Universidad de La Laguna

SECCIÓN DE MATEMÁTICAS | FACULTAD DE CIENC

Alberto García Díaz

Teoría de Galois tras el origami

Por qué el origami resuelve los problemas geométricos clásicos de la Antigua Grecia.

Trabajo Fin de Grado
Grado en Matemáticas
La Laguna, Julio de 2017

Dirigido por

Dª. Evelia Rosa García Barroso

D^a. Evelia Rosa García Barroso
Departamento de Matemáticas, Estadística e Investigación Operativa
Universidad de La Laguna
38200 La Laguna, Tenerife

Agradecimientos

Este trabajo no habría sido posible sin la gran ayuda de los profesores y profesoras de la Facultad, en particular de mi Tutora, D^a Evelia Rosa García, por aceptar mi reto, tener mucha paciencia conmigo y enseñarme a redactar y mantener el orden y el control de mi Trabajo. También han contribuido a la causa D^a Mariví Reyes, D^a Margarita Rivero y D. Néstor Torrens, que me han enseñado, salvo lo tratado esencialmente en este trabajo, lo que académicamente he recibido de Álgebra en esta carrera.

Y finalmente, y no menos importante, a mi madre, mi fuente de inspiración en la superación de retos y que, sobre todas las cosas, me enseñó que quien trabaja duro y en una dirección, acaba recogiendo el mejor de los frutos.

Resumen · Abstract

Resumen

Los geómetras griegos ya eran capaces de hacer construcciones utilizando únicamente regla y compás, como bisecar un ángulo o construir determinados polígonos regulares. En cambio, no todas las construcciones eran posibles, como la trisección de un ángulo, la cuadratura del círculo o la duplicación del cubo.
Sin embargo, el origami permite realizar algunas de dichas construcciones imposibles con regla y compás. Desde el punto de vista matemático intervienen en tal hecho la Teoría de Galois y la Teoría de Grupos.
En esta memoria mostraremos la relación entre la Teoría de Galois y las construcciones con regla y compás, así como con el origami.

Palabras clave: *Teoría de Galois – Origami – Construcciones con Regla y Compás – Geometría – Extensiones de Cuerpos – Ecuaciones algebraicas*

Abstract

Ancient Greek geometricians were able to make constructions only using a straightedge and a compass, like bisecting an angle or building regular polygons. Nevertheless, not all constructions could be made as an angle trisection, the squaring of a circle or the cube duplication. Origami lets us making some of those imposible constructions with straightedge and compass. Galois Theory and Group Theory join in this mathematical fact.
This Degree thesis will show the relationship between Galois Theory and constructions with straightedge and compass, and also with origami.

Keywords: *Galois Theory – Origami – Straightedge and compass constructions – Geometry – Field extensions – Algebraic equations*

Contenido

Introducción

La teoría de Galois proporciona gracias al análisis de los elementos algebraicos, los anillos, cocientes, cuerpos y extensiones, conjuntamente a la teoría de Grupos, la determinación de qué ecuaciones algebraicas son resolubles mediante radicales.

Por otra parte, una aplicación clásica de esta teoría, como son las construcciones con regla y compás que propusieron los griegos, pueden ser generalizadas a construcciones con algo tan básico como los pliegues de papel.

La definición de los números origami-construibles y el establecimiento de operaciones con este conjunto dan explicación a dichas construcciones.

Para poder demostrar la relación que existe entre los números construibles con regla y compás y los números construibles con origami, buscaremos las claves en la Teoría de Galois, trabajando en el plano complejo y llegando a la conclusión de que ambos conjuntos son cuerpos, y que los números origami son una extensión del cuerpo de los números construibles con regla y compás.

Serán consecuencias de estos hechos la obtención de raíces cúbicas, cuartas y trisecciones de ángulos utilizando la papiroflexia, siendo alguna de ellas imposible de hacer con regla y compás. Por tanto, es de interés determinar un criterio, que será desarrollado durante el presente trabajo, que permita decidir qué construcciones pueden hacerse con las técnicas conocidas de origami, siempre teniendo como base la teoría que desarrolló el joven matemático Evariste Galois.

Rumbo del trabajo

Este trabajo comienza mostrando las definiciones y propiedades de la Teoría de Galois que el lector necesitará para seguir los resultados que se desarrollan en los capítulos posteriores. Por limitaciones de espacio se han omitido las demostraciones.

En el segundo capítulo se presentan los movimientos básicos o axiomas para construir números con regla y compás y se estudia la estructura algebraica de este subconjunto del plano complejo. Luego se presentan algunas propiedades de estos números y, a continuación, se establece un vínculo con las extensiones de cuerpos, donde se termina caracterizando el conjunto de los números construibles a través del grado de cierta extensión de cuerpos.

Finalmente, el tercer capítulo recrea el mismo esquema para los números origami-construibles: se establecen los axiomas, se estudia la estructura algebraica para este conjunto numérico y la relación entre los números construibles con regla y compás en los origami-construibles y se presenta una propiedad que diferencia a estos últimos de los primeros. Dicha propiedad será crucial para poder construir las soluciones de cualquier ecuación algebraica de grado no superior a cuatro, según nos indica la Teoría de Galois.

Recursos utilizados

Para la realización de este trabajo se ha contado con la bibliografía indicada al final de esta memoria, así como herramientas informáticas de realización de gráficos (Geogebra), además de algunos programas para la edición de figuras (Adobe Photoshop) y el uso de un editor de textos matemáticos (Texmaker) para poder redactar la memoria, el póster y la presentación, usando LaTeX.

1

Preliminares sobre Teoría de Galois

En este capítulo vamos a resumir esencialmente los conceptos sobre la Teoría de Galois que necesitaremos para desarrollar los capítulos posteriores. Se ha seguido principalmente el esquema de desarrollo de [1]. En dicha referencia se pueden consultar las demostraciones de los resultados que aquí, por limitaciones de espacio, no podemos presentar.

1.1. Cuerpos y sus extensiones

Definición 1.1. *Una* ***extensión de un cuerpo*** K *consiste en un cuerpo* L *y un homomorfismo de anillos* $\varphi : K \longrightarrow L$*. Identificaremos* K *con su imagen* $\varphi(K)$ *en* L*. De esta forma, escribiremos una extensión de cuerpos como* $K \subset L$*, o bien* $L : K$*, y diremos simplemente que* L ***es una extensión de*** K*.*

Definición 1.2. *Sea* L *una extensión de* K*, y sea* $\alpha \in L$*. Entonces,* α *es un* ***elemento algebraico*** *sobre* K *si existe un polinomio no constante* $f \in K[x]$ *tal que* $f(\alpha) = 0$*. Si* α *no es algebraico sobre* K*, se dice que* α *es un* ***elemento trascendente*** *sobre* K*.*

Lema 1.3. *Sea* $\alpha \in L$ *un elemento algebraico sobre* K*. Entonces hay un único polinomio no constante y mónico* $p \in K[x]$ *con las siguientes dos propiedades:*

(a) α *es raíz de* p*, es decir,* $p(\alpha) = 0$*.*
(b) Si $f \in K[x]$ *es un polinomio con* α *como raíz, entonces* p *divide a* f*, es decir,* f *es múltiplo de* p*.*

Definición 1.4. *Si* $\alpha \in L$ *es un elemento algebraico sobre* K*, se denomina* ***polinomio mínimo*** *de* α *sobre* K*, y se denota por* $Irr(\alpha, K)$*, al polinomio mónico, irreducible y único de menor grado que se anula en* α*.*

Definición 1.5. *Sean $L : K$ una extensión de cuerpos y $\alpha \in L$. Se denomina* ***conjunto de expresiones polinomiales*** *en α con coeficientes en K al conjunto:*

$$K[\alpha] = \{f(\alpha) = a_0 + a_1\alpha + ... + a_n\alpha^n : a_i \in K\}.$$

Lema 1.6. *El conjunto $K[\alpha]$ es dominio de integridad.*

Observación 1.7. Dado un dominio de integridad A, vamos a definir el *conjunto de fracciones*. Para ello, acudimos a la relación binaria en $A \times A \setminus \{0\}$:

$$(a, b) \sim (c, d) \Longleftrightarrow ad = bc.$$

Esta relación es de equivalencia:

- $\sim$ es reflexiva, pues, como A es conmutativo y $ab = ba$, y esto es equivalente a que $(a, b) \sim (a, b)$.
- $\sim$ es simétrica: Si $(a, b) \sim (c, d)$, entonces $ad = bc$, y con esto, $cb = da$, lo que es equivalente a que $(c, d) \sim (a, b)$.
- $\sim$ es transitiva: Si $(a, b) \sim (c, d)$, entonces $ad = bc$, y si $(c, d) \sim (e, f)$, se da que $cf = de$. Por tanto, $adf = bcf = bde$, de donde $af = be$ y esto conlleva a que $(a, b) \sim (e, f)$

Entonces, la clase de un par es $\overline{(a, b)} = \{(c, d) \in A \times A \setminus \{0\} : ad = bc\}$, y por convenio, se denota por $\frac{a}{b}$.
Luego consideraremos el **conjunto de fracciones** de A como:

$$\mathcal{F}(A) = \left\{ \frac{a_1}{a_2} : a_1, a_2 \in A, a_2 \neq 0 \right\} = \left\{ a_1 a_2^{-1} : a_1, a_2 \in A \right\}.$$

El cuerpo de fracciones del dominio de integridad A tiene estructura algebraica de anillo con las operaciones

$$\text{Suma: } \frac{a_1}{a_2} + \frac{b_1}{b_2} = \frac{a_1 b_2 + a_2 b_1}{a_2 b_2} \qquad \text{y} \qquad \text{Producto: } \frac{a_1}{a_2} \cdot \frac{b_1}{b_2} = \frac{a_1 b_1}{a_2 b_2}.$$

Dado que A es dominio de integridad, $a_2 b_2 \neq 0$, ya que $a_2 \neq 0 \neq b_2$. Además, el inverso multiplicativo de $\frac{a_1}{a_2} \neq 0$ es $\frac{a_2}{a_1}$. Luego $\mathcal{F}(A)$ es cuerpo, llamado **cuerpo de fracciones** del dominio de integridad A.

En lo sucesivo, denotaremos por $K(\alpha)$ al **cuerpo de fracciones** del dominio de integridad $K[\alpha]$.

Lema 1.8. *Si $L : K$ es extensión de cuerpos, entonces $K(\alpha)$ es el menor cuerpo que contiene a K y a α.*

Proposición 1.9. *Sea $L : K$ una extensión, $\alpha \in L$ un elemento algebraico y $p = Irr(\alpha,\ K)$ su polinomio mínimo. Entonces*

$$K[\alpha] \cong {}^{K[x]}/_{(p)},$$

siendo (p) el ideal generado en $K[x]$ por el polinomio p, esto es

$$(p) = \{p \cdot q : q \in K[x]\}.$$

Observación 1.10. Dado que $K[\alpha]$ es dominio de integridad, el ideal principal que genera $p = \mathrm{Irr}(\alpha,\ K)$ es ideal maximal, con lo que $K[\alpha]$ es un cuerpo.

Corolario 1.11. *Sean $L : K$ una extensión y $\alpha \in L$. Entonces, α es elemento algebraico sobre K si, y solo si, $K(\alpha) = K[\alpha]$.*

Podemos ver una extensión de cuerpos $L : K$ como un $K-$espacio vectorial con las leyes de composición interna y externa dadas por:

$$\begin{array}{lll} K \times K \longrightarrow & K & \qquad K \times L \longrightarrow & L \\ (k_1, k_2) \longrightarrow & k_1 + k_2 & \qquad (k, \alpha) \longrightarrow & k \cdot \alpha := i(k) \cdot \alpha, \end{array}$$

siendo $i(k) := k$ la identificación de K en L.

Con lo que ya podemos definir el grado de la extensión:

Definición 1.12. *Dada una extensión de cuerpos $L : K$, el **grado de la extensión** es la dimensión del $K-$espacio vectorial imagen:*

$$[L : K] := \dim_K(L).$$

*Diremos que la **extensión** es **finita** cuando $[L : K]$ sea finita.*

Proposición 1.13. *Sean $L : K$ una extensión y $\alpha \in L$. Entonces, α es elemento algebraico sobre K si, y solo si, $K(\alpha) : K$ es una extensión finita.*

Además, en este caso

$$[K(\alpha) : K] = n = \deg(Irr(\alpha,\ K)).$$

Análogamente al Lema 1.6, se tiene la siguiente proposición:

Proposición 1.14. *Sea $L : K$ es una extensión de cuerpos y $\alpha_1, ..., \alpha_n \in L$, entonces el **conjunto de expresiones polinomiales** en $\alpha_1, ..., \alpha_n$ con coeficientes en K es el dominio de integridad:*

$$K[\alpha_1, ..., \alpha_n] = \left\{ \sum a_{i_1 i_2 ... i_n} \alpha_1^{i_1} ... \alpha_n^{i_n} : a_{i_1 ... i_n} \in K \right\} \subseteq L.$$

*El **cuerpo de fracciones** de este dominio de integridad es:*

$$K(\alpha_1, ..., \alpha_n) = \left\{ \frac{\sum_i a_{i_1 ... i_n} \alpha_1^{i_1} ... \alpha_n^{i_n}}{\sum_j b_{j_1 ... j_n} \alpha_1^{j_1} ... \alpha_n^{j_n}} : a_{i_1 ... i_n}, b_{j_1 ... j_n} \in K \right\}.$$

Proposición 1.15. *Sean $[L : K]$ una extensión de cuerpos y $\alpha_1, ..., \alpha_n \in L$ elementos algebraicos sobre K. Entonces se tiene:*

1. $K[\alpha_1, \alpha_2] = K[\alpha_1][\alpha_2] = \left\{ \sum_j b_j \alpha_2^j : b_j \in K[\alpha_1] \right\}$,
   donde $b_j = \sum_j a_{1j} \alpha_1^{i_j}, \quad a_{1j} \in K$.
2. *Generalizando este principio:* $K[\alpha_1, ..., \alpha_{n-1}, \alpha_n] = K[\alpha_1, ..., \alpha_{n-1}][\alpha_n]$.
3. *Además:* $K(\alpha_1, ..., \alpha_n) = K(\alpha_1, ..., \alpha_{n-1})(\alpha_n)$.

Definición 1.16. *Sea $L : K$ una extensión de cuerpos. Una* ***torre de cuerpos*** *es una sucesión de extensiones de cuerpos de la forma*

$$K = K_0 \subset K_1 \subset K_2 \subset ... \subset K_{n-1} \subset K_n = L$$

donde $K_j : K_{j-1}$ es una extensión, para cada $1 \leq j \leq n$.

Teorema 1.17 (De la torre). *Supongamos que tenemos una torre de cuerpos $K \subset F \subset L$. Entonces $L : K$ es extensión finita si, y solo si, $L : F$ y $F : K$ son extensiones finitas.*
Además, en este caso:

$$[L : K] = [L : F] \cdot [F : K].$$

Son de interés las extensiones de cuerpos que están generadas por las raíces $n-$ésimas de la unidad.

Proposición 1.18. *Sea n un entero positivo y $\xi_n = e^{\frac{2\pi i}{n}}$ una raíz $n-$ésima de la unidad. Entonces, la extensión $[\mathbb{Q}(\xi_n) : \mathbb{Q}] = \phi(n)$, siendo ϕ la función de Euler.*

Proposición 1.19. *Sea $L : K$ una extensión de cuerpos con grado $[L : K] = 2$. Entonces existe $\alpha \in L$ tal que $L = K(\sqrt{\alpha})$. Recíprocamente, si $L = K(\sqrt{\alpha})$, siendo α libre de cuadrados perfectos, entonces $[L : K] = 2$.*

Definición 1.20. *Sea $L : K$ una extensión de cuerpos. Decimos que L es una* ***extensión separable*** *si para todo elemento algebraico $\alpha \in L$, su polinomio mínimo $f = Irr(\alpha, K)$ se puede factorizar como $f = a(x - \alpha_1)...(x - \alpha_n)$, donde $a \in K$ y $\alpha_i \in L, 1 \leq i \leq n$.*

Definición 1.21. *Sea $L : K$ extensión de cuerpos y $\alpha \in K$. Se dice que α es un* ***elemento primitivo*** *de L cuando $L = K(\alpha)$.*

Teorema 1.22 (Del elemento primitivo). *Sea $L : K$ una extensión de cuerpos finita y separable. Entonces existe $\alpha \in L$, no necesariamente único, tal que $L = K(\alpha)$.*

Definición 1.23. *Sea $f \in K[x]$ arbitrario con grado $\deg(f) > 0$ y $L : K$ una extensión de cuerpos. Diremos que L es* ***cuerpo de descomposición*** *de f sobre $K[x]$ si se cumplen las dos condiciones siguientes:*

(a) $f = a(x - \alpha_1)...(x - \alpha_n)$, donde $\alpha_1, ..., \alpha_n \in L$ y $a \in K$, y
(b) $L = K(\alpha_1, ..., \alpha_n)$.

Es decir, el cuerpo de descomposición es el menor de los cuerpos donde f se puede descomponer completamente en factores lineales.

Definición 1.24. *Sea $L : K$ una extensión de cuerpos. Diremos que L es una* ***extensión normal*** *de K, y lo denotaremos por $L \trianglelefteq K$, cuando cualquier polinomio irreducible de $K[x]$ que tenga raíces $\alpha, \beta \in \mathbb{C}$, cumple que si $\alpha \in L$, entonces también $\beta \in L$.*

Estas definiciones permiten caracterizar los cuerpos de descomposición de polinomios:

Proposición 1.25. *Sean $L : K$ una extensión de cuerpos y $f \in K[x]$ un polinomio. L es cuerpo de descomposición de f sobre K, si, y solo si, $L : K$ es una extensión normal y finita.*

Definición 1.26. *Sea $L : K$ una extensión finita de cuerpos. Se define el* ***grupo de Galois*** *de la extensión como*

$$Gal(L : K) := \{\sigma \in Aut(L) : \sigma(a) = a, \text{ para cada } a \in K\}.$$

Nótese que un automorfismo del grupo de Galois de $L : K$ es una aplicación $\sigma : L \longrightarrow L$ que deja fijos los elementos del cuerpo K.

Definición 1.27. *Sea $L : K$ una extensión de cuerpos. Decimos que L es una* ***extensión de Galois*** *cuando L es finita, normal y separable.*

Proposición 1.28. *Si $L : K$ es una extensión de Galois, entonces el orden del grupo de Galois coincide con el grado de la extensión:*

$$|Gal(L : K)| = [L : K].$$

Definición 1.29. *Sean $K \subset L \subset M$ una torre de cuerpos. Se dice que M es una* ***clausura de Galois*** *de L cuando M es la extensión mínima que hace que $M : K$ sea una extensión de Galois.*

Definición 1.30. *Un grupo finito G se dice que es* ***resoluble*** *si existe una cadena de subgrupos $\{1_G\} \subseteq G_0 \subseteq ... \subseteq G_n = G$ tales que $G_i \trianglelefteq G_{i+1}$ y G_{i+1}/G_i es abeliano.*

Teorema 1.31 (De Burnside). *Sea G un grupo finito con orden $|G| = p^a q^b$, donde p, q son primos y a, b son enteros positivos. Entonces G es un grupo resoluble.*

Definición 1.32. *Sea $L : K$ una extensión finita y $G = Gal(L : K)$. Se define el **cuerpo fijo** de L por H, y se denota por L_H al cuerpo*

$$L_H = \{\alpha \in L : \sigma(\alpha) = a, \text{ para cada } a \in H, \sigma \in Aut(L)\}.$$

Teorema 1.33 (De correspondencia de Galois). *Sea $L : K$ una extensión finita y de Galois, esto es, normal y separable, y denotemos $G = Gal(L : K)$. Entonces:*

1. *Si F es un cuerpo intermedio tal que $K \subset F \subset L$ y $H = Gal(L : F)$, entonces $L_H = F$. En este caso se tiene que $|H| = [L : F]$.*
2. *Si $H \leq G$ y $F = L_H$, entonces $Gal(L : L_H) = H$. Además, $[L_H : K] = \dfrac{|G|}{|H|}$.*

2

Construcciones geométricas

La idea de construcción geométrica utilizando regla y compás se remonta a los antiguos griegos. En estas construcciones, la regla no está graduada. Este capítulo será de utilidad para descubrir la conexión entre construcciones geométricas básicas utilizando estos dos elementos y la Teoría de Galois. Probaremos un primer vínculo entre las construcciones de la Grecia Clásica con regla y compás, y las extensiones de cuerpos. Estudiaremos también algunos ejemplos clásicos de la geometría griega, justificando por qué no es posible realizarlos, así como el trabajo de Gauss descrito en el décimo capítulo de [1] que involucra la construcción de polígonos regulares.

2.1. Números construibles

Un hecho importante al que vamos a recurrir en el desarrollo de estos contenidos es considerar el isomorfismo entre el plano real $\mathbb{R}^2$ y el plano complejo $\mathbb{C}$, y así hablaremos del punto $a + ib \in \mathbb{C}$ para referirnos a $(a, b) \in \mathbb{R}^2$.

Vamos a empezar definiendo el concepto de *construcción*. La idea básica es que empezamos con algunos puntos conocidos y desde estos puntos, usaremos la regla y el compás para construir rectas y circunferencias, siguiendo los siguientes axiomas:

C1. Dados dos puntos α y β distintos, podemos dibujar la recta ℓ que los une.
C2. Dados tres puntos α, β, γ, donde α y β son distintos, podemos trazar la circunferencia $\mathcal{C}$ con centro en γ y cuyo radio es la distancia de α a β.

En estas etiquetas, C indica *construcción*. Utilizando estas rectas y circunferencias no disjuntas, obtenemos nuevos puntos a partir de sus intersecciones:

P1. El punto de intersección de dos rectas distintas ℓ_1, ℓ_2 que se construyen según C1.

P2. Los puntos de intersección de una recta ℓ_1 y una circunferencia $\mathcal{C}_1$ construidas según C1 y C2.
P3. Los puntos de intersección de dos circunferencias distintas y no disjuntas $\mathcal{C}_1$ y $\mathcal{C}_2$ construídas según C2.

Aquí P en las etiquetas anteriores significa *punto*. Ahora consideraremos como conocidos estos nuevos puntos construidos. Entonces, aplicaremos C1, C2, P1, P2 y P3 a nuestra engrosada colección de puntos conocidos. Continuaremos este proceso hasta que la construcción se complete.

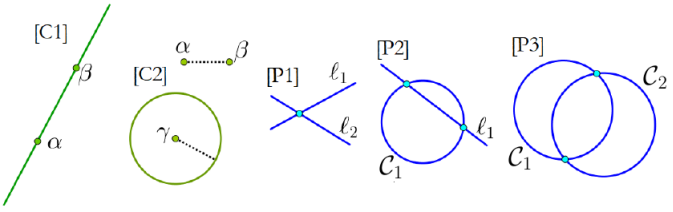


Figura 2.1. Construcciones para determinar todos los elementos construibles.

Nuestras construcciones comenzarán con los números 0 y 1. Esto motiva la siguiente definición.

Definición 2.1. *Un número complejo $\alpha \in \mathbb{C}$ es un* ***número construible con regla y compás*** *si existe una secuencia finita de construcciones con regla y compás que, empezando en 0 y 1, y utilizando* C1, C2, P1, P2 *y/o* P3, *terminan en α.*
El ***conjunto de los números construibles con regla y compás*** *se denota por*

$$\mathscr{C} = \{\alpha \in \mathbb{C} : \alpha \text{ es construible con regla y compás}\}.$$

2.1.1. Primeras construcciones con regla y compás

Comenzamos con algunas construcciones que se utilizarán en el establecimiento de los números construibles con regla y compás. La Figura 2.2 muestra dichas construcciones. Para ello será necesaria la siguiente propiedad que utilizaremos en la primera construcción.

Lema 2.2. *Dado un ángulo, existe un único movimiento que invierte sus lados. Este movimiento es la simetría axial respecto de la bisectriz.*

Demostración. Queda recogida en la lección 5ª de [9].

Bisección de un ángulo

Según ilustramos en la primera construcción de la Figura 2.2, tomemos dos semirrectas con vértices en un mismo punto O. Supongamos que ambas semirrectas determinan un ángulo no nulo. Al trazar una circunferencia $\mathcal{C}$ por O con radio $r > 0$, los puntos de intersección, según P2, los llamaremos A y B. Tomemos otro radio $r' > r$. De nuevo, sean las intersecciones $A' \in \overline{OA}$ y $B' \in \overline{OB}$. Por C1, llamaremos P a la intersección de $\overline{AB'}$ con $\overline{A'B}$.

En esta construcción hemos hallado el eje de simetría $\overline{OP}$ del movimiento que convierte $\overline{OA}$ en $\overline{OB'}$ y $\overline{OB}$ en $\overline{OA'}$. En virtud del Lema 2.2, $\overline{OP}$ es la bisectriz de $\widehat{AOB}$. Únicamente hay que justificar que la intersección $\overline{AB'}$ con $\overline{A'B}$ siempre es posible: supongamos que A es interior a $\overline{OB}$, esto es equivalente a que A' es interior a $\overline{OB'}$. Por tanto, B' es exterior a $\overline{OA'}$. Entonces, la recta $\overline{AB'}$ separa a los puntos O y B, pero no a los puntos O y A', con lo que necesariamente separa a $\overline{AB'}$, lo que conlleva a su intersección no vacía.

Construcción de la perpendicular a una recta por un punto de esta

Supongamos ahora una recta r y un punto $E \in r$ dados, según se indican en la segunda construcción de la Figura 2.2. Con radio arbitrario, trazamos una circunferencia con centro en E que corta a r en dos puntos, que llamaremos F y F'. Tomando como radio la distancia $\mathrm{dist}(F, F')$, trazamos dos circunferencias con centro en sendos puntos. La intersección de estas nuevas circunferencias son dos puntos, G y H, que están alineados con E, obteniéndose así la perpendicular buscada.

Aplicando el razonamiento de la construcción de la bisectriz, la inversión que convierte el segmento $\overline{EF}$ en $\overline{EF'}$ es una simetría axial con eje $\overline{GH}$, que se convierte en la bisectriz del ángulo llano $\widehat{FEF'}$, siendo E punto doble en la inversión, por lo que E está en la bisectriz.

Cuando el punto E es el punto medio de un segmento de recta, la perpendicular construida sobre dicho punto se denomina *mediatriz*.

Construcción de la perpendicular a una recta por un punto exterior

Tal como se indica en la tercera construcción de la Figura 2.2, sea s una recta y J un punto exterior a s. Elegimos dos puntos arbitrarios $K, K' \in s$. Trazamos las circunferencias con centros en K y K' que pasan por J. La intersección de estas nuevas circunferencias serán, por tanto, J y un nuevo punto, indicado por L en la Figura 2.2. Entonces, la perpendicular buscada es la recta $\overline{JL}$.

Nótese que el punto J es simétrico a L respecto a la recta s. Por tanto, s es bisectriz del ángulo $\widehat{JKL}$. Luego $\overline{JK}$ es simétrico de $\overline{KL}$, y con esto $\overline{JL}$ es perpendicular a s.

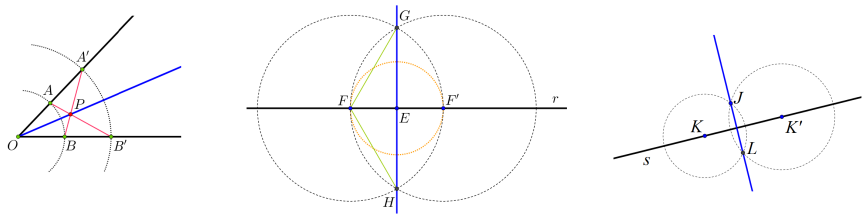


Figura 2.2. Construcciones de la bisectriz de un ángulo dado, la perpendicular a una recta por un punto de la recta y la perpendicular a una recta por un punto exterior a ésta.

Construcción de la recta paralela a otra recta dada por un punto exterior

Supongamos que tenemos la recta r y un punto b exterior a r. Sean $a \in r$ un punto arbitrario y d la distancia de a a b, que denotamos por $\mathrm{dist}(a, b)$. Trazamos la circunferencia con centro en a y radio d, en virtud de C2. Por P2, la intersección de la circunferencia con r son los puntos P y Q. Ahora tomamos $d' = \mathrm{dist}(P, b)$, y trazamos las circunferencias con centros en P y Q y radio d'.

En virtud de P3, la intersección entre ambas circunferencias son dos puntos construibles. Llamaremos M al punto de intersección que queda en el mismo semiplano que b. Entonces, la recta ℓ es la recta que pasa por b, pasa por M y es paralela a r, es decir, la recta que buscábamos.

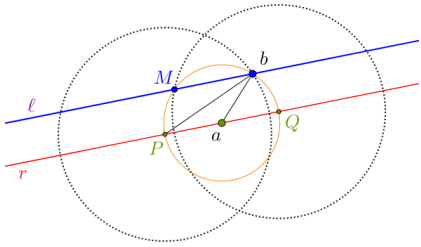


Figura 2.3. Construcción de la paralela a r por b.

Ejemplo 2.3. Presentamos algunos ejemplos de elementos construibles:

(a) El conjunto $\mathbb{Z}$ de los números enteros es construible.
De 0 y 1 obtenemos el eje OX utilizando C1 y la circunferencia de radio 1 centrada en 1 utilizando C2. Esta circunferencia interseca a OX en los puntos 0 y 2. Por P2, tenemos que 2 es construible. Iterando el procedimiento, *todos los números enteros son construibles.*

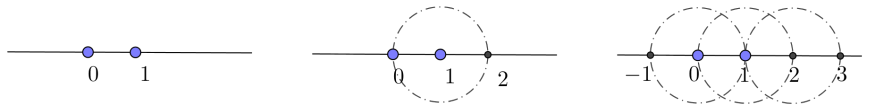


Figura 2.4. Construcción de $\mathbb{Z}$.

(b) El eje de ordenadas OY es construible.
La construcción de OY es equivalente a construir la perpendicular al eje OX por $x = 0$. En efecto, ya vimos en (a) que si $n \in \mathbb{Z}$, entonces n es construible. En particular, tomando $n = -1$ y $m = 1$ tenemos que OY es la mediatriz de la recta que une los puntos n y m. Si tomamos como radio $|m - n| = 2$, podemos trazar, según C2, las circunferencias con centros en m y n y radio 2. Sus intersecciones son construibles por P3, siendo ambos puntos del eje OY, que podemos trazar según C1 como la recta que une estos puntos ya construidos.

(c) La unidad imaginaria compleja, i, es construible.
Solo basta utilizar C2 para construir la circunferencia de radio 1 y centro 0. La intersección de dicha circunferencia con el eje OY construido en (b) son los puntos $\pm i$.

Estas construcciones nos serán muy útiles en lo sucesivo. Veamos ahora otro ejemplo:

Ejemplo 2.4. Un polígono regular es construible si, y solo si, puede construirse la raíz $n-$ésima de la unidad.

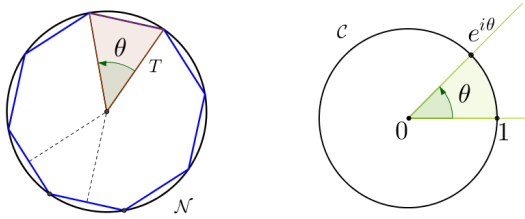


Figura 2.5. Construcción del ángulo central de un $n-$ágono regular (izquierda) y una raíz $n-$ésima de la unidad.

Supongamos que podemos construir un polígono regular de n lados (también denominado $n-$*ágono regular*) en algún lugar del plano. Utilizando dos vértices consecutivos y el centro del $n-$ágono regular, conseguimos el triángulo T de la Figura 2.5.

Nótese que el centro del $n-$ágono siempre es construible: tomando las mediatrices de dos lados cualesquiera, su intersección es exactamente el centro, y ellos determinan el ángulo central $\theta = \frac{2\pi}{n}$.

Esta situación es equivalente a considerar la circunferencia unidad $\mathcal{C}$ y al marcar θ se construye la raíz $n-$ésima de la unidad, $e^{i\theta} = e^{\frac{2\pi i}{n}}$, como puede observarse en la Figura 2.5.

Es importante recordar que el $n-$ágono puede estar girado y trasladado del origen, y que la circunferencia $\mathcal{N}$ circunscrita al $n-$ágono puede ser de radio no unitario. La traslación se hace de la siguiente manera: por un lado trazamos la circunferencia $\mathcal{C}$ de centro en 0 y radio 1 (por C2). Por otro lado, tomamos el centro del $n-$ágono y trazamos la circunferencia concéntrica de radio 1 (también por C2). En caso de que $\mathcal{N}$ tenga radio menor que 1, bastará con alargar los segmentos que unen el centro con los vértices del polígono (por C1). Medimos con el compás la distancia entre dos vértices consecutivos sobre la circunferencia concéntrica con $\mathcal{N}$ de radio 1 y trasladamos esta distancia a $\mathcal{C}$ (por P2). Hemos trazado una raíz $n-$ésima primitiva, ξ_n.

Este proceso puede ser revertido, es decir, si la raíz $n-$ésima de la unidad puede ser construida, entonces se puede construir el $n-$ágono regular.
En efecto, si podemos construir ξ_n sobre la circunferencia unidad $\mathcal{C}$ (construible), vamos haciendo circunferencias de radio $\text{dist}(1, \xi_n)$ y centros en las sucesivas potencias de ξ_n (construibles por C2) y haciendo las intersecciones de estas circunferencias con $\mathcal{C}$ (construibles por P3) vamos obteniendo los n vértices del $n-$ágono regular, que por tanto, es construible.

Por lo tanto, ξ_n *es construible si, y solo si, el* $n-$*ágono regular puede ser construido con regla y compás.* En la Sección 2.2 se determinarán los enteros positivos n de forma que el $n-$ágono regular sea construible.

A continuación presentaremos algunas propiedades algebraicas de los números construibles para, de forma constructiva, concluir que los números construibles son un cuerpo incluído en el plano complejo, y posteriormente demostraremos que la raíz cuadrada de un número construible es también construible. El primer resultado está muy relacionado con el aspecto vectorial de la suma de números complejos.

Proposición 2.5. $(\mathscr{C}, +)$ *es subgrupo de* $(\mathbb{C}, +)$.

Demostración. Dado $\alpha \in \mathscr{C} \setminus \{0\}$, podemos construir la recta que une 0 a α, según C1, y la circunferencia de radio la norma de α, $|\alpha|$, con centro en el origen, según C2. Entonces, las intersecciones de la recta y la circunferencia son los puntos $\pm\alpha$, con lo que $-\alpha$ es construible según P2.

Ahora supongamos que α y β son elementos construibles. Si α, β y 0 *no están alineados*, utilizando C2 dos veces podríamos construir la circunferencia de radio $|\alpha|$ con centro en β y la circunferencia con centro en α y radio $|\beta|$, según

se muestra en la construcción (A) de la Figura 2.6. Así tenemos que el punto de intersección de ambas circunferencias es $\alpha + \beta \in \mathscr{C}$, en virtud de P3.

Supongamos ahora que $0, \alpha, \beta$ *están alineados*. Dado que $0, \alpha \in \mathscr{C}$ podemos trazar por C1 la recta ℓ que une a 0 y α, y en particular, la ecuación de ℓ viene dada por $X = \lambda\alpha$, donde X es un punto arbitrario de ℓ y $\lambda \in \mathbb{R}$. Como $\beta \in \ell$ por hipótesis, $\beta = \lambda\alpha$, por lo que $\alpha + \beta = (\lambda + 1)\alpha$, lo que significa que $\alpha + \beta \in \ell$. Dado que $0 \in \mathscr{C}$ por definición, esto sigue que $\mathscr{C}$ es un subgrupo de $\mathbb{C}$ con la suma. □

Proposición 2.6. *Un elemento $\alpha = a + ib \in \mathbb{C}$ es construible si, y solo si, a y b son números reales construibles.*

Demostración. Sea $\alpha = a + ib \in \mathscr{C}$. Podemos trazar rectas perpendiculares a OX y OY por α de la misma forma que se construyó en la tercera ilustración de la Figura 2.2. Esto demuestra que $a, ib \in \mathscr{C}$. Como la circunferencia de centro 0 y radio $|ib| = |b|$ interseca al eje OX en b, entonces $b \in \mathscr{C}$ (según C2 y P2).

Recíprocamente, supongamos ahora que $a, b \in \mathbb{R} \cap \mathscr{C}$. Aplicamos C2 y P2 a la circunferencia de centro $0 \in \mathscr{C}$ y radio $|b|$, lo que muestra que su intersección con el eje OY, ib también es construible. Como los puntos $\alpha = a, \beta = ib$ son construibles, el punto $a + ib$ es también construible en virtud de la Proposición 2.5. □

Lema 2.7. *Sean a, b, con $a \neq 0$, elementos reales construibles. Entonces ab y $\frac{1}{a}$ también son elementos reales construibles.*

Demostración.
Tomemos, sin pérdida de generalidad, dos elementos $a, b \in \mathscr{C} \cap \{x \in \mathbb{R} : \ x > 0\}$. Esto podemos hacerlo porque 0 es construible, y si alguno o ambos valores, a o b, fueran negativos, la situación sería idéntica, en virtud de que $(\mathscr{C}, +)$ es grupo. Consideremos entonces la construcción (B.1) de la Figura 2.6. Recordamos que $i \in \mathscr{C}$ según lo comentado en el Ejemplo 2.3. En la construcción (B.1) de la Figura 2.6 se ha construido ib en virtud de la Proposición 2.6 y usado C1 para trazar la recta ℓ_1 que une i con a. Entonces podemos trazar la paralela a ℓ por ib, según se construyó la paralela en la Figura 2.3, y la llamaremos ℓ_2. Entonces, ℓ_2 corta al eje OX en el punto c. Pero $c = ab$, ya que los triángulos limitados por los ejes coordenados y las rectas ℓ_1 y ℓ_2, respectivamente, son semejantes. Con lo que $\frac{1}{a} = \frac{b}{c}$. Luego $c = ab \in \mathscr{C}$.
La construcción (B.2) de la Figura 2.6 construye $\frac{1}{a}$ cuando $a \in \mathscr{C}$. En efecto, trazamos los puntos construibles $1, i, ia$ y sea ℓ_1 la recta que une ia con 1, tenemos que la recta paralela ℓ_2 a ℓ_1 por i, que corta al eje de abscisas en un punto d. Así surgen los triángulos limitados por los ejes de coordenadas y las rectas ℓ_1 y ℓ_2, respectivamente. De nuevo, por semejanza, $\frac{1}{d} = \frac{ia}{i}$, luego $ad = 1$, de donde se concluye que $d = \frac{1}{a}$ es construible. □

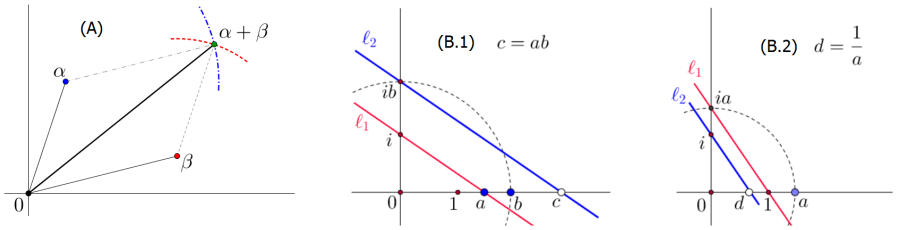


Figura 2.6. Construcciones de la suma de dos elementos construibles (A), el producto de dos elementos reales construibles (B.1) y el inverso de un elemento real construible no nulo (B.2).

Teorema 2.8. $(\mathscr{C},+,*)$ *es subcuerpo de* $(\mathbb{C},+,*)$.

Demostración. Vamos a comenzar la prueba demostrando que los números reales construibles, $\mathscr{C}\cap\mathbb{R}$, es un subcuerpo de $\mathbb{R}$.
El conjunto $\mathscr{C}\cap\mathbb{R}$ es cerrado para la suma, en virtud de la Proposición 2.5, y cerrado para el producto, según el Lema 2.7. Los elementos neutros de la suma y el producto son $0,1\in\mathscr{C}\cap\mathbb{R}$. Dado $a\in\mathscr{C}\cap\mathbb{R}\setminus\{0\}$, debemos demostrar la constructibilidad de su opuesto $-a$ y su inverso $\frac{1}{a}$. Sin pérdida de generalidad, porque el otro caso es análogo, tomaremos $a>0$. Construimos $-a$ aplicando C2 a la circunferencia de centro 0 y radio a. Como el eje OX es construible, la intersección de OX con dicha circunferencia son los puntos $\pm a$. Luego $-a\in\mathscr{C}\cap\mathbb{R}$. La construcción del inverso se demostró en el Lema 2.7. En definitiva, $\mathscr{C}\cap\mathbb{R}$ es subcuerpo de $\mathbb{R}$.

Para finalizar la prueba, demostraremos que el conjunto de números construibles (no necesariamente reales), $\mathscr{C}$, es subcuerpo de $\mathbb{C}$.
Para demostrar que $\mathscr{C}$ es cerrado respecto a la multiplicación y al cálculo de inversos de elementos no nulos, sean $\alpha=a+ib$ y $\beta=c+id$ números construibles. La Proposición 2.5 garantiza que $\mathscr{C}$ es subgrupo de $\mathbb{C}$ con la suma. Estudiamos el producto:

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

Dado que $a,b,c,d\in\mathscr{C}\cap\mathbb{R}$, y como $\mathscr{C}\cap\mathbb{R}$ es cuerpo, entonces $ac-bd, ad+bc\in\mathscr{C}\cap\mathbb{R}$.

De la Proposición 2.6 se tiene que $\alpha\beta\in\mathscr{C}$.

Además, cuando $\alpha\neq 0$, se tiene

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

De la Proposición 2.6 y del hecho que $\mathscr{C}\cap\mathbb{R}$ es subcuerpo de $\mathbb{R}$, se tiene de inmediato que $\frac{1}{\alpha}\in\mathscr{C}$ y concluimos que $\mathscr{C}$ es subcuerpo de $\mathbb{C}$. □

Corolario 2.9. $\mathbb{Q}$ *es construible.*

Demostración. Una fracción $\frac{p}{q} \in \mathbb{Q}$ podemos expresarla como $p \cdot \frac{1}{q}$, siendo $p, q \in \mathbb{Z}, q \neq 0$. Como el inverso de un número entero es construible, y el producto de dos números construibles es construible, se tiene que $\frac{p}{q} \in \mathscr{C}$.

Lema 2.10. *Sean A, B, C tres puntos de una circunferencia con centro en el punto O. El ángulo inscrito $\widehat{ABC}$ es la mitad del ángulo central $\widehat{AOC}$.*

Demostración. La prueba se llevará a cabo en tres fases, comenzando por una situación particular y la generalizaremos en las otras dos fases. Dichas fases se representan en la Figura 2.7.

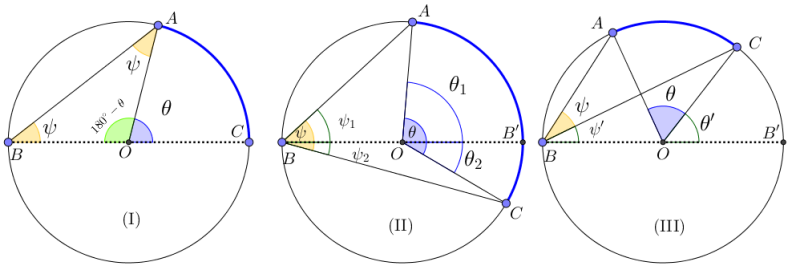


Figura 2.7. Esquema de los ángulos inscrito y central con los mismos puntos extremos.

Caso (I). Supongamos que B y C son diametralmente opuestos. Llamamos ψ al ángulo inscrito $\widehat{ABC}$ y θ al ángulo central $\widehat{AOC}$. El triángulo $\triangle AOB$ es isósceles, donde los ángulos idénticos son ψ y el tercero es suplementario a θ. Dado que la suma de ángulos es 180°, entonces $2\psi + (180° - \theta) = 180°$, de donde se concluye que $\theta = 2\psi$.

Caso (II). Supongamos ahora que A, B, C son puntos cualesquiera de la circunferencia con la única limitación de que el punto B', diametralmente opuesto a B, sea interior al arco $\widehat{AC}$. Denotamos ψ y θ igual que en la situación anterior. Al trazar el diámetro $\overline{BB'}$, los ángulos ψ y θ quedan divididos según las relaciones

$$\psi = \psi_1 + \psi_2, \ \theta = \theta_1 + \theta_2.$$

Como cada uno de los triángulos $\triangle BAB'$ y $\triangle BCB'$ tiene dos puntos sobre un diámetro de la circunferencia, se cumple la relación entre los ángulos inscrito y central (según se vió en la primera parte de la prueba). Por tanto: $\theta_1 = 2\psi_1$ y $\theta_2 = 2\psi_2$. Con lo que $\theta = \theta_1 + \theta_2 = 2(\psi_1 + \psi_2) = 2\psi$.

Caso (III). El último caso es el más general, donde supondremos que el punto diametralmente opuesto a B no está en el arco delimitado por A y C. Al

igual que en los otros dos casos, ψ y θ son los ángulos inscrito y central descritos en el enunciado. Al trazar el diámetro $\overline{BB'}$ aparecen nuevos ángulos ψ' y θ'. Por tanto, el ángulo $\widehat{CBB'}$ de nuevo tiene dos puntos sobre un diámetro de la circunferencia, con lo que $\theta' = 2\psi'$.

Pero el ángulo $\widehat{ABB'}$ también tiene dos de sus puntos sobre ese mismo diámetro de la circunferencia. Esto hace que $\theta + \theta' = 2(\psi + \psi') = 2\psi + 2\psi'$. Dado que $\theta' = 2\psi'$, entonces $\theta + 2\psi' = 2\psi + 2\psi'$, por lo que $\theta = 2\psi$. □

Proposición 2.11. *Sea α un elemento construible. Entonces $\sqrt{\alpha}$ también es construible.*

Demostración. Asumiremos que $\alpha \neq 0$. Si escribimos que $\alpha = re^{i\theta}, r = |\alpha| > 0$, entonces es suficiente demostrar que $\sqrt{r}\, e^{\frac{i\theta}{2}}$ es construible. Para ello, notamos que la construcción de α implica estos tres hechos:
En primer lugar, $\frac{\theta}{2} \in \mathscr{C}$, según se vio en la primera construcción de la Figura 2.2.
En segundo lugar, $r \in \mathscr{C}$, pues la circunferencia de centro 0 y radio $r = |\alpha|$, según C2, interseca a OX en $\pm r$.
Finalmente, si pudiéramos construir $\sqrt{r}$, entonces podríamos construir la circunferencia de centro 0 y de radio $\sqrt{r}$, según C2. Entonces, por P2, aplicado a esta circunferencia, y trasladando el ángulo $\frac{\theta}{2}$ sobre ella, habríamos construido $\sqrt{r}\, e^{\frac{i\theta}{2}}$. Vamos a construir $\sqrt{r}$. Sea $r > 0$ un número construible y definamos β según la Figura 2.8.

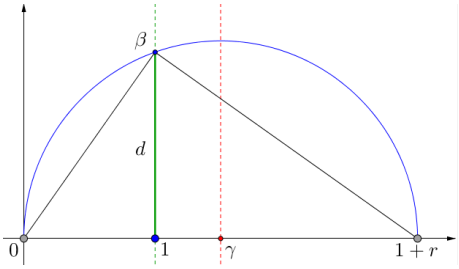


Figura 2.8. Construcción para $\sqrt{r} = \mathrm{dist}(1, \beta)$.

El punto β es construible, pues es la intersección de la mediatriz del segmento determinado por los puntos 0 y $r + 1$ trazada por el punto 1 (según la segunda construcción de la Figura 2.2) y la circunferencia con centro en γ, punto medio de dicho segmento. Nótese que $\gamma = \frac{1}{2}(1 + r) \in \mathscr{C}$. Construimos, por C2, la circunferencia centrada en γ y de radio $|\gamma|$. Nótese que en la Figura 2.8 mostramos la semicircunferencia de interés para la construcción.

En virtud del Lema 2.10, el triángulo de vértices $0, \beta, 1+r$ es rectángulo (por estar inscrito en una semicircunferencia, cuyo ángulo central mide 180°). Los dos triángulos menores que comparten el segmento de extremos 1 y β son semejantes, con lo que, si $d = \operatorname{dist}(1, \beta)$, entonces $\frac{1-0}{d} = \frac{d}{1+r-1}$, de donde $\frac{1}{d} = \frac{d}{r}$, o de forma equivalente $d^2 = r$. Por tanto, $d = \sqrt{r}$. En consecuencia, como d es construible, entonces $\sqrt{r}$ también lo es. □

Retomamos en el siguiente ejemplo la construcción de raíces primitivas.

Ejemplo 2.12. La raíz primitiva quinta de la unidad, $\xi_5 = e^{\frac{2\pi i}{5}}$, está dada según la fórmula

$$\xi_5 = \cos\left(\frac{2\pi}{5}\right) + i\,\operatorname{sen}\left(\frac{2\pi}{5}\right) = \frac{-1+\sqrt{5}}{4} + \frac{i}{2}\sqrt{\frac{5+\sqrt{5}}{2}}.$$

Dado que $\mathscr{C}$ es cerrado bajo la operación de tomar raíces cuadradas, se sigue que ξ_5 es construible, y aplicando el Ejemplo 2.4, se concluye que un pentágono regular puede construirse con regla y compás.

A continuación caracterizaremos los puntos construibles. Para ello necesitaremos demostrar algunos lemas previos.

Lema 2.13. *La recta construible mediante* C1 *admite una ecuación de la forma*

$$ax + by = c,$$

siendo sus coeficientes a, b, c reales construibles.

Demostración. Supongamos que $\alpha = (u_1, v_1), \beta = (u_2, v_2)$ son puntos construibles distintos. En virtud de la Proposición 2.6, $u_i, v_i \in \mathbb{R} \cap \mathscr{C}$. Dado que $\alpha \neq \beta$, entonces $u_2 - u_1$ y $v_2 - v_1$ no pueden anularse simultáneamente.
Supongamos en primer lugar que $u_2 - u_1 \neq 0$. Entonces $m = \frac{v_2 - v_1}{u_2 - u_1} \in \mathbb{R} \cap \mathscr{C}$, puesto que la diferencia y producto entre elementos construibles es construible, y el inverso de un elemento construible es construible.
Además, la ecuación de la recta del plano afín que pasa por α y tiene pendiente m es $y - v_1 = m(x - u_1)$, con lo que $y - v_1 = \frac{v_2 - v_1}{u_2 - u_1}(x - u_1)$, lo que nos lleva a $(u_2 - u_1)y + (v_1 - v_2)x = u_2 v_1 - u_1 v_2$. Luego, $a = u_2 - u_1, b = v_1 - v_2, c = u_2 v_1 - u_1 v_2$, son elementos reales y construibles.
Supongamos ahora que $u_1 = u_2$. Entonces los puntos α y β tienen las mismas coordenadas de abscisa, por lo que la recta que los une es de la forma $x = u_1$, luego una posible forma de escribir esta recta es tomando los coeficientes $a = 1, b = 0, c = u_1$, que también son todos elementos de $\mathbb{R} \cap \mathscr{C}$. □

Lema 2.14. *La circunferencia construible mediante* C2 *admite una ecuación de la forma*

$$x^2 + y^2 + ax + by + c = 0,$$

siendo sus coeficientes a, b, c reales construibles.

Demostración. La ecuación de una circunferencia en el plano, con centro en $P = (p_1, p_2)$ y radio $R > 0$, tiene ecuación

$$(x - p_1)^2 + (y - p_2)^2 = R^2.$$

Por otra parte, conviene recordar que una circunferencia construible mediante C2 precisa de la distancia entre dos puntos construibles, por ejemplo α y β, y el centro es también un punto construible. En nuestro caso, el centro será γ.

Escribiremos dichos puntos en forma binómica. Sean $\alpha = u_1 + iu_2, \beta = v_1 + iv_2, \gamma = w_1 + iw_2$, donde $u_i, v_i, w_i \in \mathbb{R}, i = 1, 2$. Dado que α, β, γ son elementos complejos construibles, entonces u_i, v_i, w_i son elementos reales construibles.

Se tiene que $R^2 = |\alpha - \beta|^2 = (u_1 - v_1)^2 + (u_2 - v_2)^2$.

Por tanto, tomando el centro γ y el radio calculado, tenemos:

$$(x - w_1)^2 + (y - w_2)^2 = (u_1 - v_1)^2 + (u_2 - v_2)^2,$$

es decir,

$$x^2 + y^2 - 2w_1x - 2w_2y + w_1^2 + w_2^2 - (u_1 - v_1)^2 - (u_2 - v_2)^2 = 0.$$

Luego tomando los números reales construibles $a = -2w_1, b = -2w_2, c = w_1^2 + w_2^2 - (u_1 - v_1)^2 - (u_2 - v_2)^2$, que son sumas, restas y productos de elementos reales construibles, y por tanto construibles, llegamos a la ecuación implícita de la circunferencia: $x^2 + y^2 + ax + by + c = 0$, como se pedía. □

Proposición 2.15. *Si dos rectas secantes y distintas ℓ_1 y ℓ_2 admiten ecuaciones con coeficientes construibles, entonces el punto de intersección de ambas es construible.*

Demostración. En virtud del Lema 2.13, las rectas ℓ_1 y ℓ_2 tienen ecuaciones

$$\ell_1 \equiv a_1x + b_1y = c_1, \quad \ell_2 \equiv a_2x + b_2y = c_2, \quad a_i, b_i, c_i \in \mathbb{R} \cap \mathscr{C}, i = 1, 2.$$

Dado que las rectas son secantes y distintas, existe un único punto de intersección α. Por lo tanto, las partes real e imaginaria de α determinan la única solución del sistema

$$\begin{cases} a_1x + b_1y = c_1 \\ a_2x + b_2y = c_2 \end{cases}.$$

Aplicando el Teorema de Rouché-Fröbenius, tenemos que la matriz $\begin{pmatrix} a_1 & b_1 \\ a_2 & b_2 \end{pmatrix}$ es invertible y la única solución del sistema es:

$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} a_1 & b_1 \\ a_2 & b_2 \end{pmatrix}^{-1} \begin{pmatrix} c_1 \\ c_2 \end{pmatrix}.$$

Las operaciones que realizamos para calcular la inversa de la matriz de coeficientes son sumas, inversos y productos de números construibles, que son, de nuevo, números construibles. De aquí se sigue inmediatamente que la parte real y la parte imaginaria de la solución α son elementos de $\mathbb{R} \cap \mathscr{C}$, con lo que α es construible. □

Proposición 2.16. *Si una recta ℓ y una circunferencia $\mathcal{C}$ admiten coeficientes construibles, entonces la intersección de ℓ y $\mathcal{C}$ también es construible.*

Demostración. Al igual que construimos las circunferencias y las rectas en el Lema 2.14 y la Proposición 2.15, supongamos que ℓ tiene ecuación

$$a_1 x + b_1 y = c_1, \quad a_1, b_1, c_1 \in \mathbb{R} \cap \mathscr{C}, \tag{2.1}$$

y que la circunferencia $\mathcal{C}$ tiene ecuación

$$x^2 + y^2 + a_2 x + b_2 y + c_2 = 0, \quad a_2, b_2, c_2 \in \mathbb{R} \cap \mathscr{C}. \tag{2.2}$$

Supongamos que $a_1 \neq 0$. Dividiendo (2.1) por a_1, y reetiquetando los coeficientes resultantes para ℓ obtenemos que $x + b_1 y = c_1$, lo cual es equivalente a que $x = -b_1 y + c_1$.
Sustituyendo esto en (2.2), tenemos $(-b_1 y + c_1)^2 + y^2 + a_2(-b_1 y + c_1) + b_2 y + c_2 = 0$.

Resolviendo en y obtenemos soluciones $\alpha_1, \alpha_2 \in \mathbb{C}$, mediante sumas, productos y cálculo de raíces cuadradas.

Dado que las sumas y productos de números construibles vuelven a ser construibles, y en virtud de la Proposición 2.11, las raíces cuadradas de números construibles son números construibles, queda demostrado que las partes real e imaginaria de las raíces α_1, α_2 son construibles, así como las propias raíces vistas como valores complejos.

Sólo faltaría analizar el caso en que $a_1 = 0$. Dado que ℓ es una recta del plano, $b_1 \neq 0$, su ecuación se reduce a $\ell \equiv b_1 y = c_1$, con lo que $y = \frac{c_1}{b_1} = k \in \mathbb{R} \cap \mathscr{C}$. Sustituyendo en la ecuación de la circunferencia $\mathcal{C}$, tenemos: $x^2 + k^2 + a_2 x + b_2 k + c_2 = 0$, de donde $x^2 + a_2 x + c_2 + k(k + b_2) = 0$.
Resolviendo en x obtenemos soluciones construibles. De nuevo las partes real e imaginaria de las raíces α_1, α_2 son construibles. Por tanto las intersecciones entre la recta ℓ y la circunferencia $\mathcal{C}$ son puntos construibles. □

Proposición 2.17. *Si dos circunferencias no disjuntas y distintas, $\mathcal{C}_1$ y $\mathcal{C}_2$, admiten ecuaciones con coeficientes construibles, entonces los puntos de intersección de ambas circunferencias también son construibles.*

Demostración. Según se estableció en el Lema 2.14, las ecuaciones de $\mathcal{C}_1$ y $\mathcal{C}_2$ son de la forma:

$$\begin{cases} x^2+y^2+a_1x+b_1y+c_1=0 \\ x^2+y^2+a_2x+b_2y+c_2=0 \end{cases}, \quad \text{donde} \quad a_1,a_2,b_1,b_2,c_1,c_2 \in \mathbb{R}\cap\mathscr{C}. \tag{2.3}$$

Si restamos las ecuaciones de (2.3) obtenemos:

$$(a_1-a_2)x+(b_1-b_2)y+(c_1-c_2)=0. \tag{2.4}$$

Nótese que si se anularan simultáneamente los coeficientes de x e y en (2.4), se tendría que $a_1=a_2$ y $b_1=b_2$, con lo que $\mathcal{C}_1$ y $\mathcal{C}_2$ serían circunferencias con el mismo centro (a_1,b_1) pero con distinto radio y, por tanto, disjuntas.
Entonces, la ecuación (2.4) define una recta.

Dado que ha de ser $(a_1,b_1)\neq(a_2,b_2)$, el sistema (2.3), es equivalente al sistema

$$\begin{cases} x^2+y^2+a_1x+b_1y+c_1=0 \\ (a_1-a_2)x+(b_1-b_2)y+(c_1-c_2)=0, \end{cases}$$

lo que resulta una reducción del problema al caso anterior (de intersección de recta y circunferencia), y en virtud de la Proposición 2.16, tiene soluciones construibles. □

Teorema 2.18. *Sea $\alpha\in\mathbb{C}$. Entonces $\alpha\in\mathscr{C}$ si, y solo si, existe una torre de cuerpos*

$$\mathbb{Q}=K_0\subset K_1\subset\cdots\subset K_{n-1}\subset K_n\subset\mathbb{C}$$

en donde $\alpha\in K_n$ y $[K_i:K_{i-1}]=2$, con $1\leq i\leq n$.

Demostración. Primero supondremos que tenemos una torre de cuerpos $\mathbb{Q}=K_0\subset\ldots K_n\subset\mathbb{C}$, donde $[K_i:K_{i-1}]=2$. Según la Proposición 1.19, $K_i=K_{i-1}(\sqrt{\alpha_i})$ para algún $\alpha_i\in K_{i-1}$. Demostraremos que $K_i\subset\mathscr{C}$ por inducción sobre i, cuando $0\leq i\leq n$.
Para el caso $i=0$, $K_0=\mathbb{Q}\subset\mathscr{C}$, ya que $\mathscr{C}$ es un subcuerpo de $\mathbb{C}$.

Nuestra hipótesis de inducción es que K_i es construible, para algún $\alpha_{i-1}\in K_{i-1}$, para cada $1\leq i-1\leq n-1$.

Sea ahora $\alpha_i\in K_{i-1}$ un elemento construible (pues $K_{i-1}\subset\mathscr{C}$). Dado que $\mathscr{C}$ es cerrado respecto de la raíz cuadrada, entonces $\sqrt{\alpha_i}\in\mathscr{C}$, por la Proposición 1.19. Por tanto, tomando $K_i=K_{i-1}(\sqrt{\alpha_i})\subset\mathscr{C}$, entonces $[K_i:K_{i-1}]=2$. Luego $K_n\subset\mathscr{C}$, ya que, en particular, cualquier $\alpha\in K_n$ es construible.

Recíprocamente, supongamos $\alpha\in\mathscr{C}$. Demostraremos que existe una torre de cuerpos $\mathbb{Q}=K_0\subset\cdots\subset K_n\subset\mathbb{C}$ con $[K_i:K_{i-1}]=2$ tal que K_n contiene las partes real e imaginaria de todos los números construidos durante el proceso de construcción de α. La demostración termina cuando las partes real e imaginaria de α están en K_n.
Para probar esto, lo haremos por inducción sobre el número N de veces que utilizaremos P1, P2 o P3 en la construcción de α.

Cuando $N = 0$, debemos tener que $\alpha = 0$ ó $\alpha = 1$, en cuyos casos, $K_n = K_0 = \mathbb{Q}$. Suponemos cierto que, tras $N - 1$ pasos de construcción, existe una torre de cuerpos $\mathbb{Q} = K_0 \subset \cdots \subset K_{N-1} \subset \mathbb{C}$ tal que $[K_i : K_{i-1}] = 2$ y que las partes real e imaginaria de α están en K_{N-1}.

Demostraremos el proceso para N pasos de construcción. Existen 3 posibilidades para la última construcción y obtención de α.

Caso 1: Supongamos que **el último paso de la construcción es P1** (intersección de dos rectas $\ell_1 \neq \ell_2$ construibles). En virtud de la Proposición 2.15, sólo involucra realizar sumas y productos de números construibles, por lo que $\alpha \in K_{n-1} \cap \mathscr{C}$.

Caso 2: Supongamos que **el último paso de la construcción es P2** (intersección de una recta ℓ y una circunferencia $\mathcal{C}$ construibles). En virtud de la Proposición 2.16, la determinación de las soluciones involucra realizar sumas y productos de números construibles, así como raíces cuadradas, por lo que $\alpha \in K_n \cap \mathscr{C}$, siendo $K_n = K_{n-1}(\sqrt{\alpha})$, y por tanto $[K_n : K_{n-1}] \leq 2$, ya que no descartamos que α sea un cuadrado perfecto.

Caso 3: Supongamos que **el último paso de la construcción es P3** (intersección de dos circunferencias $\mathcal{C}_1$ y $\mathcal{C}_2$ construibles). En virtud de la Proposición 2.17, se demuestra que es un caso reducible al Caso 2, lo cual termina la prueba. □

El Teorema 2.18 pone de manifiesto que el conjunto $\mathscr{C}$ de los números construibles con regla y compás es cerrado para la suma, el producto y la raíces cuadradas de uno cualquiera de sus elementos. Por tanto, surge la siguiente consecuencia.

Corolario 2.19. *$\mathscr{C}$ es el menor subcuerpo de $\mathbb{C}$ que es cerrado bajo la operación de extraer raíz cuadrada.*

Demostración. Sea K un subcuerpo de $\mathbb{C}$ cerrado bajo la operación de extraer raíz cuadrada, y supongamos $\alpha \in \mathscr{C}$. Por el Teorema 2.18, existe una torre de cuerpos $\mathbb{Q} = K_0 \subset \cdots \subset K_n \subset \mathbb{C}$ con $[K_i : K_{i-1}] = 2$ y $\alpha \in K_n$. En la primera parte del Teorema 2.18 se demuestra que $K_n \subset K$. Como $\alpha \in K_n \subset K$ y α es arbitrario, entonces $\mathscr{C} \subset K$, y con esto, $\mathscr{C}$ es un cuerpo minimal. □

El Teorema 2.18 también tiene una consecuencia muy útil en nuestro propósito de determinar qué elementos son construibles:

Corolario 2.20. *Si $\alpha \in \mathscr{C}$, entonces $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2^m$ para algún $m \geq 0$. Por tanto, cada número construible es algebraico sobre $\mathbb{Q}$, y el grado de su polinomio mínimo sobre $\mathbb{Q}$ es potencia de 2.*

Demostración. Si $\alpha \in \mathscr{C}$, en virtud del Teorema 2.18, obtenemos una torre de cuerpos $\mathbb{Q} = K_0 \subset \cdots \subset K_n \subset \mathbb{C}$ con $[K_i : K_{i-1}] = 2$ tal que $\alpha \in K_n$. Aplicando el Teorema 1.17, podemos calcular el grado de la extensión completa:

$$[K_n : \mathbb{Q}] = [K_n : K_0] = [K_n : K_{n-1}] \cdot \ldots \cdot [K_1 : K_0] = 2^n.$$

Por lo tanto, si tenemos $\mathbb{Q} \subset \mathbb{Q}(\alpha) \subset K_n$, usando el Teorema 1.17 otra vez, podemos concluir que $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ divide a $[K_n : \mathbb{Q}] = 2^n$. □

Alguno de los problemas más famosos de la Geometría Griega que no eran resolubles con regla y compás son la trisección del ángulo, la duplicación del cubo y la cuadratura del círculo. Utilizaremos el Corolario 2.20 para dar una justificación.

Ejemplo 2.21. Trisección de un ángulo.
Según la construcción descrita en la Figura 2.2, sabemos que un ángulo cualquiera puede ser bisecado utilizando regla y compás. Sin embargo, no ocurre lo mismo si queremos construir la trisección. Para ello, analizamos el siguiente contraejemplo.
El ángulo de 120° es construible, ya que si trazamos por $C2$ las circunferencias $\mathcal{C}_1, \mathcal{C}_2, \mathcal{C}_3$, todas con radio 1 y con centro en los puntos $0, -1$ y 1 respectivamente. Los puntos de intersección de dichas circunferencias, junto con los puntos -1 y 1 dividen a la circunferencia en 6 arcos iguales. Tomando dos arcos consecutivos, habremos abarcado el ángulo de 120°.
Supongamos que pudiéramos trisecar dicho ángulo. Esto implicaría la construcción de un ángulo de 40° usando regla y compás, o de forma equivalente, que la raíz novena de la unidad, $\xi_9 = e^{\frac{2\pi i}{9}}$ sería construible.

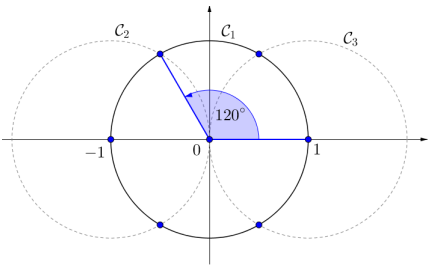


Figura 2.9. El ángulo de 120° es construible con regla y compás. En cambio, no puede trisecarse con estas herramientas.

Pero la raíz novena de la unidad es raíz del polinomio 9-ciclotómico, cuya factorización es

$$\Phi_9(x) = \frac{x^9 - 1}{\Phi_1(x)\Phi_3(x)} = \frac{x^9 - 1}{(x-1)(x^2+x+1)} = x^6 + x^3 + 1.$$

Por tanto, tenemos que $x^6 + x^3 + 1 = \mathrm{Irr}\,(\xi_9,\ \mathbb{Q})$, que es un polinomio de grado 6, y según hemos demostrado en el Corolario 2.20, un algebraico α es construible si, y solo si $\deg(\mathrm{Irr}\,(\alpha,\ \mathbb{Q})) = 2^m$, para algún m entero. Dado que $\mathrm{Irr}\,(\xi_9,\ \mathbb{Q})$ tiene grado $6 \neq 2^m$, entonces ξ_9 no es construible y, en consecuencia, no se puede trisecar un ángulo de 120° usando regla y compás.

Ejemplo 2.22. Duplicación del cubo.

En este problema clásico, se da un cubo y se pretende construir otro cubo con exactamente el doble de volumen del cubo dado. Podemos tomar nuestras unidades de medida, u, de manera que las aristas del cubo de partida sean $1 \cdot u$. En estas unidades, el volumen del cubo sería $1 \cdot u^3$. Necesitamos, por tanto, construir un cubo de volumen $2 \cdot u^3$, con lo que sería suficiente construir la longitud de arista $\alpha = \sqrt[3]{2} \cdot u$. Además, dado que la arista del cubo de partida tiene longitud $1 \cdot u$, podemos asumir que el cubo puede ser construido a partir de los puntos 0 y 1 del espacio euclídeo.

Demostrar que el cubo de doble volumen se reduce, por tanto, a probar que $\alpha = \sqrt[3]{2}$ es construible. Pero el polinomio mínimo de α sobre $\mathbb{Q}$, según se definió en la Definición 1.4, es $\mathrm{Irr}\left(\sqrt[3]{2},\ \mathbb{Q}\right) = x^3 - 2$, lo que implica que $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = \deg(x^3 - 2) = 3 \neq 2^n$, y, en virtud del Corolario 2.20, se tiene que la longitud α no es construible, y el cubo no se puede duplicar con regla y compás.

Ejemplo 2.23. Cuadratura del círculo.

En este problema se tratará de construir un cuadrado cuya área sea igual al de un círculo dado. Al igual que antes, podemos tomar unas unidades tales que el círculo de partida tenga radio $1 \cdot u$, y con esto, su área sea $\pi \cdot u^2$, con lo que nuestro cuadrado objetivo debe tener lado $\alpha = \sqrt{\pi} \cdot u$.

Partimos de un círculo de radio $1 \cdot u$. Podemos construirlo a partir de los puntos 0 y 1 del plano euclídeo, con lo que este círculo es construible con regla y compás. Probar que el cuadrado en cuestión es construible se reduce, por tanto, a demostrar que $\alpha = \sqrt{\pi}$ es construible.

Dado que $\mathscr{C}$ es un cuerpo, la constructibilidad de $\sqrt{\pi}$ implicaría que $\pi = \left(\sqrt{\pi}\right)^2$ es también construible. En virtud del Corolario 2.20, implicaría que π es un elemento algebraico sobre $\mathbb{Q}$. Pero en 1882, Lindemann (ver [8]) demostró que π es trascendente sobre $\mathbb{Q}$, lo que contradice la constructibilidad de π, y por tanto, la de $\sqrt{\pi}$ y la del cuadrado en cuestión.

Es natural preguntarse cuándo el recíproco del Corolario 2.20 es cierto, es decir, si $\alpha \in \mathbb{C}$ es un algebraico sobre $\mathbb{Q}$ y $\deg(\mathrm{Irr}\,(\alpha,\ \mathbb{Q})) = 2^n$ ¿es α construible? El siguiente resultado ayudará a dar una respuesta.

Teorema 2.24. *Sea $\alpha \in \mathbb{C}$ algebraico sobre $\mathbb{Q}$ y sea L el cuerpo de descomposición de Irr$(\alpha, \mathbb{Q})$. Entonces α es construible si, y solo si, $[L : \mathbb{Q}] = 2^m$ para algún $m \in \mathbb{Z}, m > 0$.*

Demostración. Primero supondremos que $[L : \mathbb{Q}] = 2^m$ para algún $m \in \mathbb{Z}^+$. En virtud del Teorema Fundamental del Álgebra, si $L : \mathbb{Q}$ es una extensión de Galois, se tiene que $|\mathrm{Gal}(L : \mathbb{Q})| = [L : \mathbb{Q}]$. Supongamos entonces que $|\mathrm{Gal}(L : \mathbb{Q})| = 2^m$. El grupo de Galois, $\mathrm{Gal}(L : \mathbb{Q})$, es resoluble, y con esto, tenemos un retículo de subgrupos normales

$$\{Id\} = G_m \trianglelefteq G_{m-1} \trianglelefteq \cdots \trianglelefteq G_1 \trianglelefteq G_0 = \mathrm{Gal}(L : \mathbb{Q}),$$

tales que el orden de cada uno con su anterior es $|G_i : G_{i-1}| = 2$ (ya que $|\mathrm{Gal}(L : \mathbb{Q})| = 2^m$). Con esto, tenemos la torre de cuerpos:

$$\mathbb{Q} = L_{G_0} \subset L_{G_1} \subset \cdots \subset L_{G_m} = L,$$

donde $[L_{G_i} : L_{G_{i-1}}] = 2, 1 \leq i \leq m$. En virtud del Teorema 2.18, tenemos que $\alpha \in L$ es construible.

Vamos a demostrar primero que $\mathscr{C} : \mathbb{Q}$ es una extensión normal. Para esto, tomaremos $\alpha \in \mathscr{C}$ y probaremos que $f = \mathrm{Irr}\,(\alpha, \mathbb{Q})$ se descompone completamente en $\mathscr{C}$. Como $\alpha \in \mathscr{C}$ es construible, el Teorema 2.18 demuestra la existencia de una torre de cuerpos $\mathbb{Q} = K_0 \subset \cdots \subset K_n \subset \mathbb{C}$ donde $[K_i : K_{i-1}] = 2$ con $\alpha \in K_n$. Entonces sea $M : \mathbb{Q}$ una clausura de Galois para $K_n : \mathbb{Q}$, es decir, la mínima extensión algebraica de K_n que hace que $M : \mathbb{Q}$ sea extensión de Galois, siendo $M \subset \mathbb{C}$.

Observamos que f se descompone completamente en M, dado que M es extensión normal sobre $\mathbb{Q}$, f es irreducible sobre $\mathbb{Q}$ y $\alpha \in K_n \subset M$ es una raíz de f.

Sea ahora $\beta \in M$ una raíz cualquiera de f. Existe $\sigma \in \mathrm{Gal}(M : \mathbb{Q})$ tal que $\sigma(\alpha) = \beta$. Aplicando σ a los cuerpos $\mathbb{Q} = K_0 \subset \cdots \subset K_n \subset M$, tenemos:

$$\mathbb{Q} = \sigma(\mathbb{Q}) = \sigma(K_0) \subset \cdots \subset \sigma(K_n),$$

tales que $[\sigma(K_i) : \sigma(K_{i-1})] = [K_i : K_{i-1}] = 2$, para cada $1 \leq i \leq m$. Por el Teorema 2.18, $\beta = \sigma(\alpha) \in \sigma(K_n)$ es construible. Esto demuestra que f se descompone completamente sobre $\mathscr{C}$, y $\mathscr{C} : \mathbb{Q}$ es extensión normal.

Dado que f se descompone completamente sobre $\mathscr{C}$, entonces $\mathscr{C}$ contiene un cuerpo de descomposición L de f sobre $\mathbb{Q}$. Según el Teorema del Elemento Primitivo (1.22), tenemos que $L = \mathbb{Q}(\gamma)$ para algún $\gamma \in L$. Puesto que $\gamma \in \mathscr{C}$, por el Corolario 2.20, esto implica que $[\mathbb{Q}(\gamma) : \mathbb{Q}] = [L : \mathbb{Q}] = 2^m$, como se pretendía demostrar. □

Usaremos el Teorema 2.24 para demostrar que el recíproco del Corolario 2.20 es falso en general, como se muestra en el siguiente ejemplo:

Ejemplo 2.25.

Sea α una raíz de $f = x^4 - 4x^2 + x + 1$. Para comprobar que f es irreducible sobre $\mathbb{Q}$, suponemos que puede descomponerse en dos polinomios $g, h \in K[x]$ mónicos y de segundo grado, tales que $f = gh$. Esto es, $x^4 - 4x^2 + x + 1 = (x^2 + ax + b)(x^2 + cx + d)$. Pero el sistema que resulta no tiene solución en $\mathbb{Z}$, luego f es irreducible. Por este motivo, determinamos que $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$. Sin embargo, el cuerpo de descomposición L de f sobre $\mathbb{Q}$ satisface que $[L : \mathbb{Q}] = 24$, lo que implica que, por el Teorema 2.24, $\alpha \notin \mathscr{C}$, ya que 24 no es una potencia de 2.

2.2. Polígonos regulares y raíces de la unidad

A continuación vamos a ocuparnos de construir los polígonos regulares, con lo que trabajaremos con las raíces $n-$ésimas de la unidad y las extensiones ciclotómicas.

Definición 2.26. *Un primo impar p es un **primo de Fermat** si puede ser escrito en la forma*

$$p = 2^{2^m} + 1, \quad \text{para algún } m \geq 0.$$

Gauss caracterizó los polígonos regulares como sigue:

Teorema 2.27. *Sea n un entero mayor que 2. Entonces un $n-$ágono regular puede ser construido con regla y compás si, y solo si,*

$$n = 2^s p_1 \dots p_r,$$

donde s es un entero positivo y $p_1, ..., p_r$ son $r \geq 0$ primos de Fermat distintos.

Demostración. Recordamos que en el Ejemplo 2.4 probamos que un $n-$ágono regular es construible con regla y compás si, y solo si, ξ_n es construible. Por otra parte, el Teorema 2.24 afirma que ξ_n es construible si, y solo si, $[\mathbb{Q}(\xi_n) : \mathbb{Q}] = 2^m$, para algún $m \in \mathbb{Z}^+$ y, además, en virtud de la Proposición 1.18, $[\mathbb{Q}(\xi_n) : \mathbb{Q}] = \varphi(n)$, donde φ es la función de Euler.

Concluimos por tanto que ξ_n es construible si, y solo si, $\varphi(n) = 2^m$, para algún $m \in \mathbb{Z}^+$. Demostremos ahora las dos implicaciones del Teorema.

Para probar que la condición es suficiente, supongamos que $n = 2^s p_1 \dots p_r$, donde $p_1, \dots, p_r$ son primos de Fermat distintos. Por las propiedades de la función φ de Euler tenemos que:

$$\varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right) = \begin{cases} 2^{s-1}(p_1 - 1) \dots (p_r - 1), & s > 0 \\ (p_1 - 1) \dots (p_r - 1), & s = 0 \end{cases}.$$

De aquí sigue que $\varphi(n)$ es potencia de 2, ya que los p_i son primos de Fermat.

Comprobemos ahora que la condición es necesaria: supongamos que $\varphi(n)$ es una potencia de 2 y que la factorización de n es $n = q_1^{a_1} \dots q_s^{a_s}$, donde $q_1, ..., q_s$ son primos distintos y $a_i \geq 1$. Haciendo uso nuevamente de las propiedades de la función φ de

$$\varphi(n) = n \prod_{i=1}^{s} \left(1 - \frac{1}{q_i}\right) = q_1^{a_1 - 1}(q_1 - 1) \dots q_s^{a_s - 1}(q_s - 1).$$

Si q_i es impar, entonces debe darse que $a_i = 1$, ya que $\varphi(n)$ es una potencia de 2. En particular, $q_i - 1$ ha de ser una potencia de 2. De aquí, los primos impares que dividen a n tienen exponente 1, y son primos de Fermat. □

Observación 2.28. Observemos que la potencia de 2 en el Teorema 2.27 tiene sentido, ya que si podemos construir un $n-$ágono regular, entonces también podremos construir un $2n-$ágono regular, haciendo las bisectrices de cada ángulo. La demostración del Teorema 2.27 utiliza el hecho de que el *polinomio ciclotómico* $\Phi_n(x)$ es irreducible sobre $\mathbb{Q}$.

El $m-$ésimo número de Fermat es $F_m = 2^{2^m} + 1$, pero esta fórmula no siempre da lugar a un número primo. Los únicos primos de Fermat conocidos hasta la fecha son:

$$F_0 = 3, \qquad F_1 = 5, \qquad F_2 = 17, \qquad F_3 = 257, \qquad F_4 = 65537.$$

También se sabe que $F_i, 5 \leq i \leq 32$, son compuestos, así como otros F_i con $i > 32$. Por ejemplo, se sabe que $F_{2478782}$ es divisible por $3 \cdot 2^{2478785} + 1$, y hay ejemplos de números extremadamente más largos.

3

Números origami

En este capítulo utilizaremos el *origami*, arte de plegado de papel japonés, para hacer algunas construcciones que no son posibles para las construcciones con regla y compás. También daremos una descripción cuidadosa de los *números origami* y explicaremos qué significan desde el punto de vista de la Teoría de Galois. Finalmente construiremos la solución de la ecuación de cuarto grado aplicando un argumento propio de geometría proyectiva.

3.1. Axiomas y primeras propiedades

A continuación vamos a definir los elementos básicos que participan en el origami. Luego presentaremos los axiomas o movimientos básicos que pueden hacerse con origami, cuyas construcciones se muestran gráficamente en la Figura 3.1.

En la geometría basada en el plegado de papel primero se establecen algunos conceptos básicos para luego definir los seis axiomas postulados por Humiaki Huzita (ver [5]). Posteriormente Koshiro Hatori (ver [3]) añadió un séptimo postulado que escapa de los contenidos de este trabajo.

Definición 3.1. *Una **hoja de papel** representa una porción del plano. Por tanto tiene límites y es finito, pero puede ser una representación abstracta de un plano infinito.*
*Un **doblez** es un ente análogo a un segmento de recta en la geometría euclídea. Entendemos que el papel para desarrollar los pliegues es finito, de ahí que el doblez es el concepto límite de recta. Este concepto también puede aplicarse a los bordes de la hoja.*
*Un **punto** es un concepto no definido en el origami, pero representa la intersección de dos dobleces, o bien representan las esquinas (ángulos) del papel.*

Podemos afirmar que en una hoja de papel pueden ser construidos infinitos segmentos de recta que pasan por un punto, rectas perpendiculares a otras, la bisectriz de un ángulo, la mediatriz de un segmento, y hacer también varias construcciones algo más complejas, como la que estudiaremos en la Figura 3.2 para trisecar un ángulo, o bien las demostraciones de algunos productos notables o el Teorema de Pitágoras.

Los movimientos básicos o axiomas del origami son:

O1. **Dados dos puntos distintos P_1 y P_2, existe un único doblez ℓ que pasa a través de ellos**.
Este axioma es análogo al primer axioma de Euclides: *Por dos puntos pasa una única recta*, que coincide con la construcción C1 con regla y compás.

O2. **Dados dos puntos P_1 y P_2, existe un único doblez que lleva P_1 sobre P_2**.
Este axioma se relaciona con la construcción de la mediatriz del segmento que une P_1 con P_2 realizado con regla y compás en la segunda construcción de la Figura 2.2.

O3. **Dados dos dobleces distintos, ℓ_1 y ℓ_2, existen uno o dos dobleces que sitúan ℓ_1 exactamente sobre ℓ_2.**
Cuando ℓ_1 y ℓ_2 son paralelos, entonces esta construcción equivale a encontrar la recta paralela común que equidista de ambos dobleces, según se hizo en la Figura 2.3. En caso contrario, se construye la bisectriz del ángulo que determinan ambos dobleces, como se hizo en la primera construcción de la Figura 2.2.

O4. **Dados un doblez ℓ y un punto P, existe un único doblez que deja fijo el doblez ℓ y contiene a P.**
Este axioma se relaciona con la construcción de la perpendicular a una recta que pasa por un punto que está o no en dicha recta. Es una combinación de las dos últimas construcciones de la Figura 2.2.

O5. **Dados un doblez ℓ y dos puntos P_1 y P_2, se puede encontrar un máximo de dos dobleces de forma que al situar P_1 sobre ℓ, también pertenezca a ℓ el punto P_2.** En principio, el punto P_2 se mantiene fijo, ya que la construcción mueve P_1 sobre ℓ, y P_1 recorre un movimiento circular hasta coincidir con un punto de dicho doblez. Luego P_2 es el centro de una circunferencia donde uno de sus radios es el segmento $\overline{P_1P_2}$, con lo que tenemos tantas posibilidades de cumplir el enunciado del axioma como posiciones de recta y circunferencia encontramos en el plano: dos, una o ninguna. Este axioma coincide con la construcción C2 con regla y compás.

Todas las justificaciones realizadas en cada axioma del origami demuestran que los movimientos C1, C2, P1, P2 y P3 de las construcciones con regla y compás equivalen a considerar los cinco primeros axiomas del origami. Es momento de añadir el sexto axioma, que será vital para diferenciar el conjunto de núme-

ros construibles con origami de los números construibles con regla y compás y estudiar su estructura.

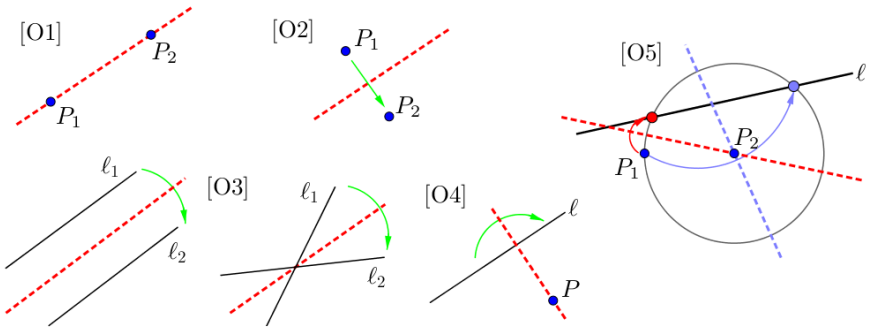


Figura 3.1. Construcciones de los cinco primeros axiomas del origami.

O6. **Dados los dobleces ℓ_1 y ℓ_2 y dos puntos P_1 y P_2 exteriores a ℓ_1 y ℓ_2 respectivamente, se puede encontrar un máximo de tres dobleces de forma de que al mover P_1 sobre ℓ_1, también quede P_2 sobre ℓ_2.**
La aplicación de este axioma se relaciona directamente con encontrar una tangente común a dos parábolas, como se estudiará en la Proposición 3.4.
En este axioma hay varias posibilidades cuando confrontamos las siguientes opciones:
(A) ℓ_1 y ℓ_2 son o no paralelos.
(B) P_1 y P_2 quedan ambos dentro de la región generada por ℓ_1 y ℓ_2, o bien solo uno de ellos, o bien ninguno.
Tales restricciones pueden comprobarse en la página 347 de [6]. Este axioma se desarrolla más adelante.

Empezaremos mostrando algunas construcciones con los axiomas del origami descritos anteriormente. En primer lugar demostramos que sí podemos hacer la trisección del ángulo con esta técnica.

Proposición 3.2 (Trisección de un ángulo). *Sea θ un ángulo con $0 < \theta < \pi$. Entonces θ puede ser trisecado utilizando origami.*

Demostración. Primero nos ocuparemos de un caso particular: tomemos el ángulo $\frac{\pi}{4} \leq \theta \leq \frac{\pi}{2}$. Lo marcamos desde el borde inferior, b, de una hoja de papel, aplicando el axioma O1, tomando como puntos el vértice P_1 y otro punto arbitrario en el borde superior de la hoja, b', según se observa en la Figura 3.2.

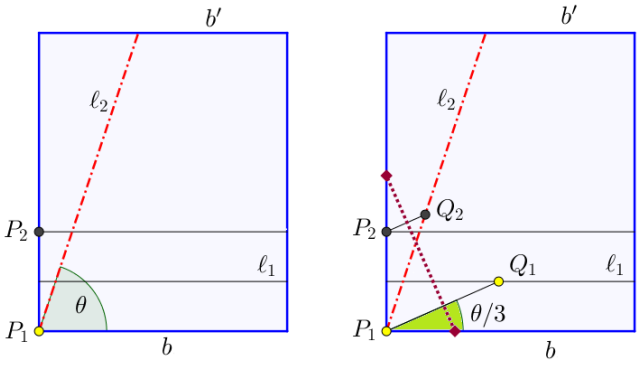


Figura 3.2. Trisección del ángulo.

Con esto, se genera el doblez ℓ_2 y, por tanto, θ es el ángulo entre las rectas ℓ_2 y b. Según se indica en la primera construcción de la Figura 3.2, doblamos la hoja dos veces para obtener dos rectas paralelas a b, obteniendo la recta ℓ_1 como la recta equidistante a las líneas paralelas que pasan por los puntos P_1 y P_2, según observamos en la misma figura. Hemos aplicado el axioma O3.

Ahora aplicaremos el axioma O6, que dobla la hoja para mover el punto P_1 sobre ℓ_1 (obteniendo Q_1) y P_2 se mueve sobre la recta l_2 (obteniendo Q_2), simultáneamente. El ángulo hecho entre la recta de la parte inferior de la hoja y la recta $\overline{P_1Q_1}$ es exactamente $\frac{\theta}{3}$. Con esto queda trisecado un ángulo arbitrario $\frac{\pi}{4} \leq \theta \leq \frac{\pi}{2}$ utilizando origami.

Si fuera $\theta > \frac{\pi}{2}$, entonces marcamos el eje vertical como la perpendicular a b que pasa por P_1 y aplicaríamos el axioma O3 a las rectas ℓ_2 y b, considerando así $\frac{\theta}{2}$ cuyo rango coincide con el del caso anterior. Una vez finalizado el proceso obtenemos $\frac{\theta}{6}$. Al replegar $\frac{\theta}{6}$ sobre sí mismo llegamos al ángulo $\frac{\theta}{3}$ buscado.

Finalmente, si fuera $\theta < \frac{\pi}{4}$, replegaríamos este ángulo sobre sí mismo, para trabajar con el ángulo doble 2θ y tener así un ángulo del primer caso. Tras terminar el procedimiento obtendríamos $\frac{2\theta}{3}$. Aplicando O3 marcamos la bisectriz de dicho ángulo y obtenemos $\frac{\theta}{3}$ como se pedía. □

El hecho de haber utilizado el axioma O6 resulta definitivo para poder realizar la construcción. Es muy importante tener una visión geométrica para poder entender por qué no era posible hacer esta construcción con regla y compás.

Geométricamente, hemos trazado *tangentes simultáneas a dos parábolas*, asunto que nos disponemos a justificar a continuación.

Consideremos una parábola genérica $\mathcal{P}$. Según su definición, una parábola es el lugar geométrico de todos los puntos P equidistantes a uno fijo P_1 (el *foco*) y a una recta fija ℓ_1 (la *directriz*), como se distingue en la Figura 3.3. En dicha figura, los segmentos $\overline{P_1P}$ y $\overline{PQ_1}$ tienen igual longitud, y $\overline{PQ_1}$ es perpendicular

a la directriz ℓ_1. Un hecho significativo es que Q_1 es el simétrico de P_1 respecto a la tangente a $\mathcal{P}$ que pasa por el punto P. También es cierto el recíproco. Esto se recoge en el siguiente resultado.

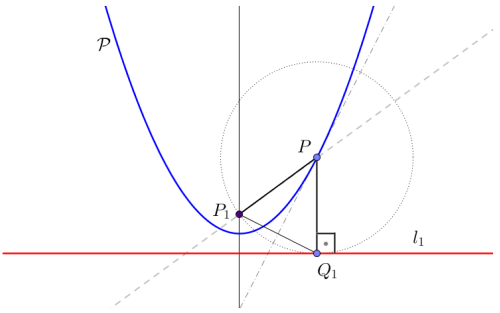


Figura 3.3. Parábola.

Lema 3.3. *En el plano, sea P_1 un punto que no está en la recta ℓ_1. Entonces, dada una recta ℓ, el punto simétrico de P_1 sobre ℓ pertenece a la recta ℓ_1 si, y solo si, ℓ es tangente a la parábola con foco en P_1 y directriz ℓ_1.*

Demostración. Después de un cambio de coordenadas, si fuera necesario, podemos suponer que $\mathcal{P}$ es la parábola con foco $P_1(0,p)$ y vértice $(0,0)$. En estas condiciones, la directriz de $\mathcal{P}$ es la recta $\ell_1 \equiv y = -p$ y la ecuación de la parábola es $\mathcal{P} \equiv x^2 - 4py = 0$.

La condición es necesaria. Dada una recta ℓ, vamos a denotar por σ_ℓ a la simetría axial con respecto a la recta ℓ. Supongamos entonces que $\sigma_\ell(P_1) \in \ell_1$, siendo ℓ_1 la directriz de $\mathcal{P}$. Sea $P \in \mathcal{P}$ un punto cualquiera, y sea Q_1 la proyección ortogonal de P en la directriz ℓ_1.

En la Figura 3.4, consideramos el ángulo $\widehat{P_1PQ_1}$ y trazamos por P la bisectriz, que coincide con la mediatriz del segmento $\overline{P_1Q_1}$, ya que el triángulo $\triangle P_1Q_1P$ es isósceles, en virtud de la definición de parábola. Nótese que por esto, $\mathrm{dist}(P_1,P) = \mathrm{dist}(P,Q_1)$.

Para probar que ℓ es la recta tangente a $\mathcal{P}$ por P, tomaremos otro punto de $\mathcal{P}$, distinto de P_1, y lo denominamos P_2. De nuevo, trazamos su proyección ortogonal sobre la directriz ℓ_1, y obtenemos el punto Q_2. Notamos que $\mathrm{dist}(P_1,P_2) = \mathrm{dist}(P_2,Q_2)$ en virtud de la definición de parábola. Además, $\mathrm{dist}(P_2,Q_2) < \mathrm{dist}(P_2,Q_1)$, por lo que $\mathrm{dist}(P_1,P_2) < \mathrm{dist}(P_2,Q_1)$.

Una recta $\ell \equiv ax + by = c$ divide el plano en dos semiplanos, que son

$$\ell_+ := ax + by > c \text{ y } \ell_- := ax + by < c.$$

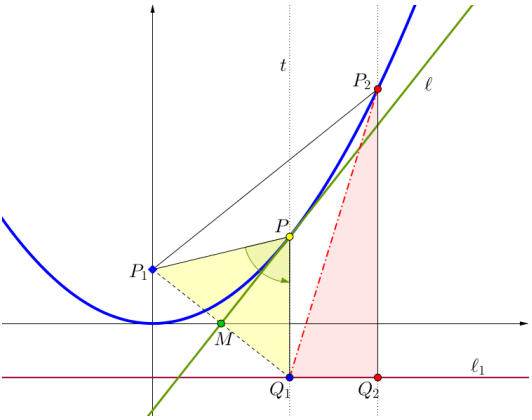


Figura 3.4. Construcción en la parábola.

Dado que $\text{dist}(P_2, Q_1) > \text{dist}(P_1, P_2)$, para cualquier $P_2 \in \mathcal{P} \setminus \{P_1\}$, se deduce que toda la parábola está contenida en el semiplano ℓ_+, y dado que la desigualdad es estricta, se tiene la condición de tangencia de ℓ a $\mathcal{P}$ por P. Nótese que justo en P se da la igualdad, debido a la construcción, con lo que ℓ es tangente o secante. Pero si hubiera otro punto donde se diera la igualdad $(\text{dist}(P_2, Q_1) = \text{dist}(P_1, P_2))$ sería otro punto de intersección con ℓ y la recta sería secante. Como esa igualdad no se da, se tiene que ℓ es necesariamente tangente a $\mathcal{P}$.

Estableceremos ahora que la condición es suficiente, aprovechando la construcción de la Figura 3.4. Debemos demostrar que el punto $Q_2 = \sigma_\ell(P_1)$ es un punto de $\ell_1 \equiv y = -p$. Nótese que $r \cap \overline{PQ_1} = \{Q_2\}$. Nuestra estrategia será obtener algebraicamente las coordenadas de Q_2.

Para ello, calcularemos las ecuaciones de las rectas $r \equiv \overline{P_1 M}$ y $t \equiv \overline{PQ_1}$ y estudiaremos su intersección. Los puntos conocidos son $P_1(0, p)$ y $P(x_0, y_0)$.

Dado que t es paralela al eje OY, entonces $t \equiv x = x_0$.

Por otra parte, la recta r es perpendicular a la mediatriz de $P_1 Q_1$ por construcción. Dado que esa mediatriz es ℓ (que es la recta tangente a $\mathcal{P}$ por $P(x_0, y_0)$) y que la pendiente de ℓ es $m_\ell = \frac{x_0}{2p}$, entonces, la pendiente de r es $m_r = \frac{-1}{m_\ell} = \frac{-2p}{x_0}$. Por tanto, la ecuación de r es: $r \equiv y - p = \frac{-2p}{x_0} x$.

Luego la intersección de ambas rectas viene dada por:

$$Q_2 \equiv r \cap t \equiv \begin{cases} x = x_0 \\ y - p = \frac{-2p}{x_0} x_0 = -2p \end{cases}.$$

De aquí que $y = -p$ y $Q_2 = (x_0, -p) \in \ell$, como había que demostrar. □

Volvamos a la Figura 3.2 para estudiar en más profundidad el axioma O6. El movimiento de origami utilizado que convierte por simetría axial P_1 en

$Q_1 \in \ell_1$ y P_2 en $Q_2 \in \ell_2$, crea un doblez en el papel para producir una tangente. Esto significa que el punto simétrico a P_1 respecto a dicha simetría axial en la Figura 3.2 está sobre la recta ℓ_1, con lo que dicho eje es ciertamente la recta tangente a la parábola con foco P_1 y directriz ℓ_1, en virtud del Lema 3.3. El mismo argumento puede aplicarse a que el mismo eje de simetría es la recta tangente a la parábola con foco en P_2 y con directriz ℓ_2. Por lo tanto, deducimos que utilizar origami implica encontrar tangentes simultáneas a dos parábolas dadas.

Ya sabemos que las construcciones con regla y compás permitían resolver ecuaciones de segundo grado, según se demostró en la Proposición 2.11. Según la equivalencia entre los movimientos de las construcciones con regla y compás y los primeros axiomas de origami, entonces el origami también sirve para resolver ecuaciones cuadráticas. En el próximo resultado estudiamos que el sexto axioma del origami nos permite resolver ecuaciones cúbicas.

Proposición 3.4. *Sean $a, b \in \mathbb{R}, b \neq 0$. Entonces el polinomio $p(x) := x^3+ax+b$ tiene raíces que pueden encontrarse aplicando el sexto axioma del origami. Es decir, existen dos parábolas $\mathcal{P}_1$ y $\mathcal{P}_2$ y una recta ℓ tangente simultánea a ambas parábolas cuya pendiente es raíz de $p(x) = 0$.*

Demostración. Nos disponemos a encontrar las raíces reales de la ecuación $p(x) = 0$, según se ha representado en la Figura 3.5. Para ello, consideremos las parábolas

$$\begin{cases} \mathcal{P}_1 \equiv \left(y - \dfrac{1}{2}a\right)^2 = 2bx \\ \mathcal{P}_2 \equiv y = \dfrac{1}{2}x^2 \end{cases}. \tag{3.1}$$

Vamos a suponer que existe una recta ℓ, con pendiente m, que es tangente simultánea a $\mathcal{P}_1$ y $\mathcal{P}_2$, digamos en los puntos $P_1(x_1, y_1)$ a la primera parábola y en $P_2(x_2, y_2)$ a la segunda. Impondremos estas condiciones manipulando las ecuaciones de las parábolas y la recta tangente.

Para que ℓ sea tangente a $\mathcal{P}_1$, su pendiente será el valor de la derivada de la función y que define su ecuación, y evaluada en el punto de contacto. Dado que la ecuación implícita de $\mathcal{P}_1$ es $(y - \frac{1}{2}a)^2 = 2bx$, derivamos con respecto a x y obtenemos $2(y - \frac{1}{2}a)y' = 2b$. Luego $\left(y - \frac{1}{2}a\right) y' = b$, y con ello,

$$m_1 = \frac{b}{y_1 - \frac{1}{2}a}.$$

Esto implica que $m \neq 0$, pues $b \neq 0$ por hipótesis, y que $y_1 - \frac{1}{2}a = \frac{b}{m}$, y llevándolo a la ecuación de $\mathcal{P}_1$,

$$x_1 = \frac{\left(y_1 - \frac{1}{2}a\right)^2}{2b} = \frac{\left(\frac{b}{m}\right)^2}{2b} = \frac{b}{2m^2}, \quad y_1 = \frac{b}{m} + \frac{a}{2}. \tag{3.2}$$

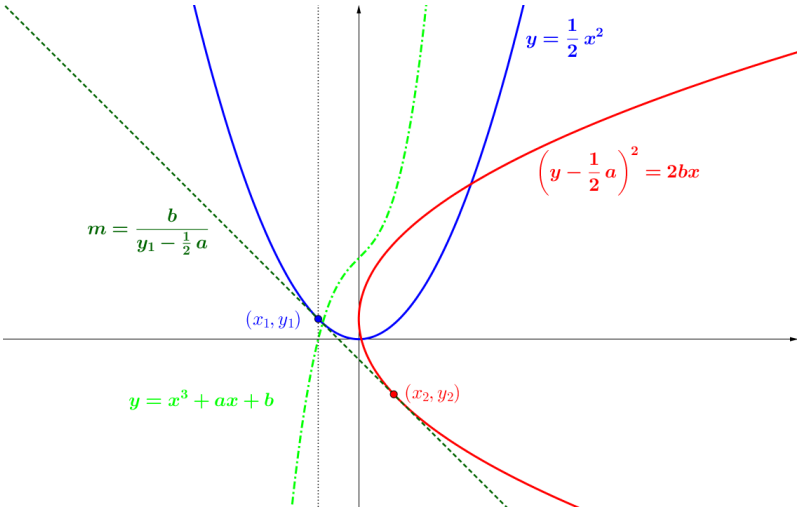


Figura 3.5. La pendiente de la tangente simultánea a dos parábolas resuelve la ecuación cúbica reducida.

Por otra parte, para imponer que ℓ sea tangente a $\mathcal{P}_2$, hacemos el mismo procedimiento para calcular su pendiente en el punto de contacto P_2, se obtiene que $m = x_2$. Sustituimos esto en la ecuación de $\mathcal{P}_2$ y obtenemos: $y_2 = \frac{m^2}{2}$. Por tanto, al imponer que ℓ sea tangente a $\mathcal{P}_2$, obtenemos las relaciones

$$x_2 = m, \quad y_2 = \frac{m^2}{2}. \tag{3.3}$$

En definitiva, han resultado los puntos de contacto a la tangente común, por lo que podemos calcular el valor de la pendiente a través de los puntos P_1 y P_2 según el cociente incremental: $m = \frac{y_2 - y_1}{x_2 - x_1}$, y obtenemos:

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

Pasando todo al miembro de la izquierda, obtenemos

$$m(2m^3 - b) - m^4 + 2bm + am^2 = 0,$$

lo que implica que $m^4 + bm + am^2 = 0$, que es equivalente a que $m(m^3 + am + b) = 0$, con lo que m cumple la ecuación polinómica $m^3 + am + b = 0$ deseada, ya que $m \neq 0$.

En conclusión, las pendientes de las tangentes simultáneas a las parábolas de (3.1) son raíces de la ecuación de tercer grado $m^3 + am + b = 0$. □

Corolario 3.5. *Sea $p(x) := ax^3 + bx^2 + cx + d$ un polinomio de tercer grado arbitrario. Entonces es posible encontrar una raíz aplicando el sexto axioma del origami.*

Demostración. Supongamos que $p(x) = ax^3 + bx^2 + cx + d$ es un polinomio de tercer grado, motivo por el cual ha de ser $a \neq 0$.
Podemos conseguir el polinomio mónico que tiene las mismas raíces que p dividiendo por a todos los coeficientes, obteniendo

$$p_1(x) = x^3 + \frac{b}{a}x^2 + \frac{c}{a}x + \frac{d}{a}.$$

Renombramos sus coeficientes

$$p_1(x) = x^3 + \tilde{b}x^2 + \tilde{c}x + \tilde{d}.$$

Podemos conseguir reducir los términos de este polinomio, eliminando el término en x^2. Para ello, hacemos el cambio $x_* = x - \frac{\tilde{b}}{3}$. De esta forma llegamos al polinomio

$$p_2(x_*) = x_*^3 + a'x_* + b'.$$

Luego estudiar las raíces de p_2 es equivalente a estudiar las del polinomio genérico p. □

Observación 3.6. El eje de simetría axial en la Figura 3.2 es un ejemplo de construcción O6. Es preciso remarcar que existen situaciones en las que la recta ℓ no satisface las condiciones de O6, es decir, que ℓ no siempre existe. Basta con poner como ejemplo las parábolas $\mathcal{P}_1 \equiv y = x^2$ y $\mathcal{P}_2 \equiv y = 2x^2 + 1$, ya que al estar $\mathcal{P}_2$ contenida completamente en el espacio cóncavo que delimita $\mathcal{P}_1$, no puede haber tangentes comunes. De hecho, la condición necesaria y suficiente de existencia de tangente común (doblez) es que los puntos P_i sean exteriores a la región delimitada por ℓ_i, $i = 1, 2$, según se enuncia en el axioma. En la práctica se deberá trabajar con un papel *lo suficientemente grande* para que se dé el resultado.

Según el Lema 3.3, O6 nos permite trazar una tangente simultánea a dos parábolas dadas (suponiendo que exista dicha tangente). Observamos que O6 construye una única recta ℓ. Una vez que tengamos ℓ, podremos construir los puntos simétricos de P_1 y P_2 respecto de ℓ por construcciones análogas a las de regla y compás.

3.2. Números origami-construibles

Según se justificaba en la sección anterior, podemos mantener los movimientos de las construcciones con regla y compás y añadir el axioma O6. Por

tanto, C1, C2 y O6 crean circunferencias y rectas, y las intersecciones de estos elementos utilizan los movimientos descritos en P1, P2 y P3 de la Sección 2.1, y originan nuevos puntos que pueden ser utilizados en construcciones posteriores. Definimos, por tanto, los números origami análogamente a como lo hacíamos con los números construibles con regla y compás:

Definición 3.7. *Un número $\alpha \in \mathbb{C}$ es un* ***número origami*** *si existe una secuencia finita de construcciones que utilizan C1, C2, O6, P1, P2 y P3 y que comenzando con 0 y 1, terminan en α.*

El conjunto de todos los números origami se denotará por $\mathscr{O}$, esto es:

$$\mathscr{O} = \{\alpha \in \mathbb{C} : \alpha \text{ es número origami}\}.$$

A continuación estudiaremos la estructura y las primeras propiedades de $\mathscr{O}$, al igual que hicimos con los números construibles con regla y compás.

Proposición 3.8. *El conjunto $\mathscr{O} = \{\alpha \in \mathbb{C} : \ \alpha$ es un número origami $\}$ es un subcuerpo de $\mathbb{C}$. Además, si $\alpha \in \mathbb{C}$, $\alpha = a + ib$, entonces $\alpha \in \mathscr{O}$ si, y solo si, $a, b \in \mathscr{O}$.*

Demostración. La demostración de que los números origami-construibles son un subcuerpo de los números complejos es análoga a la dada para los números construibles con regla y compás. También puede encontrarse en el capítulo 10 de [7]. La prueba de que un elemento es construible si, y solo si, lo son sus partes real e imaginaria es exactamente igual a la realizada en el Teorema 2.8. □

Una propiedad que marca la diferencia con los números origami-construibles con respecto de los construibles con regla y compás ya fue introducida en la Proposición 3.4. Como consecuencia de ella tenemos:

Proposición 3.9. *Sea $\alpha \in \mathscr{O}$ un número construible por origami. Entonces $\sqrt{\alpha}$, $\sqrt[3]{\alpha}$ también son origami-construibles.*

Demostración. Escribamos α en coordenadas polares, esto es, $\alpha = re^{i\theta}$. Podemos asumir que $r > 0$, ya que $0 \in \mathscr{C}$, y por tanto $0 \in \mathscr{O}$. Utilizando el compás, podemos transferir r al eje OX, y luego, utilizando la construcción con regla y compás hecha en la Proposición 2.11, se sigue que $\sqrt{r} \in \mathscr{O}$. Como podemos también bisecar θ con regla y compás, se tiene que, para $n \in \mathbb{Z}$, $\sqrt{\alpha} = \sqrt{r}e^{i\left(\frac{\theta}{2} + n\pi\right)} \in \mathscr{O}$, puesto que es producto de números origami-construibles, y el conjunto de números origami-construible es subcuerpo de $\mathbb{C}$.

Para la raíz cúbica, podemos trisecar θ utilizando la Proposición 3.2. Para construir $\sqrt[3]{r}$, consideramos la ecuación cúbica $x^3 - r = 0$, que corresponde a valores $a = 0, b = -r$. Según la Proposición 3.1, utilizamos las parábolas

$$\begin{cases} \mathcal{P}_1 \equiv y^2 = -2rx \\ \mathcal{P}_2 \equiv x^2 = 2y \end{cases}$$

para resolver la cúbica. Con esto, se determina que r es construible con regla y compás.

Según lo comentado al principio de la demostración del Lema 3.3, estas parábolas cuentan con los focos $\alpha_1 = \left(\frac{-r}{2}, 0\right), \alpha_2 = \left(0, \frac{1}{2}\right)$ y las directrices $\ell_1 \equiv x = \frac{-r}{4}$ y $\ell_2 \equiv y = \frac{-1}{2}$. Como r es un punto construible con regla y compás, y como $\mathscr{C}$ es cuerpo, entonces α_1 y α_2 son puntos construibles con regla y compás, y las directrices son dos paralelas a los ejes de coordenadas que pasan por puntos construibles, los cuales son construibles con regla y compás, y por tanto, ℓ_1 y ℓ_2 son construibles con regla y compás (y por tanto, con origami).

Aplicando O6 a $\alpha_1, \alpha_2, \ell_1$ y ℓ_2, podemos construir la tangente simultánea a ambas parábolas, y la llamamos ℓ. Según la construcción de la Proposición 3.4, entonces la pendiente m de ℓ cumple la ecuación, es decir, $m = \sqrt[3]{r}$. Esto implica que $\sqrt[3]{r} \in \mathscr{O}$, y como $\omega = e^{\frac{2\pi i}{3}} = \frac{1}{2} + i\frac{\sqrt{3}}{2} \in \mathscr{C}$, con lo que $\omega \in \mathscr{O}$, y se sigue que

$$\sqrt[3]{\alpha} = \omega^j \sqrt[3]{r}\, e^{\frac{i\theta}{3}} \in \mathscr{O}, \quad j = 0, 1, 2.$$

□

Al igual que establecimos con los números construibles con regla y compás, también podemos caracterizar los números origami haciendo uso de la Teoría de Galois:

Teorema 3.10. *Un elemento $\alpha \in \mathbb{C}$ es origami-construible si, y solo si, existe una torre de cuerpos*

$$\mathbb{Q} = K_0 \subset K_1 \subset \cdots \subset K_n \subset \mathbb{C}$$

tal que $\alpha \in K_n$ y $[K_i : K_{i-1}] = 2$ ó 3, para cada $i = 1, 2, ..., n$.

Demostración. Para demostrar la doble implicación, primero estudiaremos que la condición es suficiente, es decir, supondremos que existe una torre de cuerpos $\mathbb{Q} = K_0 \subset ... \subset K_n$ de forma que $[K_i : K_{i-1}] \in \{2, 3\}$ y $\alpha \in K_n$. Para demostrar que $\alpha \in \mathscr{O}$, para cualquier $\alpha \in K_n$, lo haremos por inducción sobre n.

El caso $n = 0$ es trivial, ya que la torre de cuerpos se reduce a $\mathbb{Q} = K_0$, pero según se estableció en el Corolario 2.9, $\mathbb{Q}$ se construye con regla y compás, y por tanto, es origami-construible.

Nuestra hipótesis de inducción es que dada una torre de cuerpos $K_0 \subset ... \subset K_j$, con $[K_i : K_{i-1}] \in \{2, 3\}$, entonces $K_j \subset \mathscr{O}$, para cada $1 \leq i \leq j \leq n-1$.

Sea ahora $\alpha \in K_n$ un elemento algebraico sobre K_{n-1}. Dado que $[K_n : K_{n-1}] \in \{2, 3\}$ y $K_{n-1} \subset \mathscr{O}$, entonces existe un polinomio $f \in \mathscr{O}[x]$ con $\deg(f) \in \{2, 3\}$ tal que $f(\alpha) = 0$. Esto implica que α se determina algebraicamente mediante raíces cuadradas o cúbicas de operaciones aritméticas realizadas sobre los coeficientes de f, que son elementos origami-construibles. Por ello, $\alpha \in \mathscr{O}$, en virtud de la Proposición 3.9, y concluimos que $K_n \subset \mathscr{O}$, puesto que α es arbitrario.

Demostraremos a continuación que la condición es necesaria, esto es, partiremos de un elemento construible $\alpha \in \mathscr{O}$ y habrá que encontrar una torre de cuerpos $\mathbb{Q} = K_0 \subset ... \subset K_n$ de forma que $[K_j : K_{j-1}] \in \{2, 3\}$ y $\alpha \in K_n$.

Probar que $\alpha = a + ib \in K_n$ es equivalente a que $a, b \in K_n$.

Se demuestra por inducción sobre N, el número de construcciones con P1, P2 y P3 para obtener α, cuando se comienza la construcción con 0 y 1. Es decir, se hace análoga a la realizada en el Teorema 2.18, por lo que sólo desarrollaremos las partes no reflejadas en dicho resultado. Así analizamos cuando terminamos con cada una de las tres construcciones y deducir que $\alpha \in K_n$.

Caso 1: El último paso para construir α es P1 (intersección de dos rectas ℓ_1 y ℓ_2). Esto da lugar a dos posibles situaciones: construir las rectas utilizando C1 (la recta que pasa por dos puntos construibles, como el único pliegue que pasa por dichos puntos, y por tanto es construible), o bien O6, caso que desarrollaremos en profundidad.

Supongamos que ℓ_1 fue construida con O6. Entonces ℓ_1 es tangente común a dos parábolas $\mathcal{P}_1$ y $\mathcal{P}_2$ cuyos focos y directrices fueron construidos en pasos anteriores.

Supongamos en primer lugar que las parábolas son:

$$\mathcal{P}_1 \equiv \left(y - \frac{a}{2}\right)^2 = 2bx, \quad \mathcal{P}_2 \equiv y = \frac{1}{2}x^2, \quad a, b \in \mathbb{R},$$

según se usaban en la Proposición 3.4. Según el razonamiento que se hizo en la implicación anterior, los parámetros $a, b \in K_n$, donde K_n es el último cuerpo de una torre $\mathbb{Q} = K_0 \subset ... \subset K_n$ tal que $[K_j : K_{j-1}] \in \{2, 3\}$, con $1 \leq j \leq n$. Además, la pendiente de ℓ_1, m_1, satisface una ecuación cuadrática o cúbica con coeficientes en $\mathscr{O}$. Por tanto, $m_1 \in K_n$. También sabemos que el punto de tangencia entre ℓ_1 y $\mathcal{P}_1$ es, según (3.2),

$$(x_1, y_1) = \left(\frac{b}{2m_1^2}, \frac{b}{m_1} + \frac{a}{2}\right) \in K_n.$$

Por tanto, haciendo variar el punto de tangencia, concluimos que ℓ_1 tiene coeficientes construibles, esto es, existen $A_1, A_2, A_3 \in K_n$ tales que $\ell_1 \equiv A_1x + A_2y = A_3$.

Supongamos ahora que tenemos dos parábolas arbitrarias $\tilde{\mathcal{P}}_1$ y $\tilde{\mathcal{P}}_2$. Tras un cambio de variable pertinente, $\tilde{\mathcal{P}}_1$ y $\tilde{\mathcal{P}}_2$ admiten ecuaciones del tipo $\mathcal{P}_1$ y $\mathcal{P}_2$. Este cambio de variable involucra operaciones aritméticas o raíces cuadradas, y con esto, habríamos determinado la torre de cuerpos que contiene tanto a los coeficientes de la recta como a las partes real, a, e imaginaria, b, de α.

Este mismo proceso se hace para determinar la ecuación de la segunda recta $\ell_2 \equiv B_1x + B_2y = B_3$, para algunos $B_1, B_2, B_3 \in K_n$. Esto permite continuar con la prueba del Teorema 2.18 y llegar al resultado.

Caso 2: El último paso para construir α es P2 (intersección de una recta ℓ y una circunferencia $\mathcal{C}$). En este caso, encontramos que ℓ puede haberse construido

mediante C1 o O6, cuyo procedimiento está ya probado. Por tanto, partimos de una recta construible y una circunferencia construible, situación completamente descrita en la demostración del Teorema 2.18.
Caso 3: El último paso para construir α es P3 (intersección de dos circunferencias $\mathcal{P}_1$ y $\mathcal{P}_2$). También es un caso completamente descrito en el Teorema 2.18. □

Continuamos con un ejemplo de aplicación del Teorema 3.10:

Ejemplo 3.11. Dada la raíz séptima de la unidad, $\xi_7 = e^{\frac{2\pi i}{7}} = \cos\left(\frac{2\pi}{7}\right) + i\,\mathrm{sen}\left(\frac{2\pi}{7}\right)$, sea $\alpha := \cos\left(\frac{2\pi}{7}\right)$, la torre de cuerpos del diagrama:

$$\mathbb{Q} \subset \mathbb{Q}(\alpha) \subset \mathbb{Q}(\alpha, i) = \mathbb{Q}(\xi_7)$$

muestra que, dado que $f = 8x^3 + 4x^2 - 4x - 1 = \mathrm{Irr}(\alpha, \mathbb{Q})$, entonces $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$, y además, $g = x^2 + 1 = \mathrm{Irr}(i, \mathbb{Q}(\alpha))$, pues $\alpha \in \mathbb{R} \subsetneq \mathbb{C}$, con lo que $[\mathbb{Q}(\xi_7) : \mathbb{Q}(\alpha)] = 2$. Entonces $[\mathbb{Q}(\xi_7) : \mathbb{Q}] = 3 \cdot 2 = 6$. Por tanto, ξ_7 es un número origami y, en consecuencia, un heptágono regular (7-ágono) puede ser construido con origami.

Teorema 3.12. *Sea $\alpha \in \mathbb{C}$ un algebraico sobre $\mathbb{Q}$ y sea L el cuerpo de descomposición de $Irr(\alpha, \mathbb{Q})$. Entonces α es un número origami si, y solo si, $[L : \mathbb{Q}] = 2^a \cdot 3^b$ para ciertos enteros $a, b \geq 0$.*

Demostración. Reproduciremos la demostración del Teorema 2.24. Sea $\alpha \in \mathscr{O}$. Primero probaremos que $\mathscr{O} : \mathbb{Q}$ es una extensión normal, o lo que es equivalente, $f = \mathrm{Irr}(\alpha, \mathbb{Q})$ se descompone por completo en $\mathscr{O}$. Dado que $\alpha \in \mathscr{O}$, en virtud del Teorema 3.10, existe una torre de cuerpos $\mathbb{Q} = K_0 \subset ... \subset K_n \subset \mathbb{C}$ donde $[K_i : K_{i-1}] \in \{2, 3\}$, siendo $\alpha \in K_n$. Si $M : K_n$ es la menor extensión que es de Galois, observamos que f se descompone completamente en M ya que M es una extensión normal sobre $\mathbb{Q}$, f es irreducible en $\mathbb{Q}[x]$ y $\alpha \in K_n \subset M$.

Si $\beta \in M$ es raíz de f, entonces existe $\sigma \in \mathrm{Gal}(M : \mathbb{Q})$ tal que $\sigma(\alpha) = \beta$. Aplicando σ a la torre de cuerpos, tenemos

$$\mathbb{Q} = \sigma(\mathbb{Q}) = \sigma(K_0) \subset \cdots \subset \sigma(K_n),$$

donde $[\sigma(K_i) : \sigma(K_{i-1})] = [K_i : K_{i-1}] \in \{2, 3\}$, para cada $1 \leq i \leq m$. Aplicando de nuevo el Teorema 3.10, obtenemos que $\beta = \sigma(\alpha) \in \sigma(K_n)$ es origami-construible, por lo que f se descompone completamente sobre $\mathscr{O}$ y $\mathscr{O} : \mathbb{Q}$ es extensión normal. Así, existe $L = \mathbb{Q}$, el cuerpo de descomposición de f sobre $\mathbb{Q}$, que por el Teorema del elemento primitivo, $L = \mathbb{Q}(\gamma)$, para algún $\gamma \in L$.

Finalmente, aplicando el Teorema 1.17 y el Teorema 3.10, concluimos que $[\mathbb{Q}(\gamma) : \mathbb{Q}] = [L : \mathbb{Q}] = 2^a \cdot 3^b$, para ciertos enteros no negativos a, b.

Para probar el recíproco, supongamos que $[L : \mathbb{Q}] = 2^a \cdot 3^b$, con $\alpha \in L$. Entonces, debido al valor de la extensión, el Teorema de Burnside (1.31) concluye

que $\mathrm{Gal}(L:\mathbb{Q})$ es resoluble. Por tanto, existe una cadena de subgrupos $\{1_G\} = G_0 \trianglelefteq ... \trianglelefteq G_n = \mathrm{Gal}(L:\mathbb{Q})$ tal que $\mathrm{Gal}(G_i/G_{i-1})$ es abeliano. Aplicando el teorema de correspondencia de Galois (Teorema 1.33) llegamos a que $\mathrm{Gal}(L : L_{G_i}) = G_i$ y $K_i = [L_{G_i} : \mathbb{Q}] = \frac{|G|}{|G_i|}$, siendo, por tanto $[K_i : K_{i-1}] \in \{2, 3\}$. Luego existe una torre de cuerpos

$$\mathbb{Q} = K_0 \subseteq ... \subseteq K_n = L, \qquad \text{tal que } [K_i : K_{i-1}] \in \{2, 3\}.$$

Con esto, si $\alpha \in L$, tenemos que L es cuerpo de descomposición de $\mathrm{Irr}\,(\alpha,\ \mathbb{Q})$ y $[L:\mathbb{Q}] = 2^a \cdot 3^b$. Luego $\alpha \in \mathscr{O}$. □

Ejemplo 3.13.

Si $\xi_{11} = e^{\frac{2\pi}{11}}$ es la raíz undécima de la unidad, la extensión $\mathbb{Q}(\xi_{11}) : \mathbb{Q}$ es una extensión de Galois de grado 10, ya que $\mathrm{Irr}\,(\xi_{11},\ \mathbb{Q}) = x^{10}+x^9+...+x+1$. Dado que 10 no puede escribirse en la forma $2^a 3^b$, con a, b enteros positivos, entonces ξ_{11} no puede ser construido con origami.

Es importante no confundir la condición dada en el Teorema 3.12: el hecho de que $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ se pueda escribir en la forma $2^a \cdot 3^b$ no es definitiva para deducir que α sea origami-construible, salvo que $\mathbb{Q}(\alpha)$ sea el cuerpo de descomposición de $\mathrm{Irr}\,(\alpha,\ \mathbb{Q})$. Lo ilustramos en el siguiente ejemplo.

Ejemplo 3.14.

Sea $\alpha \in \mathbb{C}$ una raíz de $f = x^6 + x + 1$. Utilizando la reducción a $\mathbb{Z}_2[x]$ obtenemos que f es irreducible sobre $\mathbb{Q}$. En efecto, dado que $\deg(f) = 6$, entonces si $f = gh$, donde $1 < \deg(g) \leq \deg(h) < 5$, tenemos que $\deg(g) = 2$ o bien $\deg(g) = 3$.

En particular para estos grados, en $\mathbb{Z}_2[x]$ encontramos que los únicos polinomios irreducibles son $x^2 + x + 1$, $x^3 + x + 1$ y $x^3 + x^2 + 1$. Pero ninguno de estos polinomios divide a $f \in \mathbb{Z}_2[x]$, por lo que f es irreducible sobre $\mathbb{Q}$.

Por ello, $\mathbb{Q}(\alpha) : \mathbb{Q}$ es una extensión de grado 6 sobre $\mathbb{Q}$. Pero, aunque $6 = 2 \cdot 3$, α no es un origami-construible.

Esto es consecuencia de que el cuerpo de descomposición L de f (que no coincide con $\mathbb{Q}(\alpha)$) tiene como grupo de Galois $\mathrm{Gal}(L:\mathbb{Q}) \cong S_6$. Entonces, el Teorema 3.12 implica que $\alpha \notin \mathscr{O}$, dado que

$$[L:\mathbb{Q}] = |\mathrm{Gal}(L:\mathbb{Q})| = 6! = 2^4 \cdot 3^2 \cdot 5.$$

Una de las consecuencias de la Teoría de Galois es la resolubilidad de ecuaciones de cuarto grado, también conocidas como *cuárticas*. Antes de enunciar y demostrar el resultado, vamos a recordar algunas nociones de geometría proyectiva que serán necesarias para el desarrollo del último resultado del presente trabajo.

Una **cónica** en el espacio euclídeo tiene ecuación

$$\mathcal{C} \equiv a_{11}\tilde{x}^2 + a_{22}\tilde{y}^2 + 2a_{12}\tilde{x}\tilde{y} + 2a_{13}\tilde{x} + 2a_{23}\tilde{y} + a_{33} = 0.$$

Haciendo el cambio a coordenadas homogéneas dado por $\tilde{x} = \frac{x}{z}, \tilde{y} = \frac{y}{z}, z \neq 0$, entonces la cónica tiene ecuación

$$\mathcal{C} \equiv a_{11}x^2 + a_{22}y^2 + 2a_{12}xy + 2a_{13}xz + 2a_{23}yz + a_{33}z^2 = 0.$$

Matricialmente:

$$\mathcal{C} \equiv X^T M X, \qquad \text{donde } X = \begin{pmatrix} x \\ y \\ z \end{pmatrix} \text{ y } M = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{12} & a_{22} & a_{23} \\ a_{13} & a_{23} & a_{33} \end{pmatrix}.$$

De esta forma, una cónica viene definida por la matriz de coeficientes M, que es simétrica y, para que $\mathcal{C}$ sea una cónica *no degenerada*, entonces $\det(M) \neq 0$. Por ello, se puede definir la **cónica dual** de $\mathcal{C}$, y la simbolizaremos por $\hat{\mathcal{C}}$, a la cónica definida por M^{-1}. Por tanto: $\hat{\mathcal{C}} \equiv X^T M^{-1} X$.

También podemos definir una aplicación biyectiva entre una cónica $\mathcal{C}$ y su cónica dual $\hat{\mathcal{C}}$ dada por

$$\begin{aligned} \mathcal{C} &\longrightarrow \hat{\mathcal{C}} \\ P &\longrightarrow Q = MP^{\cdot} \end{aligned}$$

Sólo hay que tener en cuenta que M es simétrica. En particular, $Q^T M^{-1} Q = (MP)^T M^{-1}(MP) = P^T M^T M^{-1} M P = P^T M M^{-1} M P = P^T M P$.

El último aspecto importante a recordar es la relación matricial entre una cónica y una tangente en un punto a la misma en el plano proyectivo. En particular, el gradiente a la cónica $\mathcal{C}$ en un punto X es $\nabla_X \mathcal{C} = (2a_{11}x + 2a_{12}y + 2a_{13}z, 2a_{22}y + 2a_{12}x + 2a_{23}z, 2a_{33}z + 2a_{13}x + 2a_{23}y) = 2X^T M$. Por tanto, la recta tangente a $\mathcal{C}$ que pase por un punto $P = (p_1, p_2, p_3)^T$ ha de tener dirección perpendicular a $\nabla_X \mathcal{C}$, y responde a la expresión $P^T M X = 0$. Si aplicamos a la expresión de la tangente la aplicación biyectiva, esto es $Q = MP$, o de forma equivalente, $P = M^{-1}Q$, obtenemos:

$$0 = P^T M X = (M^{-1}Q)^T M X = Q^T (M^{-1})^T M X = Q^T M^{-1} M X = Q^T X.$$

Por tanto, la recta tangente a $\mathcal{C}$ en P es equivalente al punto $Q^T X$ en su cónica dual. Es decir, una recta en el plano proyectivo con ecuación $Ax + By + Cz = 0$ puede entenderse como el punto $(A, B, C) \in \hat{\mathcal{C}}$. Luego hemos demostrado que *una tangente común a dos cónicas es equivalente a un punto común a sus dos cónicas duales.*

Proposición 3.15. *Sea $f(x) = x^4 + bx^2 + 2cx + d$ un polinomio reducido de grado $\deg(f) = 4$, donde $c^2 - bd < 0$ y $d < 0$. Entonces, las raíces de $f(x)$ son números origami, esto es, se puede resolver $f(x) = 0$ con origami.*

Demostración. Tomemos la ecuación reducida de cuarto grado $x^4 + bx^2 + cx + d = 0$. Demostraremos que podemos construir las soluciones encontrando las tangentes comunes a dos cónicas, que serán una parábola y una circunferencia.

Tomemos los valores b, c, d que representan el término cuadrático de la ecuación, $bx^2 + cx + d$, que ha de ser negativo para que pueda existir una raíz real, y supongamos $c^2 - bd < 0$ con $d < 0$. Definimos

$$e := \pm\frac{\sqrt{bd - c^2}}{d}, \qquad r := |e|\sqrt{-d}.$$

Estos valores cumplen que $-de^2 = r^2$ y $de^2 = b - \frac{c^2}{d}$. Sea también la circunferencia $\mathcal{C}$ y parábola $\mathcal{P}$ definidas a continuación:

$$\mathcal{C} \equiv x^2 + y^2 = r^2, \qquad \mathcal{P} \equiv c^2x^2 - 2cdexy + d^2e^2y^2 - 4d^2ex = 0.$$

Tras convertir a coordenadas homogéneas y expresar matricialmente, obtenemos:

$$\mathcal{C} \leftrightarrows M_1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -r^2 \end{pmatrix}, \qquad \mathcal{P} \leftrightarrows M_2 = \begin{pmatrix} c^2 & -cde & -2d^2e \\ -cde & d^2e^2 & 0 \\ -2d^2e & 0 & 0 \end{pmatrix}.$$

Sus cónicas duales están definidas (salvo factor de proporcionalidad) por las matrices inversas:

$$\hat{\mathcal{C}} \leftrightarrows M_1^{-1} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1/r^2 \end{pmatrix}, \qquad \hat{\mathcal{P}} \leftrightarrows M_2^{-1} = \begin{pmatrix} 0 & 0 & de/2 \\ 0 & -d & c/2 \\ de/2 & c/2 & 0 \end{pmatrix}.$$

Finalmente, estudiamos la intersección de las cónicas duales $\hat{\mathcal{C}}$ y $\hat{\mathcal{P}}$. Sea $(A, B, C)^T$ un punto de intersección (que representaría la recta tangente $Ax + By + Cz = 0$ en coordenadas homogéneas). Entonces, al expresar ambas cónicas en forma polinómica y sustituir sus coordenadas, tenemos:

$$A^2 + B^2 = \frac{1}{r^2}C^2, \qquad deAC = dB^2 - cBC.$$

Deshaciendo el cambio a homogéneas y tomando $z = 1, B = -1$, se tienen:

$$A^2 + 1 = \frac{1}{r^2}C^2, \qquad deAC = cC + d.$$

Multiplicando por de^2C ambas ecuaciones y sustituyendo la segunda en la primera:

$$\underbrace{-\frac{de^2}{r^2}}_{=1}C^4 + \underbrace{\left(de^2 + \frac{c^2}{d}\right)}_{=b-\frac{c^2}{d}+\frac{c^2}{d}=b}C^2 + 2cC + d = 0.$$

Por tanto, las ordenadas en el origen de las rectas tangentes cumplen la ecuación cuártica reducida.

Corolario 3.16. *Sea $f(x) \in \mathbb{Q}[x]$ un polinomio de grado $\deg(f) \leq 4$. Entonces, las raíces de $f(x)$ son números origami, esto es, se puede resolver $f(x) = 0$ con origami.*

Demostración. Dado el polinomio $p(x) := ax^4 + bx^3 + cx^2 + dx + e$, tomamos el polinomio mónico que tiene las mismas raíces que p dividiendo dicho polinomio por a ($a \neq 0$ por ser de cuarto grado). Tenemos entonces

$$p_1(x) = x^4 + \tilde{a}x^3 + \tilde{b}x^2 + \tilde{c}x + \tilde{d}.$$

Ahora hacemos el cambio de variable $x_* := x + \frac{\tilde{a}}{4}$, de donde $x = x_* - \frac{\tilde{a}}{4}$. Nótese que al desarrollar x^4 en función de la nueva variable, el coeficiente de x_*^3 es exactamente $-\tilde{a}$, que será cancelado con $\tilde{a}x_*^3$, que aparece al desarrollar x^3. La expresión final de p_1 tras el cambio de variable es

$$p_2(x_*) := x_*^4 + \left(\tilde{b} - \frac{3\tilde{a}^2}{8}\right)x_*^2 + \left(\tilde{c} - \frac{\tilde{a}\tilde{b}}{2} + \frac{\tilde{a}^3}{8}\right)x_* + \left(\tilde{d} - \frac{\tilde{a}\tilde{c}}{4} + \frac{\tilde{a}^2\tilde{b}}{16} - \frac{3\tilde{a}^4}{256}\right).$$

En definitiva, existen $B, C, D \in \mathbb{Q}$ tales que p puede reducirse a $x^4 + Bx^2 + 2Cx + D$, que puede resolverse mediante los axiomas de origami, en virtud de la Proposición 3.15. □

Geométricamente la construcción anterior requiere localizar el foco y la directriz de la parábola $\mathcal{P}$, cuya ecuación podemos reducir haciendo un cambio de variable conveniente como $\mathcal{P} \equiv X^2 = 4d^3e^2Y$. En estas nuevas coordenadas, el foco y la directriz tienen estas expresiones:

$$F' = (0, d^3e^2), \qquad \ell' \equiv y = -d^3e^2.$$

Las coordenadas (x, y) del origen O' para las coordenadas (X, Y) está dado por $O' = \left(\frac{c^2e}{b^2}, -\frac{bc+cde^2}{b^2}\right)$. Deshaciendo el cambio de coordenadas, tenemos que las expresiones del foco y la directriz son:

$$F = O' + (d^4e^3, cd^3e^2) = \left(\frac{c^2e}{b^2} + d^4e^3, cd^3e^2 - \frac{bc + cde^2}{b^2}\right),$$

$$\ell \equiv O' + [(d^4e^3, cd^3e^2) + t(c, -de)] = \left(\frac{c^2e}{b^2} + d^4e^3, cd^3e^2 - \frac{bc + cde^2}{b^2}\right) + t(c, -de).$$

Para construir las soluciones, verificaremos que los coeficientes cumplen $c^2 - bd < 0$, $d < 0$, luego calcularemos e y r según se indican en la Proposición 3.15 y trazaremos (por C2) la circunferencia $\mathcal{C}^*$ con centro en el origen de coordenadas y radio $2r$. Dibujaremos el foco F (que es construible) y la directriz ℓ (por C1). Finalmente haremos los dobleces de forma que el origen O se mueva sobre la circunferencia y el foco F se mueva sobre la directriz simultáneamente. Esos

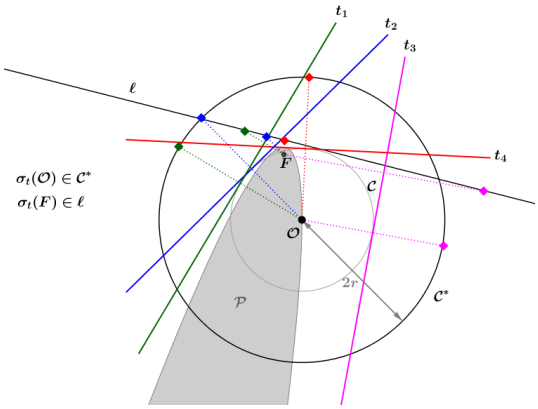


Figura 3.6. Cada doblez t_i $(1 \leq i \leq 4)$ mueve el centro de la circunferencia O' a la circunferencia de radio $2r$, $\mathcal{C}^*$ y, a su vez, mueve el foco F de la parábola $\mathcal{P}$ hasta su directriz ℓ.

cuatro dobleces son las tangentes comunes a $\mathcal{C}$ y $\mathcal{P}$, y las intersecciones de estas tangentes con el eje de ordenadas son cada una de las raíces de la ecuación cuártica.

Ejemplo 3.17. Para ilustrar este procedimiento, tomaremos el polinomio

$$p(x) = \left(x - \frac{107}{100}\right)\left(x - \frac{13}{25}\right)\left(x - \frac{41}{100}\right)(x+2) = x^4 - \frac{14}{5}x^2 + \frac{11}{5}x - \frac{23}{50}$$

que encontramos representado en línea discontinua en la Figura 3.7.

Calculamos los valores e y r dados en la Proposición 3.15, obteniéndose $e \simeq \frac{61}{100}$ y $r \simeq \frac{41}{100}$. Luego trazamos la circunferencia $\mathcal{C} \equiv x^2 + y^2 = \left(\frac{41}{100}\right)^2$ y la parábola $\mathcal{P} \equiv \frac{121}{100}x^2 - \frac{61}{100}xy + \frac{2}{25}y^2 + \frac{51}{100}x = 0$. Entonces las tangentes comunes tienen ecuaciones

$$t_1 \equiv y = \frac{12}{5}x + \frac{107}{100},\ t_2 \equiv y = \frac{77}{100}x + \frac{13}{25},\ t_3 \equiv \frac{119}{25}x - 2,\ t_4 \equiv -\frac{1}{20}x + \frac{41}{100}.$$

Por tanto, las raíces de la ecuación corresponden con los valores de las ordenadas en el origen de dichas rectas.

El procedimiento con origami, reproducido en la Figura 3.6, implica construir los ejes de coordenadas, trazamos la circunferencia de radio $2r$, $\mathcal{C}^* \equiv x^2 + y^2 = \left(\frac{41}{50}\right)^2$, el foco de la parábola, de coordenadas aproximadas $F\left(-\frac{1}{10}, \frac{19}{50}\right)$ y la directriz de ecuación $\ell \equiv y = -\frac{1}{4}x + \frac{43}{100}$. Entonces aplicamos 4 veces el axioma O6, situando el origen de coordenadas $\mathcal{O}$ sobre la circunferencia $\mathcal{C}^*$ y, simultáneamente, el foco F sobre la directriz ℓ.

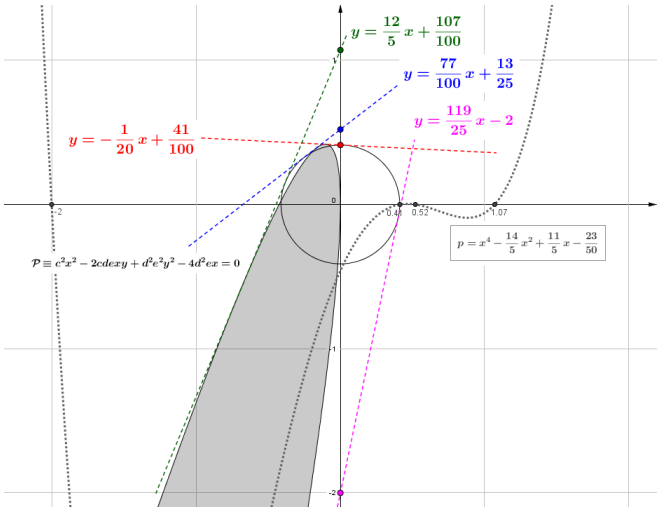


Figura 3.7. Cálculo analítico para encontrar las raíces siguiendo los movimientos de origami descritos en la Proposición 3.15.

3.3. ¿Por dónde continuar?

Llegados a este punto de desarrollo se abre la posibilidad de investigar sobre construcciones con regla graduada y compás, donde ahora la regla cuenta únicamente con una marca en el 0 y otra en el 1. Aunque parece un aspecto trivial, el resultado es que las construcciones con regla graduada y compás son equivalentes a las construcciones realizadas con origami.

Una construcción interesante con regla y compás, y que no hemos desarrollado por motivos de extensión, es la construcción de los n puntos que dividen una lemniscata en arcos de igual longitud, que será posible si, y solo si, $n = 2^m p_1 ... p_r$, siendo p_i = primos de Fermat, es decir, son de la forma $p_i = 2^{2^k} + 1$, para ciertos k enteros no negativos, según definíamos en la Sección 2.2. Estas divisiones, por tanto, también pueden ser construidas con origami, ya que son construibles con regla y compás.

Finalmente, sería de gran interés hacer un estudio histórico de todo lo desarrollado en los capítulos 2 y 3. Nosotros no hemos podido hacerlo por limitaciones de espacio.

Bibliografía

[1] D. Cox, *Galois Theory*, Wisley, 2012, 2nd edition, April.

[2] B. C. Edwards, J. Shurman, *Folding Quartic Roots*, 2001, Mathematical Association of America, Mathematics Magazine, Vol. 74, No. 1, pp. 19-25, http://www.jstor.org/stable/2691149.

[3] K. Hatori, *Origami Construction*, 2003, Ensayo parcial extraído de http://origami.ousaan.com/library/conste.html.

[4] U. Hernández, Ó. J. Palacio, L. Solanilla, *El Teorema de Abel para la Lemniscata*, 2010, Revista Ingenierías Universidad de Medellín, vol. 9, No. 17, pp. 207-214, http://www.scielo.org.co/pdf/rium/v9n17/v9n17a18.pdf.

[5] H. Huzita, *Axiomatic development of origami geometry*, 1989, Proceedings of the First International Meeting of Origami Science and Technology, pp. 143-158.

[6] C. M. Jaramillo , Z. M. Santa, *Aplicaciones de la geometría del doblado de papel a las secciones cónicas*, 2010, Revista Virtual Universidad Católica del Norte, No. 31, pp. 338-362, http://revistavirtual.ucn.edu.co/index.php/RevistaUCN/article/download/48/105.

[7] G.E. Martin, *Geometric Constructions*, Springer, 1998.

[8] S. Mayer, *The trascendence of* π, 2006, 3 pages, http://sixthform.info/maths/files/pitrans.pdf.

[9] P. Puig Adam, *Curso de Geometría Métrica, Tomo I: Fundamentos*, Euler Editorial SA, 1986, 372 pages.

[10] I. Stewart, *Galois Theory*, Chapman & Hall - CRC mathematics, 2003, 3rd edition.

Galois Theory behind origami

Alberto García Díaz
Facultad de Ciencias · Sección de Matemáticas
Universidad de La Laguna
alu0100013283@ull.edu.es

1. Abstract

Origami solves the imposibility of making some geometric constructions from Ancient Greece using a non-marked straightedge and a compass. This is the motivation to look for an explanation of this fact where Group and Galois theories hidden behind this oriental paper folding art are the key.

2. Constructions with straightedge and compass

2.1 Axioms

If we denote by $\alpha, \beta, \gamma \in \mathbb{C}$ some different points, $\ell_1, \ell_2 \subset \mathbb{C}$ some different lines and $\mathcal{C}_1, \mathcal{C}_2 \subset \mathbb{C}$ some different circles in the complex plane, we can postulate these axioms:

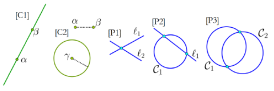
C1. Given α, β, we can trace the only line ℓ_1 which joins them.

C2. Given α, β, γ, we can trace the circle with center on γ and radius $|\alpha - \beta|$.

P1. Given ℓ_1, ℓ_2, we can plot the only intersection point $\ell_1 \cap \ell_2$.

P2. Given ℓ_1 and $\mathcal{C}_1$, we can plot one or two intersection points, when $\ell_1 \cap \mathcal{C}_1 \neq \emptyset$.

P3. Given $\mathcal{C}_1, \mathcal{C}_2$, we can plot one or two intersection points, when $\mathcal{C}_1 \cap \mathcal{C}_2 \neq \emptyset$.



2.2 Constructible numbers

The constructible numbers with straightedge and compass are all numbers we can construct beginning with 0 and 1 and aplying the five axioms from Section 2.1. We note this set by $\mathscr{C}$.

2.3 Properties

Theorem

- $(\mathscr{C}, +, *)$ is a subfield of $\mathbb{C}$.
- $\mathscr{C}$ is the least field that contains $\sqrt{\alpha}$, for all $\alpha \in \mathscr{C}$.
- All roots of $p(x) = 0$, with $\deg(p) \leq 2$, are elements from $\mathscr{C}$.

2.4 Relation to Galois Theory

Theorem

Let $\alpha \in \mathbb{C}$. Then $\alpha \in \mathscr{C}$ if, and only if, it exists a tower of fields $\mathbb{Q} = K_0 \subset K_1 \subset \cdots \subset K_n \subset \mathbb{C}$, where $\alpha \in K_n$ and $[K_i : K_{i-1}] = 2$, for every $i = 1, ..., n$.

As a consequence:

Corollary

Let $\alpha \in \mathscr{C}$ and L the splitting field for $\text{Irr}(\alpha, \mathbb{Q})$. Then $[L : \mathbb{Q}] = 2^m$, for any $m \in \mathbb{Z}, m \geq 0$.

2.5 Limitations with straightedge and compass

- We can not trisect an arbitrary angle. For example, if we try to divide $\theta = 2\pi/3$ in three same parts, this is equivalent to consider the ninth primitive root of the unit, $\xi_9 = \exp(2\pi i/9)$, to be a constructible number. But $\text{Irr}(\xi_9, \mathbb{Q}) = x^6 + x^3 + 1$, so $[\mathbb{Q}(\xi_9) : \mathbb{Q}] = 6 \neq 2^m$, for all non-negative integer m. So $\xi_9 \notin \mathscr{C}$.
- We can not duplicate a cube of volume V. This is equivalent to trace the edge of a cube with $2V$ volume. It is possible iff $\alpha = \sqrt[3]{2} \in \mathscr{C}$. But $\text{Irr}(\alpha, \mathbb{Q}) = x^3 - 2$. So $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3 \neq 2^m$, and $\alpha \notin \mathscr{C}$.
- We can not square a circle with area A. This is equivalent to trace the side of a square with area A. It is possible iff $\sqrt{\pi} \in \mathscr{C}$. But π is a trascendental number, so we can not find a polynomial $p \in \mathbb{Q}[x]$ which $p(\pi) = 0$. Then $\pi \notin \mathscr{C}$.

3. Constructions with origami

3.1 Axioms

If we denote by $\alpha, \beta \in \mathbb{C}$ some different points, ℓ_1, ℓ_2 some different foldings, we can postulate these six axioms:

O1. Given α, β, we can make the fold ℓ where they lie.

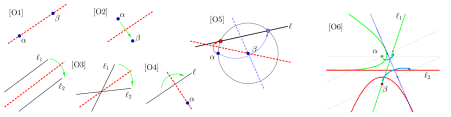
O2. Given α, β, we can make fold which moves α on β.

O3. Given ℓ_1, ℓ_2, we can make one or two folds that moves ℓ_1 on ℓ_2.

O4. Given ℓ_1 and α, we can make the fold that moves α on ℓ_1.

O5. Given ℓ_1 and $\alpha, \beta \notin \ell_1$, we can make one or two folds which moves α and β on ℓ_1.

O6. Given ℓ_1, ℓ_2 and $\alpha \in \mathbb{C} \setminus \ell_1, \beta \in \mathbb{C} \setminus \ell_2$, we can make a maximum of three folds that moves α on ℓ_1 and β on ℓ_2.



Axioms O1-O5 are equivalent to axioms from Section 2.1.

3.2 Constructible numbers

The constructible numbers with origami are all numbers we can construct beginning with 0 and 1 and aplying the six axioms from Section 3.1. We note this set by $\mathscr{O}$.

3.3 Properties

Theorem

- $(\mathscr{O}, +, *)$ is a subfield of $\mathbb{C}$.
- $\mathscr{O}$ is the least field that contains $\sqrt{\alpha}$ and $\sqrt[3]{\alpha}$, for all $\alpha \in \mathscr{O}$.
- All roots of $p(x) = 0$, with $\deg(p) \leq 4$, are elements from $\mathscr{O}$.

3.4 Relation to Galois Theory

Theorem

Let $\alpha \in \mathbb{C}$. Then $\alpha \in \mathscr{O}$ if, and only if, it exists a tower of fields $\mathbb{Q} = K_0 \subset K_1 \subset \cdots \subset K_n \subset \mathbb{C}$, where $\alpha \in K_n$ and $[K_i : K_{i-1}] \in \{2, 3\}$, for every $i = 1, ..., n$.

As a consequence:

Corollary

Let $\alpha \in \mathscr{O}$ and L de splitting field for $\text{Irr}(\alpha, \mathbb{Q})$. Then $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2^m \cdot 3^n$, for any $m, n \in \mathbb{Z}, m, n \geq 0$.

3.5 Breaking limitations from Straightedge and compass

- We can trisect any angle with origami using the axiom O6.
- We can duplicate the cube with origami. This is equivalent to consider $\alpha = \sqrt[3]{2} \in \mathscr{O}$. But $\text{Irr}(\alpha, \mathbb{Q}) = x^3 - 2$. So $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3 = 2^0 \cdot 3$, then $\alpha \in \mathscr{O}$.

3.6 Limitations

- We can not square the circle with origami because π is a trascendental number, then $\pi \notin \mathscr{O}$.

4. Conclusions

Thanks to origami we got a practical way to solve some of the geometrical problems that Ancient Greek could not solve. There are origami constructions to build the solutions for polynomial equations $p(x) = 0$, when $\deg(p) \leq 4$, and Galois Theory discard the existence of constructible roots when $\deg(p) \geq 5$. So, any algebraical root of a polynomial can be constructed with origami.

References

[1] Carter, B., Shurman, J., *Folding Quartic Roots (2001)*.

[2] Cox, D., *Galois Theory (2012)*, Wisley.

[3] Hatori, K. *Origami Constructions (2003)*.

[4] Santa, Z., Jaramillo, C., *Aplicaciones de la geometría del doblado de papel a las secciones cónicas*.

DEGREE THESIS. July, 2017.