . \tag{6.3}$$

Lema 6.1.1 *Si $\wp(\alpha)$ és construïble, també ho és $\wp(\frac{\alpha}{2})$.*

En l'expressió (6.2) substituïm $z = \frac{\alpha}{1+i}$ i observem aleshores que $\wp(\frac{\alpha}{1+i})$ satisfà una equació quadràtica amb coeficients construïbles. Per tant $\wp(\frac{\alpha}{1+i})$ és construïble. Substituïm ara $z = \frac{\alpha}{2}$ a (6.3). Aleshores, com que

$$\wp((1-i)\frac{\alpha}{2}) = \wp\left((1-i)\frac{(1+i)\alpha}{(1+i)2}\right) = \wp\left(\frac{\alpha}{1+i}\right)$$

és construïble, $\wp(\frac{\alpha}{2})$ és solució d'una equació quadràtica amb coeficients construïbles, i per tant $\wp(\frac{\alpha}{2})$ és construïble.

Corol·lari 6.1.1 *Siguin $a, b, n \in \mathbb{Z}$ tals que $ab \neq 0$ i $n \geq 1$. Aleshores, els nombres*

$$\wp\left(\frac{2a\omega + 2bi\omega}{2^n}\right)$$

són construïbles.

Sabem que els nombres $\{\wp(\omega), \wp(i\omega), \wp((1+i)\omega)\}$ són construïbles. A més, com que $\wp'^2(z) = 4\wp(z)^3 - \frac{1}{4}\wp(z)$ i $\wp''(z) = 6\wp^2(z) - \frac{1}{8}$ es dedueix que si $\wp(z)$ és construïble també ho són $\wp'(z)$ i $\wp''(z)$. Així, utilitzant (5.4) veiem que si $\wp(\omega)$ és construïble també ho és $\wp(2\omega)$. Per inducció provem doncs que $\wp(2n\omega)$ és construïble per $n \in \mathbb{N}-0$. Fent servir aleshores que $\wp$ és una funció parell, provem que $\wp(2a\omega)$ és construïble per $a \in \mathbb{Z}, a \neq 0$. Raonant de forma anàloga es demostra que $\wp(2bi\omega)$ és construïble per $b \in \mathbb{Z}, b \neq 0$ i utilitzant altre cop la llei d'addició de $\wp$, provem que $\wp(2a\omega + 2bi\omega)$ és construïble per $a, b \in \mathbb{Z},\ ab \neq 0$. Així hem demostrat l'enunciat pel cas $n = 1$ i a, b general. Per provar el cas n qualsevol s'utilitza inducció i el lema 6.1.1.

Proposició 6.1.1 *$\varphi(\alpha)$ és construïble si i només si $\wp(\alpha)$ és construïble.*

Demostrarem primer la condició necessària. Notem que la funció φ és el·líptica respecte la ret Λ_{lem}, cosa que ja sabíem, però també ho és respecte la ret Λ, ja que es compleix $\Lambda \subset \Lambda_{\text{lem}}$. Per a demostrar la condició necessària considerarem φ com una funció el·líptica respecte Λ. Així, és fàcil veure que els zeros i pols de φ mòdul Λ són respectivament $\{0, \omega, i\omega, (1+i)\omega\}$ i $\{\frac{(1+i)\omega}{2}, \frac{(3+i)\omega}{2}, \frac{(1+3i)\omega}{2}, \frac{(3+3i)\omega}{2}\}$. La funció $\wp'(z)$ també té com a zeros els punts $\omega, i\omega, (1+i)\omega$ mòdul Λ. A més

$$\wp\left(\frac{(1+i)\omega}{2}\right) = \wp\left(\frac{(3+3i)\omega}{2}\right) \quad \text{i} \quad \wp\left(\frac{(3+i)\omega}{2}\right) = \wp\left(\frac{(1+3i)\omega}{2}\right).$$

La funció

$$g(z) = \frac{\wp'(z)}{(\wp(z) - \wp(\frac{(1+i)\omega}{2}))(\wp(z) - \wp(\frac{(3+i)\omega}{2}))}$$

té els mateixos zeros i pols mòdul Λ que φ . Per tant, existeix $M \in \mathbb{C}$ tal que $\varphi(z) = Mg(z)$. Com que $\varphi(\frac{\omega}{2}) = 1$ i $g(\frac{\omega}{2})$ és construïble pel corol·lari 6.1.1, deduïm que M és construïble. De fet, fent els càlculs adients, hom troba que $M = \frac{-1}{2}$. Aleshores si $\wp(\alpha)$ és construïble, $g(\alpha)$ també ho és, i per tant, $\varphi(\alpha)$ és construïble.

Provem ara la condició suficient. Hem vist que $\varphi(z)$ és una funció el·líptica respecte de la ret $\Lambda_{\text{lem}} = \{m(1+i)\omega + n(1-i)\omega \mid m, n \in \mathbb{Z}\}$. Els zeros i el pols de φ mòdul Λ_{lem} són respectivament $\{0, \omega\}$ i $\{\frac{(1+i)\omega}{2}, \frac{(1-i)\omega}{2}\}$. Comparant els zeros i els pols deduïm l'existència d'una constant $C \in \mathbb{C}$ tal que

$$\varphi(z) = C\frac{\wp_{\text{lem}}(z) - \wp_{\text{lem}}(\omega)}{\wp'_{\text{lem}}(z)}.$$

Vegem que C és construïble. Sabem que $\varphi(\frac{\omega}{2}) = 1$. A més, de la relació

$$\wp_{\text{lem}}(\frac{\omega}{2}) = 2i\wp(\frac{(1+i)\omega}{2})$$

i el corol·lari 6.1.1 deduïm que $\wp_{\text{lem}}(\frac{\omega}{2})$ és construïble, i per tant, $\wp_{\text{lem}}(\omega)$ i $\wp'_{\text{lem}}(\frac{\omega}{2})$ també ho són. Aleshores C també és construïble, ja que s'expressa com a producte de nombres construïbles. De fet, calculant les sèries de Laurent entorn de $z = 0$ de les funcions involucrades, hom troba que $C = -2$. `Xavi, cuidadin con lo de involucrades`

Siguin $u_0 = \frac{(1+i)\omega}{2}$ i $u_1 = \frac{(1-i)\omega}{2}$. Com que els zeros de $\wp'_{\text{lem}}(z)$ són u_0, u_1 i ω, trobem

$$\begin{aligned}\varphi^2(z) &= C^2\frac{(\wp_{\text{lem}}(z) - \wp_{\text{lem}}(\omega))^2}{\wp'_{\text{lem}}(z)^2} \\ &= \frac{C^2}{4}\frac{\wp_{\text{lem}}(z) - \wp_{\text{lem}}(\omega)}{(\wp_{\text{lem}}(z) - \wp_{\text{lem}}(u_0))(\wp_{\text{lem}}(z) - \wp_{\text{lem}}(u_1))}. \qquad (6.4)\end{aligned}$$

Del fet que $g_2(\Lambda) = \frac{1}{4}$ i $g_3(\Lambda) = 0$ es dedueix que $g_2(\Lambda_{\text{lem}}) = -1$ i $g_3(\Lambda_{\text{lem}}) = 0$, amb la qual cosa tenim que els nombres $\wp_{\text{lem}}(u_0)$ i $\wp_{\text{lem}}(u_1)$ són construïbles. Aleshores, si $\varphi(\alpha)$ és construïble, tindrem que $\wp_{\text{lem}}(\alpha)$ és solució d'una equació quadràtica amb coeficients construïbles, i per tant també serà construïble. A més com que

$$\wp_{\text{lem}}(z) = 2i\wp((1+i)z) = \frac{1}{4}\frac{4\wp^2(z) - \frac{1}{4}}{\wp(z)} \ ,$$

si $\wp_{\text{lem}}(\alpha)$ és construïble, es dedueix que $\wp(\alpha)$ també ho és. Això acaba la prova de la proposició.

Hem vist, doncs, que estudiar la constructibilitat dels punts de N-divisió de la lemniscata és equivalent a estudiar la constructibilitat dels punts $\wp(\frac{2k\omega}{N})$ per $k = 0, \ldots, N-1$, qüestió que tractarem tot seguit.

Tercer pas. Considerem el subgrup $E[N]$ de E. Atesa la llei d'addició de la funció $\wp$, resulta que les coordenades cartesianes dels punts de $E[N]$ són algebraiques sobre $\mathbb{Q}$. Sigui $\mathbf{K}_N/\mathbb{Q}$ la *mínima extensió* de cossos que conté tots aquests nombres. Vegem que $\mathbf{K}_N/\mathbb{Q}$ és de Galois. Sigui $\mathrm{G}_{\mathbb{Q}}$ el grup de Galois absolut $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Aleshores definim el morfisme de grups

$$\rho \ : \mathrm{G}_{\mathbb{Q}} \longrightarrow \mathrm{Aut}([E[N]) \ ,$$

on $\mathrm{Aut}(E[N])$ denota el grup de automorfismes de $E[N]$. Es compleix

$$\mathrm{Aut}(E[N]) \simeq \mathrm{Aut}(\Lambda/N\Lambda) \simeq \mathrm{Aut}(\mathbb{Z}/N\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}) \simeq \mathrm{Gl}_2(\mathbb{Z}/N\mathbb{Z}).$$

El primer teorema de isomorfisme ens diu que $\mathrm{Nuc}\rho \lhd \mathrm{G}_{\mathbb{Q}}$ i $\mathrm{G}_{\mathbb{Q}}/\mathrm{Nuc}\rho \simeq \mathrm{Im}\rho$. Però $\mathrm{Nuc}\rho = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbf{K}_N)$, ja que per definició està format pels $\sigma \in \mathrm{G}_{\mathbb{Q}}$ que deixen fixos els elements de $E[N]$. Per tant, tenim que $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbf{K}_N) \lhd \mathrm{G}_{\mathbb{Q}}$, i per tant $\mathbf{K}_N/\mathbb{Q}$ és una extensió de Galois.

Denotem per G_N el seu grup de Galois. Aleshores G_N té una acció sobre $E[N]$ que ens dóna un morfisme injectiu $G_N \hookrightarrow \mathrm{Aut}(E[N])$. En el cas que N sigui un nombre primer, l'ordre de $\mathrm{Gl}_2(\mathbb{Z}/N\mathbb{Z})$ és igual al nombre de bases de $\mathbb{Z}/N\mathbb{Z} \oplus \mathbb{Z}/N\mathbb{Z}$, és a dir, $(N^2-1)(N^2-N)$. Aquest nombre és divisible per $N(N+1)$, la qual cosa implica que si $N \geq 2$ no pot ser una potència de dos. Com que l'únic que podem afirmar és que l'ordre de G_N divideix $(N^2-1)(N^2-N)$, els arguments anteriors no permeten, a priori, concloure res sobre la constructibilitat dels punts de $E[N]$.

Ara farem servir el fet que la ret $\Lambda =< 2\omega, 2\omega i >= 2\omega\mathbb{Z}[i]$ és un $\mathbb{Z}[i]$-mòdul. Així, com que la corba el·líptica $E = \mathbb{C}/\Lambda$ té multiplicació complexa per $\mathbb{Z}[i]$, dotem a E d'una estructura de $\mathbb{Z}[i]$-mòdul. Hem vist abans que $\wp(iz) = -\wp(z)$ i $\wp'(iz) = i\wp'(z)$, amb la qual cosa tenim que l'acció de i sobre E ve donada per $i(x,y) = (-x, iy)$. Per tant podem considerar $E[N] \simeq \frac{1}{n}\Lambda/\Lambda \simeq \Lambda/N\Lambda \simeq \mathbb{Z}[i]/N\mathbb{Z}[i]$ com a $\mathbb{Z}[i]$-mòdul.

Sigui $K = \mathbb{Q}(i)$ i adjuntem les coordenades cartesianes de $E[N]$ a K. El cos resultant el denotem per K_N, i sigui $\mathcal{G}_N$ el seu grup de Galois sobre K. Com que $\mathcal{G}_N$ deixa i fix, $\mathcal{G}_N$ té una acció sobre $E[N]$ que preserva la seva estructura de $\mathbb{Z}[i]$-mòdul. Així, cada $\sigma \in \mathcal{G}_N$ es pot considerar com un $\mathbb{Z}[i]$-automorfisme de $E[N]$, la qual cosa ens dóna un morfisme injectiu de $\mathcal{G}_N$ al grup dels $\mathbb{Z}[i]$-automorfismes de $E[N]$. Com que $E[N] \simeq \mathbb{Z}[i]/N\mathbb{Z}[i]$, tindrem

$$\mathrm{Aut}_{\mathbb{Z}[i]}(E[N]) \simeq \mathrm{Aut}_{\mathbb{Z}[i]}(\mathbb{Z}[i]/N\mathbb{Z}[i]) \simeq (\mathbb{Z}[i]/N\mathbb{Z}[i])^* \ .$$

Proposició 6.1.2 *El grup $\mathcal{G}_N$ és abelià. Si $(\mathbb{Z}[i]/N\mathbb{Z}[i])^*$ té ordre potència de 2, aleshores els nombres*

$$\wp\left(\frac{2a\omega + 2bi\omega}{N}\right), \wp'\left(\frac{2a\omega + 2bi\omega}{N}\right)$$

són construïbles.

Que el grup $\mathcal{G}_{\mathcal{N}}$ és abelià es dedueix del fet que la seva imatge pel morfisme injectiu abans descrit és un subgrup de $(\mathbb{Z}[i]/N\mathbb{Z}[i])^*$. L'afirmació sobre la constructibilitat se segueix del fet que K_N/K és una extensió de Galois i $[K_N : K]$ és potència de 2, i per tant, pel criteri 3 de constructibilitat, deduïm que els elements de $E[N]$ són construïbles.

Considerem ara el següent lema.

Lema 6.1.2 *$(\mathbb{Z}[i]/N\mathbb{Z}[i])^*$ és un grup d'ordre potència de dos si i només si $N = 2^n p_1 \cdots p_k$, on els p_i són primers de Fermat diferents dos a dos.*

Per provar aquest resultat hem d'estudiar quins són els primers a $\mathbb{Z}[i]$, que és un anell euclidià per la norma

$$\begin{array}{rccc} \mathbf{N} & : & \mathbb{Z}[i] & \to & \mathbb{Z} \\ & & a+bi & \mapsto & a^2+b^2. \end{array}$$

Els fets següents són coneguts:

1. Sigui $p \in \mathbb{Z}$ un nombre primer. Aleshores

- Si $p = 2$, es té que $1 + i$ és primer a $\mathbb{Z}[i]$ i $2 = i^3(1 + i)^2$.
- Si $p \equiv 1 \bmod 4$, existeix un primer $\pi \in \mathbb{Z}[i]$ tal que $p = \pi\bar{\pi}$, i els primers π i $\bar{\pi}$ són no associats a $\mathbb{Z}[i]$.
- Si $p \equiv 3 \bmod 4$, aleshores p és primer a $\mathbb{Z}[i]$.

A més, qualsevol primer de $\mathbb{Z}[i]$ és associat a un dels primers esmentats anteriorment.

2. Sigui $\mathfrak{a}$ un ideal de $\mathbb{Z}[i]$, i sigui $\mathfrak{a} = \prod_{j=1}^{r} \mathfrak{p}_j^{n_j}$ la seva factorització en ideals primers. Aleshores

$$|(\mathbb{Z}[i]/\mathfrak{a})^*| = \prod \mathbf{N}(\mathfrak{p}_j)^{n_j-1}(\mathbf{N}(\mathfrak{p}_j) - 1) \ .$$

Volem saber quan $|(\mathbb{Z}[i]/N\mathbb{Z}[i])^*|$ és una potència de 2. Sigui $N = p_1^{n_1} \cdots p_r^{n_r}$ la factorització de N en nombres primers. Per **1** es pot donar

1. $p_j \equiv 1 \mod 4$ i aleshores $p_j = \pi_j\bar{\pi}_j$ i $\mathbf{N}(\pi_j) = \mathbf{N}(\bar{\pi}_j) = p_j$
2. $p_j \equiv 3 \mod 4$ i per tant p_j és primer, amb la qual cosa $\mathbf{N}(p_j) = p_j^2$

3. Si $p_j = 2$ aleshores $2 = i^3(1+i)^2$ i $\mathbf{N}(1+i) = 2$.

Així, tindrem

$$\mathfrak{a} = N\mathbb{Z}[i] = (p_1^{n_1} \cdots p_r^{n_r})\mathbb{Z}[i] = p_1^{n_1}\mathbb{Z}[i] \cdots p_r^{n_r}\mathbb{Z}[i] \ ,$$

amb $p_i \neq p_j$ si $i \neq j$, i aleshores

$$p_j^{n_j}\mathbb{Z}[i] = \begin{cases} \pi_j^{n_j}\mathbb{Z}[i]\bar{\pi}_j^{n_j}\mathbb{Z}[i] & p_j \equiv 1 \mod 4 \\ \\ p_j^{n_j}\mathbb{Z}[i] & p_j \equiv 3 \mod 4 \ . \end{cases}$$

Per **2** tenim que cada factor primer $p_j \neq 2$ de N contribuirà al cardinal de $\mathbb{Z}[i]/N\mathbb{Z}[i]$ amb els factors $p_j^{n_j-1}(p_j-1)$ ó $p_j^{2(n_j-1)}(p_j^2-1)$, amb la qual cosa és necessari que $n_j = 1$, ja que altrament $|(\mathbb{Z}[i]/N\mathbb{Z}[i])^*|$ seria divisible per factors diferents de 2. Ens queda per estudiar quan les quantitats $p_j - 1$ i $p_j^2 - 1$ són potències de dos. Si $p_j = 3$ es compleix trivialment. Suposem doncs $p_j > 3$ i $p_j^2 - 1 = 2^m = (p_j-1)(p_j+1)$. Tindrem

$$\begin{aligned} p_j + 1 &= 2^{m_1} \\ p_j - 1 &= 2^{m_2} \qquad \text{on} \quad m_1 + m_2 = m \end{aligned} \tag{6.5}$$

amb la qual cosa $p_j = 2^{m_1-1} + 2^{m_2-1}$ i com que $p_j > 3$ és un primer senar arribem a un absurd. Per tant el cas $p_j^2 - 1 = 2^m$ és impossible, i s'haurà de complir $p_j - 1 = 2^m$. Observem, però, que en aquest cas el nombre m no pot tenir divisors senars. Altrament tindríem que si $2l+1 \mid m$ llavors $p_j = 2^m + 1 = x^{2l+1} + 1$ i fent servir la igualtat

$$\frac{x^{2l+1}+1}{x+1} = x^{2l} - x^{2l-1} + \ldots + (-1)^k x^{2l-k} + \ldots + 1$$

s'arriba a la conclusió que p_j no és primer. Per tant, p_j és de la forma $2^{2^m}+1$ és a dir, és un primer de Fermat. Així, acabem de provar que $N = 2^n p_1 \cdots p_r$, on els p_i són primers de Fermat, que és el que afirmava el lema 6.1.2.

Amb el lema anterior i la proposició 6.1.2 queda demostrada la condició suficient del teorema, que va ser la condició que va provar **Abel**. Per provar la condició necessària, deguda a **Rosen**, primer demostrarem el següent lema, que utilitza el resultat de multiplicació complexa de la secció 5.2 .

Lema 6.1.3 *Sigui F_N el cos que s'obté en adjuntar $\wp(\frac{2\omega}{N})^2$ a $K = \mathbb{Q}(i)$. Aleshores F_N/K és una extensió de Galois i el seu grup de Galois és isomorf a $(\mathbb{Z}[i]/N\mathbb{Z}[i])^*$ mòdul la imatge del grup $\{\pm 1, \pm i\}$.*

Considerem la ret Λ_0 i la funció $\wp_0(z)$. Definim $h(z) = \frac{\wp_0(z)^2}{g_2(\Lambda_0)}$. Com que $\jmath(\Lambda_0) = 1728$ i $g_3(\Lambda_0) = 0$, amb la qual cosa

$$\tau(\frac{1}{N}, \Lambda_0) = \frac{g_2(\Lambda_0)^2}{g_2(\Lambda_0)^3}\wp_0^2\left(\frac{1}{N}\right) = \frac{\wp_0(\frac{1}{N})^2}{g_2(\Lambda_0)} = h\left(\frac{1}{N}\right) \ ,$$

se segueix del teorema 5.2.1 apartat i) que $K(h(\frac{1}{N}))$ és el *cos de classes* de K corresponent al mòdul $N\mathbb{Z}[i]$. El *grup de classes* és $\mathrm{Cl}(\mathbb{Z} + N\mathbb{Z}[i])$, que per (5.9) és isomorf a $(\mathbb{Z}[i]/N\mathbb{Z}[i])^*$ mòdul la imatge del grup $\{\pm 1, \pm i\}$. Per a completar la demostració cal comprovar que $h(\frac{1}{N}) = 4\wp(\frac{2\omega}{N})^2$.

Sabem que $\wp(2\omega z) = \frac{1}{(2\omega)^2}\wp_0(z)$. Més endavant demostrarem que

$$\sum_{\gamma \in \mathbb{Z}[i]-0} \frac{1}{\gamma^4} = \frac{\omega^4}{15}$$

i per tant, $g_2(\Lambda_0) = 60 \sum_{\gamma\in\mathbb{Z}[i]} \frac{1}{\gamma^4} = 4\omega^4$. Així, s'obté que

$$h(z) = \frac{1}{4\omega^4}(2\omega)^4\wp(2\omega z)^2 = 4\wp(2\omega z)^2 \ .$$

Provem ara la condició necessària del teorema d'Abel-Rosen. Suposem doncs que el N-àgon regular lemniscàtic és construïble amb regla i compàs. Això implica que $\varphi(\frac{2\omega}{N})$ és construïble, i per la proposició 6.1.1 tenim que $\wp(\frac{2\omega}{N})$ també ho és. Així, el criteri 1 de constructibilitat ens diu que $[\mathbb{Q} : \mathbb{Q}(\wp(\frac{2\omega}{N})^2]$ és potència de 2, la qual cosa implica que $[F_N : K]$ també ho és. Aleshores, pel lema 6.1.3, $(\mathbb{Z}[i]/N\mathbb{Z}[i])^*$ té ordre potència de 2, i llavors, fent servir el lema 6.1.2, concloem que $N = 2^n p_1 \cdots p_r$ on els p_i són primers de Fermat diferents dos a dos.

Per completar la prova del teorema d'Abel-Rosen resta comprovar que per a la ret $\Lambda = \{2a\omega + 2bi\omega \mid a, b \in \mathbb{Z}\}$ es compleix

$$g_2(\Lambda) = 60 \sum_{\gamma\in\Lambda-0} \frac{1}{\gamma^4} = \frac{1}{4} \quad \text{i} \quad g_3(\Lambda) = 140 \sum_{\gamma\in\Lambda-0} \frac{1}{\gamma^6} = 0 \ .$$

És immediat veure que $g_2(\alpha\Lambda) = \alpha^{-4}g_2(\Lambda)$ i $g_3(\alpha\Lambda) = \alpha^{-6}g_3(\Lambda)$. Aleshores, com que $i\Lambda = \Lambda$ es té que $g_3(\Lambda) = g_3(i\Lambda) = i^{-6}g_3(\Lambda) = -g_3(\Lambda)$, i per tant

$g_3 = 0$. Ocupem-nos del cas g_2. Considerem les rets disjuntes

$$\begin{aligned} L_0 &= \{a\omega + bi\omega \mid a, b \in \mathbb{N}\}, \\ L_1 &= \left\{\frac{a\omega + bi\omega}{2} \mid a \text{ i } b \text{ senars}\right\}, \\ L_2 &= \left\{\frac{a\omega + bi\omega}{2} \mid a - b \text{ senar}\right\}. \end{aligned}$$

Aleshores $\frac{1}{2}L_0 = L_0 \cup L_1 \cup L_2$ i $L_2 = \frac{1+i}{2}L_1$. Definim $|L| = \sum_{l\in L} \frac{1}{l^4}$. Aleshores

$$16\,|L_0| = \left|\frac{1}{2}L_0\right| = |L_0| + |L_1| + |L_2| \quad \text{i} \quad |L_2| = \left(\frac{2}{1+i}\right)|L_1| = -4\,|L_1|$$

i per tant, $|L_1| = -5\,|L_0|$. Provarem la igualtat $|L_0| = \frac{1}{15}$, que és equivalent a afirmar que $g_2 = \frac{1}{4}$, però per això necessitem encara una altra relació entre $|L_1|$ i $|L_0|$. Per fer-ho utilitzem que L_0 és la ret dels zeros de $\varphi(z)$ i que L_1 és la ret dels seus pols. Com que $\varphi'(0) = 1$ tenim

$$\varphi(z) = z \prod_{\alpha\in L_0}\left(1 - \frac{z}{\alpha}\right)\prod_{\beta\in L_1}\left(1 - \frac{z}{\beta}\right)^{-1}$$

on els productes infinits s'han d'entendre com a límit de productes finits sobre $|\alpha|, |\beta| \le M$ amb $M \to \infty$. Els elements no nuls de les rets L_0 i L_1 es poden separar en 4 classes de la forma $\{\pm\gamma, \pm i\gamma\}$, amb la qual cosa podem posar

$$\varphi(z) = z \prod\left(1 - \frac{z}{\alpha^4}\right)\prod\left(1 - \frac{z}{\beta^4}\right)^{-1}$$

on $0 \le \arg\alpha, \arg\beta < \frac{\pi}{2}$. A més, com que la funció $\frac{\varphi(z)}{z}$ és invariant pel canvi $z \to -z$ ó $z \to \pm iz$, tindrem que $\frac{\varphi(z)}{z}$ és funció de z^4 i ens queda la següent expressió per $\varphi(z)$

$$\varphi(z) = z \prod\left(1 - \frac{z^4}{\alpha^4}\right)\prod\left(1 - \frac{z^4}{\beta^4}\right)^{-1}.$$

Per tant, la seva derivada logarítmica resulta ser

$$z\frac{\varphi'(z)}{\varphi(z)} = z\frac{d}{dz}\log\varphi(z) = 1 + (|L_1| - |L_0|)z^4 + \ldots \tag{6.6}$$

Tenim $\varphi(z) = z(1 + cz^4 + \ldots)$. A més, $(\varphi'(z))^2 = 1 - \varphi^4(z)$. Per tant,

$$(1 + 5cz^4 + \ldots) = 1 - z^4(1 + cz^4 + \ldots)^4$$

d'on es dedueix que $c = -\frac{1}{10}$. Se segueix doncs que

$$z\frac{\varphi'(z)}{\varphi(z)} = 1 + 4cz^4 + \ldots = 1 - \frac{2}{5}z^4 + \ldots \tag{6.7}$$

Comparant (6.6) amb (6.7) deduïm que $|L_1| - |L_0| = -\frac{2}{5}$. Com que $|L_1| = -5\,|L_0|$ arribem a la conclusió que $|L_0| = \frac{1}{15}$, que és el que volíem veure.

Acabem de provar que $\sum_{\gamma\in\mathbb{Z}[i]-0} \frac{1}{\gamma^4} = \frac{\omega^4}{15}$. Més en general, **Hurwitz** demostra que

$$\sum_{\gamma\in\mathbb{Z}[i]-0} \frac{1}{\gamma^{4n}} = \frac{(2\omega)^{4n}}{(4n)!}E_n \ ,$$

on els E_n són nombres racionals (cf. [Hur]). Pels càlculs anteriors deduïm que $E_1 = \frac{1}{10}$. Recordem que existeix un resultat anàleg en el cas del enters, que és el següent:

$$\sum_{n\in\mathbb{Z}-0} \frac{1}{n^{2k}} = (-1)^{k-1}\frac{(\pi)^{2k}}{(2k)!}B_{2k} \ ,$$

on els B_{2k} són també nombres racionals, i reben el nom de *nombres de Bernoulli*. **Hurwitz** va ser també el primer en demostrar que els nombres E_n satisfacien propietats anàlogues als nombres de Bernoulli, i per això els E_n reben el nom de *nombres de Hurwitz.*

6.2 Polinomis lemniscàtics

En aquest apartat estudiem els *polinomis* de N-divisió de la lemniscata per tal de trobar de forma efectiva els punts que formen el N-àgon lemniscàtic, i poder procedir així a la seva construcció amb regla i compàs. Sabem que aquests punts són aquells que compleixen que l'arc comprès entre ells i l'origen és igual a $\alpha = \frac{2k\omega}{N}$ per $k = 0, \ldots, N-1$. Per a construir aquests punts és suficient trobar els segments $r = \varphi(\alpha)$, ja que per a la construcció efectiva suposem que tenim dibuixada la lemniscata. Com que $N\alpha = 2k\omega$, se segueix que $\varphi(N\alpha) = 0$. El teorema d'addició de la funció φ ens permet expressar algebraicament $\varphi(N\alpha)$ en funció de $\varphi(\alpha)$. Per tant,

per trobar els punts de N-divisió haurem de resoldre l'equació $\varphi(N\alpha) = 0$. Suposem, però, que volem dividir un pètal de lemniscata. Hauríem de trobar els punts tals que $\alpha = \frac{k\omega}{N}$ per $k = 0, \ldots, N-1$, és a dir, seran solució de $\varphi(N\alpha) = \varphi(k\omega) = 0$. Per tant, en solucionar l'equació de la divisió de la lemniscata en N parts iguals també podrem trobar els punts de $2N$-divisió.

Utilitzant la llei d'addició de φ, s'obté la següent expressió per $\varphi(2\alpha)$:

$$\varphi(2\alpha) = \frac{2\varphi(\alpha)\varphi'(\alpha)}{1+\varphi^4(\alpha)} = \frac{2\varphi\sqrt{1-\varphi^4}}{1+\varphi^4} \ . \tag{6.8}$$

Sabem que les solucions de $\varphi(2\alpha) = 0$, o sigui les solucions de $\varphi\sqrt{1-\varphi^4} = 0$, són els punts de 2-divisió de la lemniscata. Les solucions reals seran $\varphi = 0, 1, -1$. La solució $\varphi = 0$ correspon a dividir la lemniscata en 2 parts, fet que es pot deduir trivialment. Les altres solucions ens donen els punts de 4-divisió.

La relació

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

es dedueix aplicant la llei d'addició de la funció φ. A partir d'aquesta expressió trobem la següent fórmula recursiva per a calcular $\varphi(N\alpha)$:

$$\varphi(N\alpha) = \begin{cases} \dfrac{2\varphi((n+1)\alpha)\sqrt{1-\varphi^4(n\alpha)}}{1\varphi^2((n+1)\alpha)\varphi^2(n\alpha)} - \varphi(\alpha) \ , & N = 2n+1 \\ \dfrac{2\varphi(n\alpha)\sqrt{1-\varphi^4(n\alpha)}}{1+\varphi^4(n\alpha)} \ , & N = 2n \ . \end{cases}$$

Un cop tenim calculat $\varphi(N\alpha)$ en funció de $\varphi(\alpha)$ haurem de solucionar l'equació $\varphi(N\alpha) = 0$. Per això només cal estudiar el numerador de $\varphi(N\alpha)$. Així, a continuació fem una llista amb els numeradors de $\varphi(N\alpha)$ per $N = 3, \ldots, 9$, on els càlculs han estat realitzats amb `Maple V`.

Les arrels reals amb valor absolut menor que 1 dels polinomis anteriors es corresponen amb els paràmetres dels punts de N-divisió. A continuació llistem les arrels que compleixen aquesta condició per $N = 3, 5, 6, 8$.

$$N = 3$$
$$0\ ,\ \sqrt[4]{-3+2\sqrt{3}}\ ,\ -\sqrt[4]{-3+2\sqrt{3}}$$

$$N = 5$$
$$0\ ,\ \sqrt[4]{-13+6\sqrt{5}+2\sqrt{85-38\sqrt{5}}}\ ,\ -\sqrt[4]{-13+6\sqrt{5}+2\sqrt{85-38\sqrt{5}}}$$
$$\sqrt[4]{-13+6\sqrt{5}-2\sqrt{85-38\sqrt{5}}}\ ,\ -\sqrt[4]{-13+6\sqrt{5}-2\sqrt{85-38\sqrt{5}}}$$

$$N = 6$$
$$0\ ,\ \sqrt[4]{-3+2\sqrt{3}}\ ,\ -\sqrt[4]{-3+2\sqrt{3}}$$

$$N = 8$$
$$0\ ,\ 1\ ,\ -1\ ,\ \sqrt{\sqrt{2}-1}\ ,\ -\sqrt{\sqrt{2}-1}$$

6.3 Construccions efectives

Aquest apartat està dedicat a la construcció efectiva amb regla i compàs dels polígons regulars lemniscàtics de 3, 5, 6 i 8 costats. Per tal de no fer tediosa aquesta feina suposarem que tenim dibuixada la lemniscata, encara que el resultat d'Abel-Rosen es demostra sense admetre aquesta hipòtesi. En qualsevol cas, els nombres que construïm utilitzant la lemniscata són tots ells construïbles amb regla i compàs. Els valors $r = \varphi(\frac{2k\omega}{N})$ per $k = 0, \ldots, N-1$ són calculats a l'apèndix 2 d'aquest treball.

Per a totes les construccions partim doncs de la lemniscata i els eixos coordenats.

Construcció del triangle equilàter

Hem de construir el segment $\sqrt[4]{2\sqrt{3}-3}$. Considerem la següent construcció:

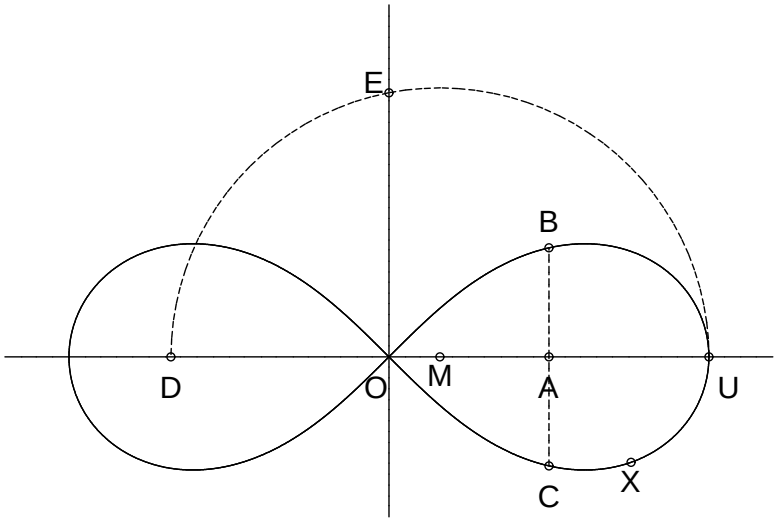

Figura 6.2: X és un vèrtex del triangle equilater lemniscàtic

(i) Construïm A el punt mig del segment unitat, és a dir, del segment OU.

(ii) Construïm la perpendicular a l'eix horitzontal per A i siguin B i C els punts de tall amb la lemniscata. Aleshores $\overline{BC} = \sqrt{2\sqrt{3}-3}$.

(iii) Construïm D tal que $\overline{OD} = \overline{BC}$.

(iv) Construïm M el punt mig del segment DU.

(v) Tracem la circumferència amb centre M i radi $\overline{MU}$. Sigui E el punt d'intersecció amb el semieix vertical positiu. Aleshores $\overline{OE} = \sqrt[4]{2\sqrt{3}-3}$.

(vi) Tracem la circumferència amb centre O i radi OE i sigui X el punt d'intersecció amb la lemniscata que es troba al quart quadrant. Tenim que l'arc $\widehat{OX} = \frac{2\omega}{3}$.

(vii) L'altre punt del 3-àgon és el punt d'intersecció de la circumferència anterior i la lemniscata situat al segon quadrant.

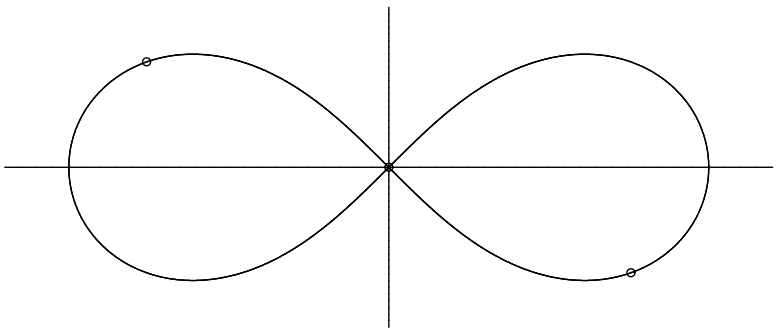

Figura 6.3: Triangle regular lemniscàtic

Construcció del pentàgon regular

Per a la construcció del pentàgon cal construir els segments

$$r_1 = \sqrt[4]{-13 + 6\sqrt{5} - 2\sqrt{85 - 38\sqrt{5}}}$$

$$r_2 = \sqrt[4]{-13 + 6\sqrt{5} + 2\sqrt{85 - 38\sqrt{5}}}\ .$$

Abans de procedir a la construcció establirem una sèrie d'igualtats que ens seran profitoses a l'hora de dur-la a terme. Es té

$$-13 + 6\sqrt{5} = (\sqrt{5} - 2)(4 - \sqrt{5}) \quad , \quad 85 - 38\sqrt{5} = \sqrt{5}(\sqrt{5} - 2)(9 - 4\sqrt{5})\ .$$

Utilitzant que $\sqrt{9 - 4\sqrt{5}} = \sqrt{5} - 2$ tenim la igualtat

$$\sqrt{85 - 38\sqrt{5}} = (\sqrt{5} - 2)\sqrt{\sqrt{5}(\sqrt{5} - 2)}\ .$$

Treient factor comú $\sqrt{5}-2$ trobem les següents expressions:

$$r_1 = \sqrt{\sqrt{\sqrt{5}-2}\sqrt{4-\sqrt{5}-2\sqrt{5-2\sqrt{5}}}}\,,$$

$$r_2 = \sqrt{\sqrt{\sqrt{5}-2}\sqrt{4-\sqrt{5}+2\sqrt{5-2\sqrt{5}}}}\,.$$

Farem la construcció en tres etapes:

1. Construcció del segment $\sqrt{4-\sqrt{5}-2\sqrt{5-2\sqrt{5}}}$.
2. Construcció del segment r_1.
3. Construcció del pentàgon regular lemniscàtic.

Etapa 1.

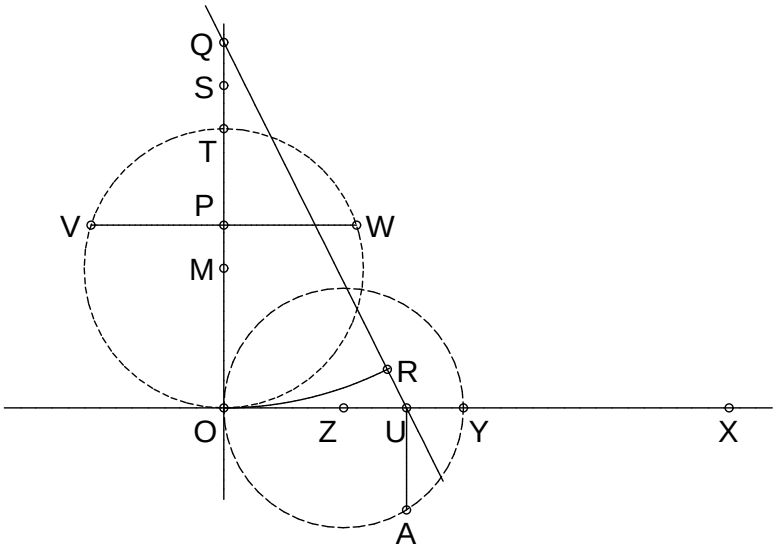

Figura 6.4: Construcció pentàgon lemniscàtic: Etapa 1.

(i) Sigui el segment unitat OU i construïm punts P i Q tals que $\overline{OU} = \overline{OP} = \overline{PQ}$, amb la qual cosa $\overline{QU} = \sqrt{5}$.

(ii) Tracem la circumferència amb centre Q i radi $\overline{OQ} = 2$ i obtenim el punt R. Es compleix $\overline{UR} = \sqrt{5} - 2$.

(iii) Construïm S tal que $\overline{QS} = \overline{UR}$. Així $\overline{OS} = 4 - \sqrt{5}$.

(iv) Construïm T tal que $\overline{ST} = \overline{UR}$. Tenim $\overline{OT} = 5 - 2\sqrt{5}$.

(v) Construïm M el punt mig de OT.

(vi) Tracem la circumferència de centre M i radi OM.

(vii) Construïm la perpendicular a l'eix vertical per P i obtenim els punts V i W, que compleixen $\overline{VW} = 2\sqrt{5 - 2\sqrt{5}}$.

(viii) Construïm X sobre l'eix horitzontal tal que $\overline{UX} = \overline{OS} = 4 - \sqrt{5}$.

(ix) Construïm X sobre l'eix horitzontal tal que $\overline{XY} = \overline{VW}$. Així, $\overline{UY} = 4 - \sqrt{5} - 2\sqrt{5 - 2\sqrt{5}}$.

(x) Construïm Z el punt mig del segment OY.

(xi) Tracem la circumferència amb centre Z i radi $\overline{OZ}$.

(xii) Tracem la perpendicular a l'eix vertical pel punt U, i obtenim el punt A com a intersecció d'aquesta recta i la circumferència anterior, amb la qual cosa $\overline{UA} = \sqrt{4 - \sqrt{5} - 2\sqrt{5 - 2\sqrt{5}}}$.

Notem que en aquesta etapa també podem construir el segment

$$\sqrt{4 - \sqrt{5} + 2\sqrt{5 - 2\sqrt{5}}}$$

modificant el pas (ix).

Etapa 2.

(i) Tracem la circumferència amb centre O i radi unitat i obtenim el punt P sobre l'eix vertical. Aleshores $\overline{UP} = \sqrt{2}$.

(ii) Tracem la circumferència amb centre U i radi UP, amb la qual cosa obtenim el punt Q d'intersecció amb la lemniscata. Aleshores $\overline{OQ} = \sqrt{\sqrt{5} - 2}$.

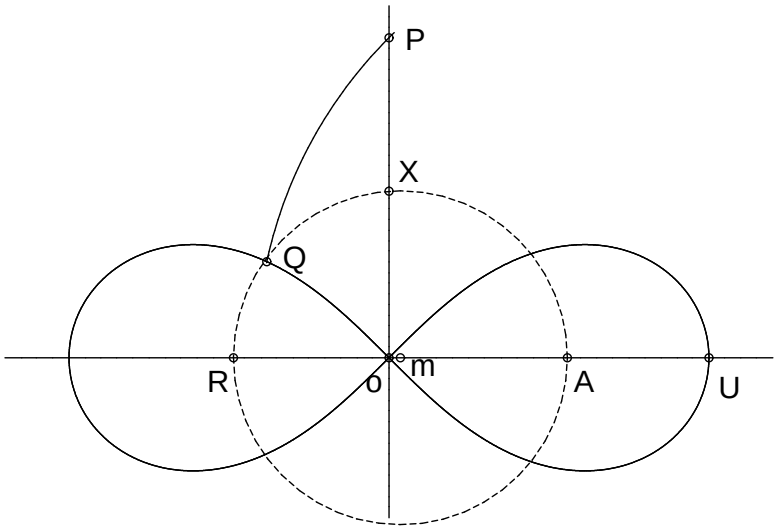

Figura 6.5: Construcció pentàgon lemniscàtic: Etapa 2.

(iii) Construïm R sobre l'eix horitzontal tal que $\overline{OR} = \overline{OQ}$.

(iv) Construïm A sobre l'eix horitzontal tal que $\overline{OA} = \sqrt{4 - \sqrt{5} - 2\sqrt{5 - 2\sqrt{5}}}$, on aquest últim segment l'hem construït al pas 1.

(v) Construïm m el punt mig del segment AR.

(vi) Construïm la circumferència de centre m i radi $\overline{mR}$ i trobem X com a intersecció d'aquesta circumferència i l'eix vertical. Es té $\overline{OX} = \sqrt{\overline{OR} \cdot \overline{OA}} = r_1$.

Repetint l'etapa 2 amb el segment $\sqrt{4 - \sqrt{5} + 2\sqrt{5 - 2\sqrt{5}}}$ obtenim el segment r_2.

Etapa 3.

(i) Construïm la circumferència de centre O i radi r_1. Siguin B i C els punts d'intersecció d'aquesta circumferència i la lemniscata que es troben, respectivament, als quadrants quart i segon.

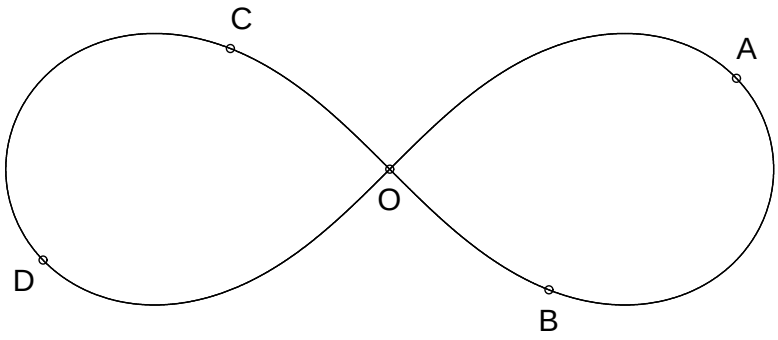

Figura 6.6: Pentàgon regular lemniscàtic.

(ii) Construïm la circumferència de centre O i radi r_2. Siguin A i D els punts d'intersecció d'aquesta circumferència i la lemniscata que es troben, respectivament, als quadrants primer i tercer. Aleshores es compleix que la longitud dels arcs $\widehat{OA}$, $\widehat{AB}$, $\widehat{BC}$,$\widehat{CD}$ i $\widehat{DO}$ és $\frac{2\omega}{5}$.

Construcció de l'hexàgon regular lemniscàtic

L'hexàgon lemniscàtic l'obtenim intersecant la lemniscata amb la circumferència de centre O i radi $\sqrt[4]{2\sqrt{3}-3}$, i aquest segment ja el vam obtenir en construir el 3-àgon lemniscàtic.

Construcció de l'octàgon regular lemniscàtic

Hem de construir els segments 1,-1, $\sqrt{\sqrt{2}-1}$ i $-\sqrt{\sqrt{2}-1}$. Així, només hem de saber com construir el segment $\sqrt{\sqrt{2}-1}$.

(i) Tracem la circumferència amb centre O i radi $\overline{OU}$ i sigui A el punt d'intersecció amb el semieix vertical positiu. Aleshores $\overline{AU} = \sqrt{2}$.

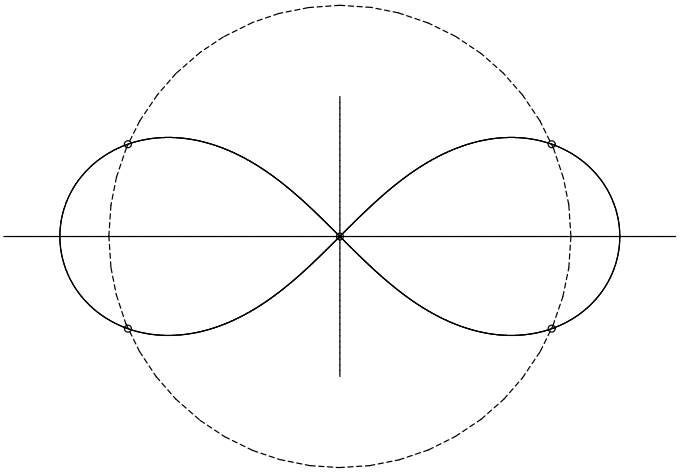

Figura 6.7: Hexàgon lemniscàtic.

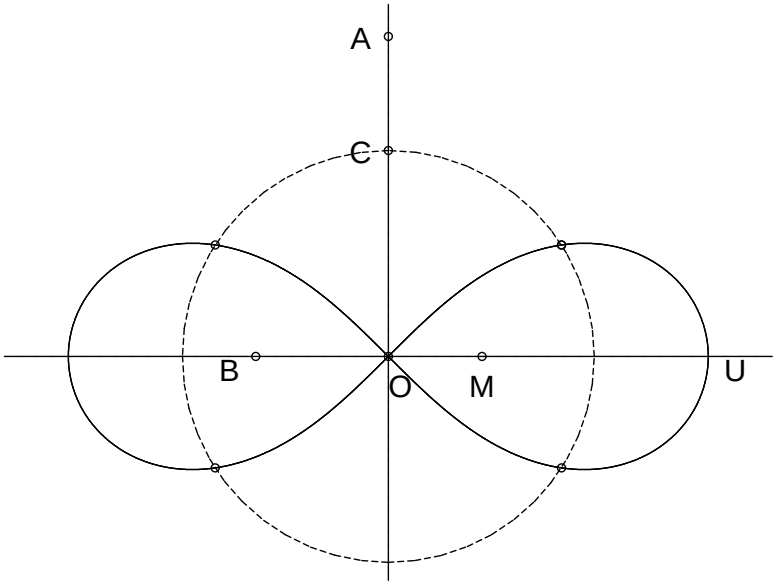

Figura 6.8: Construcció de l'octàgon lemniscàtic.

(ii) Construïm B sobre l'eix horitzontal tal que $\overline{BU} = \overline{AU}$.

(iii) Construïm M el punt mig del segment BU.

(iv) Tracem la circumferència amb centre M i radi $\overline{MU}$. El punt d'intersecció C amb l'eix vertical és tal que $\overline{OC} = \sqrt{\sqrt{2} - 1}$.

(v) Construïm la circumferència amb centre O i radi $\overline{OC}$. Aleshores els punts d'intersecció amb la lemniscata són vèrtexs del 8-àgon lemniscàtic.

Afegint els punts $(1, 0)$ i $(-1, 0)$ acabem de construir el 8-àgon lemniscàtic.

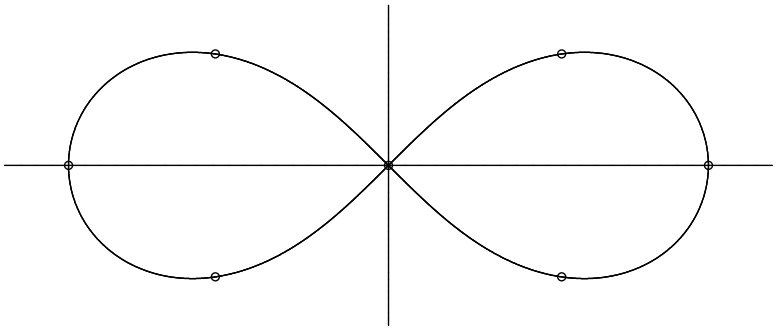

Figura 6.9: Octàgon regular lemniscàtic.

$N=3$	$\varphi(-3+\varphi^8+6\,\varphi^4)$
$N=4$	$4\,\varphi\sqrt{1-\varphi^4}\,(1+\varphi^4)\,(\varphi^8-6\,\varphi^4+1)$
$N=5$	$\varphi(\varphi^8-2\,\varphi^4+5)\,(\varphi^{16}+52\,\varphi^{12}-26\,\varphi^8-12\,\varphi^4+1)$
$N=6$	$2\,\sqrt{1-\varphi^4}\,\varphi(-1-6\,\varphi^4+3\,\varphi^8)$ $(\varphi^{16}-28\,\varphi^{12}+6\,\varphi^8-28\,\varphi^4+1)(-3+\varphi^8+6\,\varphi^4)$
$N=7$	$\varphi(-7+308\,\varphi^4+2954\,\varphi^8-19852\,\varphi^{12}+35231\,\varphi^{16}$ $-82264\,\varphi^{20}+111916\,\varphi^{24}-42168\,\varphi^{28}-15673\,\varphi^{32}$ $+14756\,\varphi^{36}-1302\,\varphi^{40}+196\,\varphi^{44}+\varphi^{48})$
$N=8$	$8\varphi\sqrt{1-\varphi^4}\,(1+\varphi^4)\,(\varphi^8-6\,\varphi^4+1)$ $(1+20\,\varphi^4-26\,\varphi^8+20\,\varphi^{12}+\varphi^{16})$ $(\varphi^{32}-88\,\varphi^{28}+92\,\varphi^{24}-872\,\varphi^{20}+1990\,\varphi^{16}$ $-872\,\varphi^{12}+92\,\varphi^8-88\,\varphi^4+1)$
$N=9$	$\varphi(-3+\varphi^8+6\,\varphi^4)(\varphi^{72}+534\,\varphi^{68}-10923\,\varphi^{64}+342864\,\varphi^{60}$ $-2304684\,\varphi^{56}+7820712\,\varphi^{52}-13729068\,\varphi^{48}+22321584\,\varphi^{44}$ $-39775986\,\varphi^{40}+44431044\,\varphi^{36}-19899882\,\varphi^{32}-3546576\,\varphi^{28}$ $+8458020\,\varphi^{24}-4009176\,\varphi^{20}+273348\,\varphi^{16}$ $-121392\,\varphi^{12}+11385\,\varphi^8+342\,\varphi^4-3)$

Taula 6.1: Polinomis lemniscàtics N=3,...,9

Apèndix A

Problemes oberts

Sabem que només és possible construir amb regla i compàs els polígons regulars de costats $N = 2^n p_1 \cdots p_r$, on els p_i són primers de Fermat diferents dos a dos. Existeix, però, un mètode aproximat per a construir qualsevol polígon regular sobre la circumferència amb regla i compàs, que s'estudia a l'ensenyament elemental. Consisteix en el següent:

(i) Tracem una circumferència arbitrària i tracem també un diàmetre d'aquesta.

(ii) Dividim el diàmetre en N parts iguals, amb la qual cosa obtenim $N+1$ punts, que numerem ordenadament $P_0, \ldots, P_N$.

(iii) Tracem les circumferències amb centres P_0, P_N i radi $\overline{P_0P_N}$, que anomenem C_1 i C_2 respectivament.

(iv) Considerem A un dels punts d'intersecció de C_1 i C_2. Aleshores tracem la recta que uneix aquest punt i el punt P_1. Dels dos punts d'intersecció de la recta amb la circumferència original, només ens interessa el que està situat més lluny del punt A.

(v) Iterem el procés anterior passant de P_i a P_{i+2}.

(vi) Tornem a repetir el mateix amb l'altre punt d'intersecció de C_1 i C_2, i obtindrem d'aquesta manera N punts sobre la circumferència, que són els vèrtexs de la construcció aproximada amb regla i compàs del N-àgon regular.

A la figura 16 s'exemplifica aquesta construcció per al heptàgon regular.

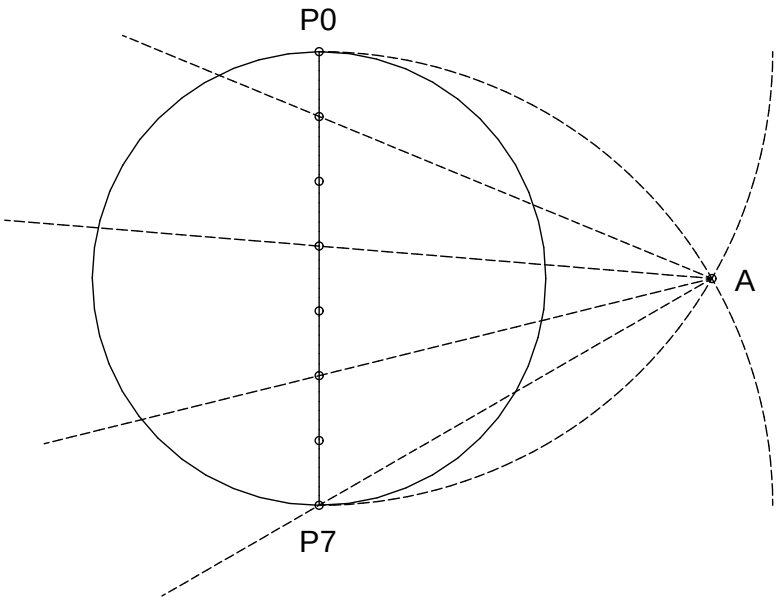

Figura A.1: Construcció aproximada del heptàgon regular.

Un problema que queda plantejat aleshores és el de trobar un mètode per a construir de forma aproximada el N-àgon regular lemniscàtic amb regla i compàs. A priori, no sabem si aquest problema té solució o no, però és un objectiu interessant trobar la contrapartida lemniscàtica al mètode descrit abans.

D'altra banda, a la demostració que s'ha explicat en aquest treball, s'ha pres la decisió de no fer ús de les interseccions de circumferències i rectes amb la lemniscata. Una altra qüestió que es pot plantejar, doncs, és esbrinar si es poden construir més polígons amb regla i compàs que els que afirma el teorema si no es considera aquesta restricció, ja que en aquest cas es poden obtenir irracionalitats no quadràtiques.

Un altre problema obert és el de donar un procediment senzill amb regla i compàs per a construir bisectruis sobre la lemniscata, és a dir, que donat un arc lemniscàtic poguem trobar el punt que el divideix en dos arcs de la mateixa longitud.