Números Constructibles

Francisco Nieto Rueda

Números Constructibles

Francisco Nieto Rueda

Memoria presentada como parte de los requisitos para la obtención del título de Grado en Matemáticas por la Universidad de Sevilla.

Tutorizada por

Manuel Jesus Gago Vargas

Índice general

English Abstract / Resumen

The main goal in this work is the comparison between the classical methods of drawing a figure using straight edge and compass and a new approach that uses folding a paper. These new numbers are called origami numbers, which allow us trisect an angle and duplicate the cube. We compare too the conditions for a regular polygon to be constructed, based on theorems from Galois Theory.

El objetivo del trabajo es la comparativa entre las construcciones clásicas mediante regla y compás y las que se obtienen con la adicion de un tipo de plegado que da lugar a los números origami. Mediante estos últimos es posible la construcción de la trisección del angulo y de la duplicación del cubo, así como ampliar el conjunto de polígonos regulares que se pueden obtener con estas nuevas operaciones. Las demostraciones implican el uso de conceptos procedentes de la teoría de Galois.

Introducción

Un número constructible es un número que puede ser obtenido en base a unas operaciones permitidas. Las construcciones con regla y compás han sido el método de construcción más utilizado y conocido en toda la historia y es en lo que nos centraremos en la primera parte de nuestro trabajo. Estas creaciones siguen siendo muy importantes en la actualidad en especial para la geometría y el dibujo. En un principio veremos qué elementos podemos elaborar con movimientos de regla y compás, como pueden ser la bisección del angulo y la perpendicular a una recta para luego formalizar qué operaciones son permitidas y qué puntos iniciales tomamos.

La formalización de los puntos es importante ya que elaboraremos una base con la que poder trabajar sobre los números que consideraremos constructibles. Un ejemplo será la obtención de rectas a partir de puntos constructibles ya que la intersección de estas resultara en puntos también constructibles.

Con la idea en mente de expandir el número de puntos constructibles que podemos conseguir con los movimientos de regla y compás le damos estructura de cuerpo al conjunto de números constructibles de forma que podemos saber si un número es o no constructible en base a su valor sin tener que ser representado gráficamente ni obtenerlo desde cero. También veremos cadenas de extensiones de cuerpos y algunos corolarios que nos ayudarán a poder discernir mas fácilmente si un número es constructible.

La teoría de Galois también nos será útil para localizar números constructibles ya que estudiando el polinomio mínimo de una raíz α podremos saber si dicha raíz es constructible. En concreto podremos ver que siendo L el cuerpo de descomposición del polinomio mínimo de α sobre $\mathbb{Q}$, si $[L:\mathbb{Q}]$ es una potencia de 2 entonces α será constructible.

Con todo esto estaremos preparados para ver si un polígono regular es o no constructible por regla y compás. Para ello nos ayudaremos de los primos de Fermat. Estos primos tienen la característica principal de que pueden ser escritos de la forma $p = 2^{2^m} + 1$ con $m \geq 0$. A pesar de haber pocos primos de esa forma resultan muy útiles para nuestro cometido ya que sabremos si un polígono de n lados es constructible viendo si se puede expresar de la forma $n = 2^s p_1 \cdots p_r$, con $s \geq 0$ un entero y $p_1, \ldots, p_r$ primos de Fermat distintos.

Ademas podremos comprobar si el resultado de algunos problemas clásicos son constructibles como puede ser la trisección del angulo o la duplicación del cubo donde podremos ver los primeras limitaciones de la regla y el compás. Aquí es donde entra la parte de Origami.

El Origami es un arte originado en Asia que consiste en realizar pliegues en una hoja de papel. Aunque pueda parecer algo sin importancia en un campo como el de las matemáticas es un potente método de construcción para la geometría. Uno de los matemáticos que más ha aportado a este campo ha sido Robert J. Lang del cual hablaremos mas adelante.

Lo primero que veremos será algo que para regla y compás es imposible que es la trisección del angulo. Veremos paso a paso cómo conseguir la trisección de un angulo dado mediante origami (puede verse aquí:`https://youtu.be/Q8AphvZ2UPU`). Esto nos será útil para la inclusión de un nuevo axioma a los usados en regla y compás el cual nos permite expandir el conjunto de números constructibles. Al igual que para el caso de regla y compás veremos qué nos aporta este nuevo axioma a la estructura de cuerpo ya que podremos construir un nuevo cuerpo que nos permitirá cosas como por ejemplo la construcción del heptágono que para solo regla y compás es imposible.

La teoría de Galois también hará aparición aquí para clasificar los números de origami ya que siendo L el cuerpo de descomposición del polinomio mínimo de α sobre $\mathbb{Q}$, si $[L : \mathbb{Q}] = 2^a 3^b$ para $a, b \geq 0$ enteros entonces α será un número de origami.

Es fácil ver que el añadido es grande y lo primero que veremos será qué polígonos regulares podemos construir con el añadido. Para el caso de origami nos ayudaremos de los primos de Pierpont, primos que pueden ser construidos de la forma $p = 2^u 3^v + 1$ con u y v no negativos. Igual que lo hacían los primos de Fermat para el caso de regla y compás estos lo harán para Origami sabiendo si un polígono regular de n lados será o no constructible. Basta ver si n se puede expresar de la forma $n = 2^a 3^b p_1 p_2 \cdots p_s$, donde $a, b \geq 0$ y $p_1, \ldots, p_s$ son primos de Pierpont distintos.

También veremos los avances en los problemas clásicos ya que aunque vemos el caso de la trisección al principio faltarían otros por ver como la duplicación el cubo.

Ademas veremos brevemente otras formas de obtener los números de origami como son la regla marcada y la intersección de cónicas. La regla marcada no es más que una regla con dos marcas que indican la medida de una unidad. Esto nos permite transportar dicha medida a cualquier lugar y obtener elementos que con una regla normal sería imposible. La intersección de cónicas también nos aportarán nuevos números constructibles intersecando cónicas cuyos coeficientes sean números reales ya obtenidos entre ellas o con una recta. También llegaremos a la conclusión de que las construcciones de origami serán las mismas que las de estos dos métodos por teoremas de caracterización.

Para finalizar hablaremos de los axiomas de Lang. Aunque se aleja un poco del interés del trabajo ya que Lang en este caso solo trabaja con movimientos de Origami en exclusividad veremos la importancia de qué axiomas se toman a la hora de exponer si un elemento es constructible así como cuales son los axiomas que Lang expone para la obtención de elementos constructibles por origami exclusivamente.

Preliminares

Veamos algunos resultados que nos serán útiles a lo largo de todo el trabajo

Definición 0.1. *Un grupo es un par* $(G, *)$*, donde* G *es un conjunto no vacío y* $*$ *es una operación binaria interna*

$$\begin{array}{rccc} * : & G \times G & \longrightarrow & G \\ & (a,b) & \longmapsto & a * b \end{array}$$

que cumple las siguientes propiedades:

1. *Propiedad asociativa:* $(a * b) * c = a * (b * c)$ *para todo* $a \in G$.
2. *Elemento neutro: existe un* $\epsilon \in G$ *tal que* $a * \epsilon = \epsilon * a = a$ *para todo* $a \in G$.
3. *Elemento inverso: para todo* $a \in G$ *existe un elemento* $\tilde{a} \in G$*, llamado el inverso de* a *tal que* $a * \tilde{a} = \tilde{a} * a = \epsilon$.

Ademas, el grupo G *se dice abeliano si cumple la propiedad conmutativa:* $a * b = b * a$ *para todos* $a, b \in G$.

Definición 0.2. *Sea* $(G, *)$ *un grupo. Un subconjunto no vacío* $H \subset G$ *es un subgrupo de* G *si* $(H, *)$ *es un grupo. En este caso escribiremos* $H \leq G$.

Teorema 0.1. ***Teorema de Lagrange****: Dado un grupo finito* G *y un subgrupo* $H \leq G$*, entonces* $|H|$ *divide a* $|G|$.

Definición 0.3. *Un subgrupo* $H \leq G$ *se dice normal, y se denotará* $H \lhd G$*, si* $a * H = H * a$ *para todo* $a \in G$.

Definición 0.4. *Un grupo se dice resoluble si existe una serie finita de subgrupos*

$$\epsilon = G_0 \leq G_1 \leq \cdots \leq G_n = G$$

tal que

1. $G_i \lhd G_{i+1}$ *para* $i = 0, \ldots, n-1$.
2. G_{i+1}/G_i *es abeliano para* $i = 0, \ldots, n-1$.

Definición 0.5. *Un cuerpo K es una terna $(K, +, \bullet)$ tal que verifica:*

1. $(K, +)$ *es grupo abeliano*
2. $(K, \bullet)$ *es un grupo abeliano*
3. *Propiedad distributiva:* $\forall a, b, c \in K : a \bullet (b + c) = a \bullet b + a \bullet c$

Un subcuerpo k de K es un cuerpo contenido K

Definición 0.6. *Un cuerpo K es una extensión del cuerpo k si k es un subcuerpo de K. En este caso, se notará K/k.*

Definición 0.7. *Se llama grado de la extensión K/k a la dimensión de K como $k-$espacio vectorial, denotada $[K : k]$. Diremos que K es una extensión finita de k si $[K : k] < \infty$.*

Teorema 0.2. ***Teorema de extensiones de cuerpos**: Si K/k y L/K son dos extensiones finitas, entonces la extensión L/k también es finita, y se tiene*

$$[L : k] = [L : K] \cdot [K : k]$$

Definición 0.8. *Sea K/k una extensión de cuerpos. Un elemento $\alpha \in K$ se dice algebraico sobre k si existe un polinomio $f \in k[x]$ no nulo tal que $f(\alpha) = 0$. En caso contrario, se dice que α es trascendente sobre k. Si todo elemento de K es algebraico sobre k, diremos que la extensión K/k es algebraica.*

Definición 0.9. *Sea K/k una extensión de cuerpos y $\alpha \in K$ algebraico sobre k. Llamaremos polinomio mínimo de α al polinomio mónico de menor grado que anula a α.*

Definición 0.10. *Sea $f \in k[x]$. Una extensión K/k se dice un cuerpo de descomposición de f sobre k si existen $\alpha_1, \alpha_2, \ldots, \alpha_n \in K$ tales que:*

1. $f(x) = a(x-\alpha_1)(x-\alpha 2)\cdots(x-\alpha_n)$.
2. $K = k(\alpha_1, \alpha_2, \cdots, \alpha_n)$.

Definición 0.11. *Un polinomio $f \in k[x]$ se dice separable si no tiene raíces múltiples en su cuerpo de descomposición. Un elemento de una extensión K/k se dice separable sobre k si su polinomio mínimo sobre k es separable. Una extensión K/k se dice separable si todo elemento de K es separable sobre k.*

Teorema 0.3. ***Teorema del elemento primitivo**. Sea K/k una extensión finita y separable. Entonces existe un elemento $\alpha \in K$ tal que $K = k(\alpha)$. Dicho elemento se llama elemento primitivo de la extensión.*

Definición 0.12. *Dos elementos $\alpha, \beta \in K$ se dicen conjugados si tienen el mismo polinomio mínimo sobre k.*

Teorema 0.4. *Sea K/k una extensión finita. Las condiciones siguientes son equivalentes:*

1. *K es el cuerpo de descomposición de un polinomio $f \in k[x]$.*
2. *Para todo $\alpha \in K$, el polinomio mínimo de α sobre k tiene todas sus raíces en K (es decir, todos los posibles conjugados de α sobre k están en K)*

En tal caso, diremos que la extensión K/k es normal.

Definición 0.13. *Una extensión de cuerpos K/k es una extensión de Galois si es separable y normal. En tal caso, llamaremos grupo de Galois de K/k al grupo de k-automorfismos de K:*

$$G(K/k) = Aut(K/k) = \{\sigma : K \xrightarrow{\cong} K \mid \quad \sigma_{|_k} = Id_k\}$$

Dado un polinomio $f \in k[x]$, su grupo de Galois es el grupo de Galois de su cuerpo de descomposición, si este es separable.

Teorema 0.5. ***(Teorema fundamental de la teoría de Galois)*** *Sea K/k una extensión de Galois, sea $G = \mathrm{Gal}(K/k)$ su grupo de Galois y sea K^H el cuerpo fijo asociado al subgrupo H*

1. *Existe una correspondencia biyectiva entre los subcuerpos de K que contienen a k y los subgrupos de G, dada por:*

$$\begin{array}{ccc} \{\text{Subcuerpos } M | k \subset M \subset K\} & \longleftrightarrow & \{\text{Subgrupos } H | \{id\} \leq H \leq G\} \\ M & \longmapsto & G(K/M) \\ K^H & \longleftarrow & H \end{array}$$

   Esta correspondencia invierte las inclusiones.
2. *La extensión M/k es normal si y solo si el subgrupo $H = G(K/M)$ es normal en G. Y en este caso, el grupo de Galois $G(M/k)$ es isomorfo al cociente G/H. Es decir:*

$$G(K/k)/G(K/M) \cong G(M/k).$$

3. *Para todo subcuerpo M, si denotamos $H = G(K/M)$, se tiene:*

$$[K : M] = |H|, \qquad [M : k] = \frac{|G|}{|H|}.$$

Proposición 0.1. Sea K el cuerpo de descomposición de un polinomio en $F[x]$, y supongamos que $h \in F[x]$ es irreducible y tiene las raíces $\alpha, \beta \in K$. Entonces existe el isomorfismo $\sigma : K \to K$ que es la identidad en F y va de α a β.

Definición 0.14. *Dado un entero positivo n, se define la función $\phi(n)$ de euler como el número de enteros positivos menores o iguales a n y coprimos con n, es decir*

$$\phi(m) = |\{n \in \mathbb{N} | n \leq m \wedge mcd(m, n) = 1\}|$$

Lema 0.1. Sea ϕ la función definida anteriormente.

1. Si n y m enteros son coprimos, entonces $\phi(nm) = \phi(n)\phi(m)$.
2. Si $n > 1$ es un entero, entonces

$$\phi(n) = n \prod_{p|n} (1 - \frac{1}{p}),$$

   donde el producto es sobre todos los primos p que dividen a n

Corolario 0.1. Sea $\zeta_n = e^{2\pi/n}$ la raíz n-ésima primitiva de la unidad. Entonces se tiene $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \phi(n)$.

1 Construcciones Geométricas básicas

A lo largo del trabajo usaremos técnicas básicas de construcción de elementos geométricos como por ejemplo la bisección del angulo. Aquí expondremos la construcción de algunos de estos elementos por diferentes métodos básicos que nos ayudarán en los siguientes capítulos. Los métodos usados serán regla y compás, donde los métodos son muy conocidos, y Origami, donde no lo son tanto.

1.1 Bisección del angulo

Regla y compás: Sean r y s dos rectas $r \neq s$ que se cortan en un punto γ. Trazamos una circunferencia de radio $|\alpha| > 0$ y centro γ que corta a las rectas en los puntos R y S respectivamente. Luego trazamos dos circunferencias de mismo radio y centros R y S. La recta que une los dos puntos de corte de las dos ultimas circunferencias será la recta que divide el angulo en dos. La construcción aparece en la figura 1.1.

Origami: Sean r y s dos rectas $r \neq s$ que se cortan en un punto γ. Doblamos el papel de forma que las rectas se superpongan (trivialmente pasaremos por el punto γ). La recta generada por el doblez es la que divide el angulo en dos. La construcción aparece en la figura 1.2.

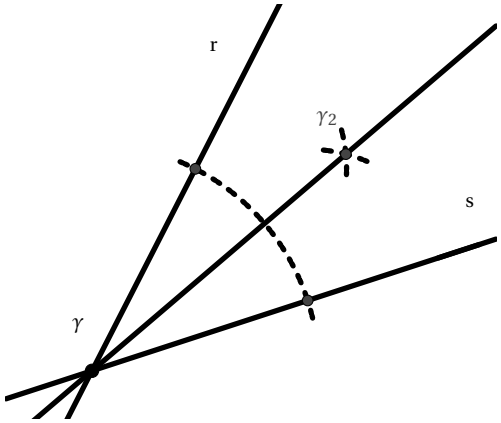


Figura 1.1: Bisección del angulo

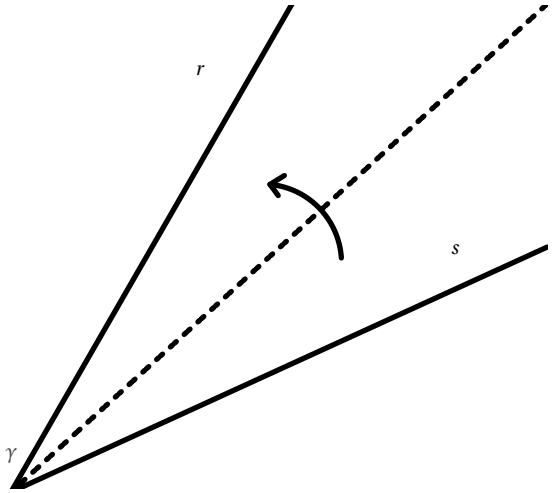


Figura 1.2: Bisección del angulo (Origami)

1.2 Perpendicular a una recta en un punto

Regla y compás: Sea r una recta y γ un punto de ella. Trazamos la circunferencia de centro el punto y radio $\alpha > 0$. La intersección con la recta nos da dos puntos R y S. Ahora hacemos las circunferencias de radio $d(R,S)$ y de centro R y otra del mismo radio de centro S. La recta que se forma con la unión de los puntos de intersección de las circunferencias es perpendicular a la recta pasando por γ. La construcción aparece en la figura 1.3.

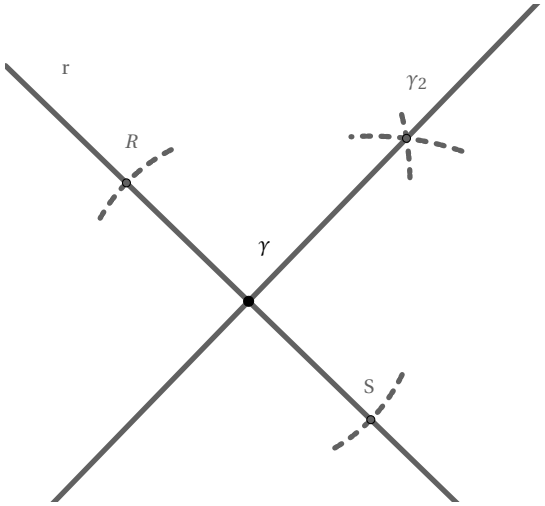


Figura 1.3: Perpendicular a una recta en un punto

Origami: A partir de la recta y el punto γ contenido en ella basta con superponer la recta consigo misma a través de un plegado del papel dejando el punto γ dentro de la recta que se genera al haber doblado dicho papel. La recta generada es la perpendicular a γ. La construcción aparece en la figura 1.4.

1.3 Paralela a una recta que pasa por un punto

Regla y compás: Sea r la recta y γ el punto por el que pasará la paralela. Primero hacemos una circunferencia de centro γ y radio $\alpha > 0$ tal que la recta r corte a la circunferencia. Luego a partir del punto de corte, que llamaremos γ_2, con el mismo radio trazamos la circunferencia que pasa por γ y corta la recta en γ_3. Ahora trazamos otra circunferencia de centro γ_3 y radio $d(\gamma_2, \gamma_3)$ y llamaremos γ_4 al punto de corte de esta circunferencia con con la primera circunferencia que hicimos. La recta que pasa por γ y γ_4 será nuestra paralela. La construcción aparece en la figura 1.5.

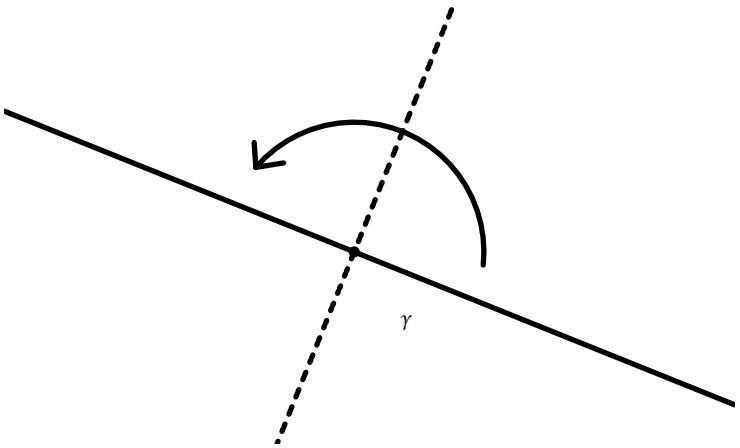


Figura 1.4: Perpendicular a una recta en un punto (Origami)

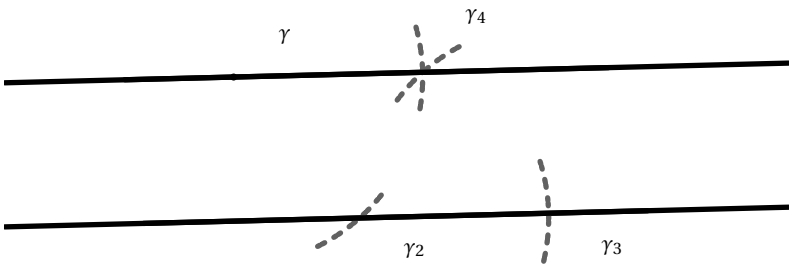


Figura 1.5: Paralela a una recta que pasa por un punto

Origami: Sea r la recta y γ el punto. El método mas fácil para el calculo de la paralela no es mas que usar el método de calculo de perpendiculares dos veces. Calculas la perpendicular que pasa por γ y luego otra perpendicular a la anterior que pase por γ de nuevo. Con esto tendremos la recta paralela. La construcción aparece en la figura 1.6.

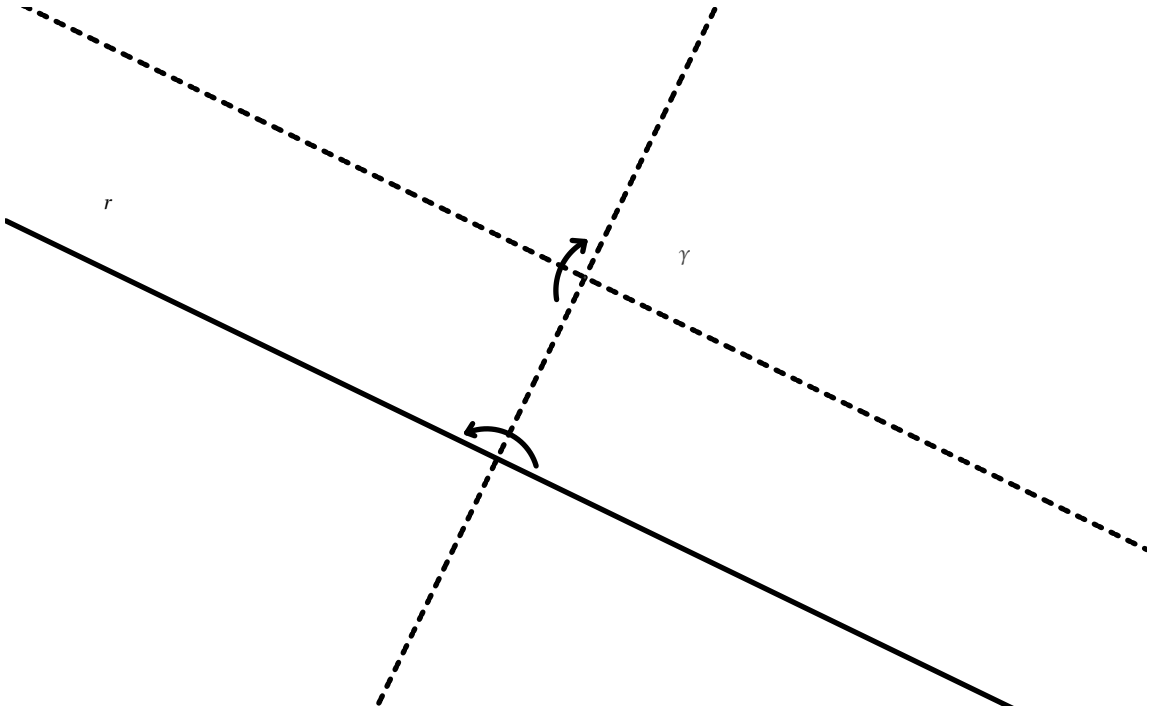


Figura 1.6: Paralela a una recta que pasa por un punto (Origami)

2 Regla y Compás

La idea de hacer construcciones geométricas usando regla y compás se remonta a los antiguos griegos (en el caso de no mencionarlo nos referiremos siempre a la regla no marcada). En este capitulo veremos la formalización de las operaciones permitidas así como la conexión existente entre la teoría de Galois y dichas construcciones geométricas.

2.1 Operaciones permitidas

Antes hemos podido ver construcciones básicas de regla y compás como puede ser la bisección del angulo o la perpendicular a una recta dada pero para probar teoremas sobre construcciones geométricas debemos tener cuidado describiendo qué es una construcción.

La idea es empezar con algunos puntos conocidos y, a partir de estos, caracterizar los que podemos construir. Teniendo en cuenta que a partir de la regla podemos construir la linea que une dos puntos y que con el compás podemos construir círculos a partir de un radio conocido (que puede ser la distancia entre dos puntos) es intuitivo que las primeras construcciones sean las siguientes:

C1. Con $\alpha \neq \beta$, podemos dibujar la recta l que une α y β.

C2. Con γ y $\alpha \neq \beta$, podemos dibujar un círculo C de centro γ y radio la distancia de α a β.

Ademas, a partir de estas construcciones, podemos construir nuevos puntos con la intersección de estos:

P1. El punto de intersección de dos rectas $l_1,\ l_2$ construidas por C1.

P2. Los puntos de intersección de la recta l de C1 y la circunferencia C de C2.

P3. Los puntos de intersección de dos circunferencias C_1, C_2 construidas por C2.

De modo que a partir de dos puntos iniciales y una secuencia de C1, C2, P1, P2 y P3 podremos obtener un conjunto de puntos. Para nosotros, el plano será el conjunto de los números complejos $\mathbb{C}$ y los dos puntos iniciales serán 0 y 1.

2.2 Números constructibles

Definición 2.1. *Un número complejo α es constructible si se puede construir con una secuencia finita de construcciones con regla y compás usando C1, C2, P1, P2 y P3 tal que comenzando con 0 y 1 podemos construir α.*

Ejemplo 2.1. Desde 0 y 1 podemos obtener el eje x usando C1 y la circunferencia de radio 1 centrada en 1 usando C2. Esta interseca en los números 0 y 2. Por P2, 2 es constructible. La iteración de esto resulta en que todo $n \in \mathbb{Z}$ es constructible.

Una vez formalizadas los operaciones permitidas necesitaremos formalizar las construcciones básicas vistas anteriormente.

Ejemplo 2.2. **Bisectriz:** Sean r y s dos rectas $r \neq s$ que se cortan en un punto γ. Por C2 trazamos una circunferencia de centro γ y radio $|\alpha| > 0$. Por P2 la intersección de la circunferencia con las rectas nos dan los puntos R y S. Ahora por C2 trazamos las circunferencias de centro R y S con mismo radio. La intersección de ambas circunferencias, por P3, será un punto constructible y por tanto podemos obtener la bisectriz.

Ejemplo 2.3. **Perpendicular:** Sea r una recta y γ un punto de ella. Por C2 trazamos la circunferencia de radio $\alpha > 0$ y centro γ. Por P2 la intersección de la circunferencia y la recta nos da los puntos R y S. Ahora por C2 trazamos las circunferencias de radio $d(R,S)$ y centro R y S. Los puntos generados por la intersección de circunferencias, por P3, son constructibles. Por tanto se puede obtener la perpendicular a una recta en un punto ya que la recta que une dichos puntos es dicha perpendicular.

Ejemplo 2.4. **Paralela:** Sea r la recta y γ el punto por el que pasará la paralela. Por C2 trazamos la circunferencia de centro γ y radio $\alpha > 0$ tal que la recta r corte a la circunferencia. Por P2 dicha intersección nos dará el punto γ_2. Por C2 nuevamente trazamos la circunferencia de centro γ_2 y radio α.Por P2 la intersección de la circunferencia anterior y la recta nos da el punto γ_3.

Ahora por C2 trazamos la circunferencia de centro γ_2 y radio $d(\gamma_2,\gamma_3)$. El punto generado por la intersección de esta circunferencia y la primera que hicimos, por P3, es constructible. Por tanto se puede obtener la paralela a una recta que pase por un punto ya que es la recta que une γ con γ_4.

2.3 Estructura de cuerpo

Teorema 2.1. *El conjunto* $\mathscr{C} = \{\alpha \in \mathbb{C} \mid \alpha \text{ es constructible}\}$ *es un subcuerpo de* $\mathbb{C}$. *Ademas:*

1. *Sea* $\alpha = a + ib \in \mathbb{C}$, *donde* $a, b \in \mathbb{R}$. *Entonces* $\alpha \in \mathscr{C}$ *si y solo si* $a, b \in \mathscr{C}$.
2. *Si* $\alpha \in \mathscr{C}$ *entonces* $\sqrt{\alpha} \in \mathscr{C}$

Demostración. Primero vamos a probar que $\mathscr{C}$ es un subgrupo para la suma. Tomamos $\alpha \in \mathscr{C} - \{0\}$ y construimos la recta que conecta el 0 con α mediante C1 y el círculo de radio $|\alpha|$ centrado en el origen mediante C2. Como esto interseca en $\pm\alpha$,el número $-\alpha$ es constructible por P2.

Supongamos ahora que α y β son constructibles. Si α, β y 0 no son colineales entonces usamos C2 dos veces para construir la circunferencia de radio $|\alpha|$ con centro el punto β y la circunferencia de radio $|\beta|$ con centro α. La intersección de ambas circunferencias es $\alpha + \beta$:

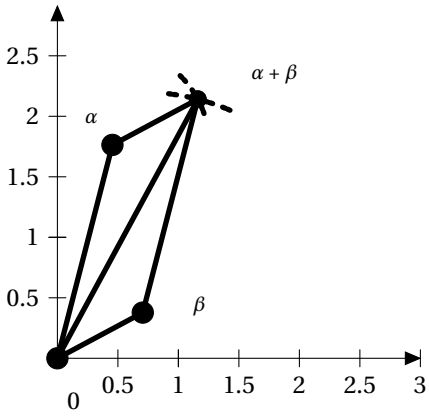


Figura 2.1: Suma de α y β

Por P3, podemos concluir que $\alpha+\beta$ es constructible. Si α, β y 0 estuvieran alineados basta con construir mediante C2 la circunferencia de radio $|\beta|$ y centro α. La intersección de la circunferencia y la recta que conecta los tres puntos nos da $\alpha+\beta$ que por P2 es constructible. Como $0 \in \mathscr{C}$ por definición, se tiene que $\mathscr{C}$ es un subgrupo de $\mathbb{C}$ para la suma.

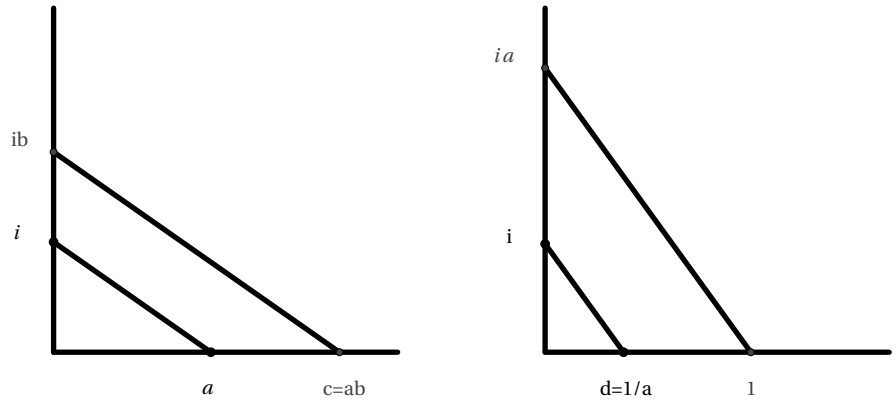
Probemos ahora el apartado (a). Veamos primero la constructibilidad de los ejes X e Y.

Ambos ejes son constructibles ya que una vez tienes el eje X, construido en el ejemplo anterior, también puedes obtener el eje Y con el método de construcción de perpendiculares a una recta ejemplo 2.3 (pág.18). Por lo tanto el eje Y es constructible.

Dado $\alpha = a + ib \in \mathscr{C}$, podemos trazar perpendiculares desde α hasta el eje X y el eje Y. Esto prueba que tanto a como $ib \in \mathscr{C}$. Como el círculo de radio $|i\beta|$ centrado en 0 interseca el eje X con b, C2 y P2 implican que $b \in \mathscr{C}$.

En el otro sentido, dados $a, b \in \mathscr{C} \cap \mathbb{R}$, aplicando C2 y P2 al círculo de radio $|b|$ centrado en 0 nos da que ib es constructible y como ya hemos demostrado que la suma de dos elementos constructibles es constructible, se tiene la prueba de (a).

Ahora tomamos $a, b \in \mathscr{C} \cap \{x \in \mathbb{R} \mid x > 0\}$ y consideramos las siguientes figuras:



Teniendo el eje Y basta hacer la intersección de la circunferencia de centro 0 y radio 1 con el eje para tener $\pm i$, constructible por P2 tenemos que i es constructible. Entonces construimos ib como vimos anteriormente y después usamos C1 para dibujar la recta l que contiene los puntos i y a. Ahora trazamos la paralela a l que pasa por ib por el método de construcción de paralelas ejemplo 2.4 (pág.18) y la llamaremos l'. Entonces por P1 tenemos que l' y el eje X intersecan en un número constructible que llamaremos c, y ademas como $c = ab$ se tiene que ab es constructible. Siguiendo la misma estrategia se puede ver que $1/a$ es constructible.

Para probar que $\mathscr{C}$ es cerrado para la multiplicación y poder tomar los inversos de elementos distintos de cero tomamos $\alpha = a + bi$ y $\beta = c + di$ números constructibles. Entonces:

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

Ademas $a, b, c, d \in \mathscr{C} \cap \mathbb{R}$ por el apartado 1 (pág.19), por lo tanto $ac - bd, ad + bc \in \mathscr{C} \cap \mathbb{R}$. Usando el apartado 1 de nuevo podemos concluir que $\alpha\beta \in \mathscr{C}$. Ademas, si $\alpha \neq 0$ entonces

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

Usando el apartado 1 (pág.19) y que $\mathscr{C} \cap \mathbb{R}$ es un subgrupo de $\mathbb{R}$ se tiene que $\frac{1}{\alpha} \in \mathscr{C}$ y por tanto $\mathscr{C}$ es un subcuerpo de $\mathbb{C}$.

Finalmente vamos a demostrar que $\sqrt{\alpha}$ es constructible cuando α lo es. Asumiremos que $\alpha \neq 0$. Si escribimos $\alpha = re^{i\phi}$, $r = |\alpha| > 0$ basta probar que $\sqrt{r}e^{\frac{i\phi}{2}}$ es constructible. Para probar esto usaremos que implica el hecho de que α sea constructible:

1. Primero, usando el eje X y la recta que contiene el 0 y α (por C1), podemos construir el ángulo ϕ, al cual le podemos calcular la bisectriz por el método visto 2.2 (pág.18). Por tanto el ángulo $\frac{\phi}{2}$ es constructible.
2. Segundo, el círculo de radio $r = |\alpha|$ centrado en el 0 (por C2) interseca al eje X en $\pm r$. Por P2, r es constructible.
3. Tercero, si podemos construir $\sqrt{r}$, podemos construir el círculo de radio $\sqrt{r}$ centrado en el origen por C2. Entonces aplicando P2 a dicho círculo y al ángulo $\frac{\phi}{2}$ (construido anteriormente) implica que $\sqrt{r}e^{\frac{i\phi}{2}}$ es constructible.

Para estudiar $\sqrt{r}$, tomamos $r > 0$ constructible y definimos el punto β con el diagrama siguiente:

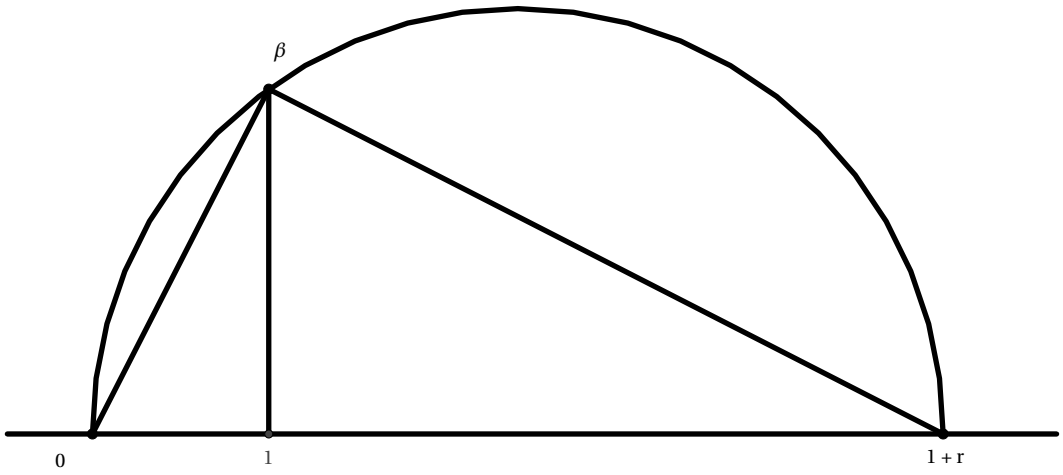


Figura 2.2: Raíz de π

β, la intersección de la recta $x = 1$ con la semicircunferencia, es constructible ya que si r lo es $r + 1$ también lo es por ser la suma de dos puntos constructibles asi que calculando el punto medio de 0 y $r + 1$ por C2 se tiene la constructibilidad. Por geometría euclídea, el triangulo de vértices 1, β y $1 + r$ es un triangulo rectángulo. Los dos triángulos separados por la recta que va de 1 a β son semejantes. Por tanto

$$\frac{1}{d} = \frac{d}{r}, \tag{2.1}$$

donde d es la distancia de 1 a β. Asi que $d^2 = r$ y $d = \sqrt{r}$. Como d es constructible se tiene que $\sqrt{r}$ es constructible como queríamos probar.

Ejemplo 2.5. Tomemos por ejemplo la raíz quinta de la unidad $\zeta_5 = e^{2\pi i/5}$ dada por la formula:

$$\zeta_5 = \frac{-1+\sqrt{5}}{4} + \frac{i}{2}\sqrt{\frac{5+\sqrt{5}}{2}}.$$

Como $\mathscr{C}$ es cerrado para las raíces cuadradas, se tiene que ζ_5 es constructible. Más adelante veremos la relación que tiene $\zeta_n = e^{2\pi i/n}$ con el estudio de la constructibilidad de polígonos regulares ya que con esto tendríamos la constructibilidad del pentágono.

2.4 Relación con extensiones de cuerpo

Llamaremos $\mathscr{C}$ al cuerpo de los números constructibles. Estudiemos primeramente la estructura de $\mathscr{C}$.

Teorema 2.2. *Sea α un número complejo. Entonces $\alpha \in \mathscr{C}$ si y solo si se tiene la siguiente la cadena de subcuerpos:*

$$\mathbb{Q} = F_0 \subset F_1 \subset \ldots \subset F_n \subset \mathbb{C}$$

tal que $\alpha \in F_n$ y $[F_i : F_{i-1}] = 2$ para $1 \leq i \leq n$.

Demostración. Primero supongamos que tenemos $\mathbb{Q} = F_0 \subset F_1 \subset \ldots \subset F_n \subset \mathbb{C}$ donde $[F_i : F_{i-1}] = 2$. Sabemos que $F_i = F_{i-1}(\sqrt{\alpha_i})$ para algún $\alpha_i \in F_{i-1}$. Vamos a probar que $F_i \subset \mathscr{C}$ por inducción en $0 \leq i \leq n$.

El caso particular de $F_0 = \mathbb{Q} \subset \mathscr{C}$ se tiene ya que $\mathscr{C}$ es un subcuerpo de $\mathbb{C}$. Ahora supongamos que $F_{i-1} \subset \mathscr{C}$. Entonces $\alpha_i \in F_{i-1}$ es constructible, lo que implica $\sqrt{\alpha_i} \in \mathscr{C}$ por el teorema 2.1 (pág.19). Por tanto $F_i = F_{i-1}(\sqrt{\alpha_i}) \subset \mathscr{C}$ como indicábamos. Esto prueba que $F_n \subset \mathscr{C}$ y en particular que $\alpha \in F_n$ es constructible.

Ahora veamos el caso contrario. Dado $\alpha \in \mathscr{C}$, tenemos que crear una sucesión de extensiones cuadráticas que empiecen en $\mathbb{Q}$ y que terminen conteniendo a α. Tenemos que probar que dadas las extensiones $\mathbb{Q} = F_0 \subset F_1 \subset ... \subset F_n \subset \mathbb{C}$ donde $[F_i : F_{i-1}] = 2$ se tiene que F_n contiene la parte real y la parte imaginaria de todos los números constructibles durante el proceso de construcción de α. Entonces hay que probar que si $\alpha = a + bi$ implica que $a + b \in F_n$ y por tanto que $\alpha \in F_n(i)$.

Vamos a probar esto por inducción sobre N que es el número de veces que usamos P1, P2 o P3 en la construcción de α. Cuando $N = 0$, tenemos que α cero o uno, y en ambos casos $F_n = F_0 = \mathbb{Q}$. Ahora supongamos que α es construible en $N > 1$ pasos, donde el ultimo paso usa P1, la intersección de las rectas l_1 y l_2 distintas. Pero entonces l_1 puede construirse usando los puntos α_1 y $\beta_1$distintos usando C1, y l_2 igual a partir de los puntos α_2 y β_2 distintos. Por hipótesis de inducción existen extensiones $\mathbb{Q} = F_0 \subset F_1 \subset ... \subset F_n \subset \mathbb{C}$ donde $[F_i : F_{i-1}] = 2$ tal que F_n contiene la parte real y la parte imaginaria de $\alpha_1, \alpha_2, \beta_1, \beta_2$. Vamos a probar que F_n contiene las partes real e imaginaria de α.

La recta l_1 tiene una ecuación de la forma $a_1 x + b_1 y = c_1$ y pasa por $\alpha_1 \neq \beta_1$. Veamos primero que los coeficientes a_1, b_1 y c_1 están en F_n. Para ello ponemos la ecuación de la recta de la forma $y = -\frac{a_1}{b1} x + \frac{c_1}{b_1}$. Es fácil ver que $-\frac{a_1}{b_1}$ es la pendiente m de la recta y como F_n contiene la parte real e imaginaria de α_1 y β_1, $a_1, b_1 \in F_n$. Sustituyendo uno de los dos puntos y m también se comprueba que $c_1 \in F_n$. De la misma forma l_2 tiene una ecuación de la forma $a_2 x + b_2 y = c_2$ con a_2, b_2 y c_2 en F_n. Por lo tanto la parte real e imaginaria de α forman una única solución de las ecuaciones

$$\begin{cases} a_1 x + b_1 y = c_1, \\ a_2 x + b_2 y = c_2. \end{cases}$$

En esta situación, el álgebra lineal nos indica que la matriz

$$\begin{bmatrix} a_1 & b_1 \\ a_2 & b_2 \end{bmatrix}$$

es invertible, por lo tanto la única solución es

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

Y entonces se tiene que la parte real e imaginaria de α estan en F_n.

Ahora supongamos que el ultimo paso de la construcción de α usa P2, la intersección de una recta l y un círculo C. Asi, l es la recta que pasa por $\alpha_1 \neq \beta_1$ desde C1, y C es el círculo de centro γ_2 y radio $\mid \alpha_2 - \beta_2 \mid$ desde C2. Por lo tanto por la hipótesis de inducción existen las extensiones $\mathbb{Q} = F_0 \subset F_1 \subset ... \subset F_n \subset \mathbb{C}$ donde $[F_i : F_{i-1}] = 2$ tal que F_n contiene la parte real y la parte imaginaria de los cinco puntos $\alpha_1, \alpha_2, \beta_1, \beta_2, \gamma_2$.

Veamos ahora que la parte real e imaginaria de α pertenecen a F_n o a una extensión cuadrática de F_n. Como anteriormente l esta dada por la ecuación

$$a_1 x + b_1 y = c_1 \text{ con } a_1, b_1, c_1 \in F_n \tag{2.2}$$

y C esta dada por la ecuación

$$x^2 + y^2 + a_2 x + b_2 y + c_2 = 0. \tag{2.3}$$

Igual que para el caso de la recta veamos que los coeficientes de la circunferencia $a_2, b_2, c_2 \in F_n$. Sea $(x_1, y_1) = \gamma_2$ y $r = \mid \alpha_2 - \beta_2 \mid$. La ecuación general de una circunferencia de centro γ_2 y radio r es $(x - x_1)^2 + (y - y_1)^2 = r^2$ por tanto los valores a_2, b_2, c_2 salen a partir del producto o la suma de elementos de F_n lo que nos prueba que $a_2, b_2, c_2 \in F_n$.

Supongamos que $a_1 \neq 0$ y dividimos la ecuación 2.2 (pág.25) por a_1 de forma que la recta l estará dada por $x + b_1 y = c_1$. Sustituyendo $x = -b_1 y + c_1$ en la ecuación 2.3 (pág.25) tenemos:

$$(-b_1 y + c_1)^2 + y^2 + a_2(-b_1 y + c_1) + b_2 y + c_2 = 0. \tag{2.4}$$

Por la formula cuadrática, los valores de y implican la raíz cuadrada de una expresión en F_n. Si esta contenido en F_n, entonces hacemos y y $x = -b_1 y + c_1$ y esto prueba que tanto la parte real como la imaginaria de α estan en F_n.

Por otro lado, si esta raíz cuadrada no pertenece a F_n entonces esta contenida en la extensión cuadrática $F_n \subset F_{n+1}$. Entonces y y $x = -b_1 y + c_1$ también pertenecen a F_{n+1}, y por lo tanto la parte real como la imaginaria de α estan en F_n. Cuando $a_1 = 0$ se siguen los mismos pasos.

Finalmente, supongamos que el ultimo paso en la construcción de α usa P3. Como anteriormente, podemos encontrar $\mathbb{Q} = F_0 \subset F_1 \subset ... \subset F_n \subset \mathbb{C}$ donde $[F_i : F_{i-1}] = 2$ y las circunferencias de P3 nos dan las siguientes ecuaciones:

$$x^2 + y^2 + a_1 x + b_1 y + c_1 = 0, x^2 + y^2 + a_2 x + b_2 y + c_2 = 0, \tag{2.5}$$

con todos sus coeficientes perteneciendo a F_n. Ademas, sabemos que las partes reales e imaginarias de α dan una solución para 2.5 (pág.26). Si restamos estas ecuaciones obtenemos:

$$(a_1 - a_2)x + (b_1 - b_2)y + (c_1 - c_2) = 0. \tag{2.6}$$

Mientras los círculos de 2.5 (pág.26) sean distintos pero no disjuntos, se puede ver fácilmente que los coeficientes de x y y en 2.6 (pág.26) no se anulan simultáneamente. Por tanto 2.6 define una recta. Ademas si combinamos esta ecuación con la primera ecuación de 2.5 (pág.26) estaremos en el caso anterior de intersección de una circunferencia y una recta. Por tanto concluimos que tanto la parte real como la imaginaria de α pertenecen a F_n o a una extensión cuadrática de F_n, lo que completa la prueba.

Corolario 2.1. $\mathscr{C}$ es el menor subcuerpo de $\mathbb{C}$ que es cerrado para la operación de tomar raíces cuadradas.

Demostración. Por el teorema 2.1 (pág.19), sabemos que $\alpha \in \mathscr{C}$ implica que $\sqrt{\alpha} \in \mathscr{C}$. Ahora supongamos F un subcuerpo de $\mathscr{C}$ cerrado para raíces cuadradas y supongamos $\alpha \in \mathscr{C}$. Por el teorema 2.2 (pág.23) tenemos que $\mathbb{Q} = F_0 \subset F_1 \subset ... \subset F_n \subset \mathbb{C}$ donde $[F_i : F_{i-1}] = 2$ y $\alpha \in F_n$. El primer apartado de la prueba del teorema 2.2 (pág.23) prueba que $F_n \subset F$. Por tanto $\alpha \in F_n \subset F$, y $\mathscr{C} \subset F$ como queríamos probar.

Corolario 2.2. Si $\alpha \in \mathscr{C}$, entonces $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2^m$ para algún $m \geq 0$. Entonces todo número constructible es algebraico sobre $\mathbb{Q}$ y el grado de su polinomio mínimo sobre $\mathbb{Q}$ es una potencia de 2.

Demostración. Si $\alpha \in \mathscr{C}$ entonces el teorema 2.2 (pág.23) nos da la extensión $\mathbb{Q} = F_0 \subset F_1 \subset ... \subset F_n \subset \mathbb{C}$ donde $[F_i : F_{i-1}] = 2$ y $\alpha \in F_n$; por lo tanto:

$$[F_n : \mathbb{Q}] = [F_n : F_0] = [F_n : F_{n-1}] \cdots [F_1 : F_0] = 2^n,$$

por el Teorema de extensiones de cuerpos. No obstante, seguimos teniendo $\mathbb{Q} \subset \mathbb{Q}(\alpha) \subset F_n$. Usando de nuevo el teorema tenemos que $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ divide a $[F_n : \mathbb{Q}] = 2^n$.

2.5 Problemas clásicos

Veamos ahora cuáles de los problemas clásicos griegos pueden ser resueltos de manera que el resultado sea constructible y cuáles no

Ejemplo 2.6. **Trisección del ángulo**. En el primera sección podemos vimos que es posible calcular la bisección de un ángulo. Vamos a probar que no todo ángulo se puede dividir en tres. Supongamos que podemos dividir en tres un ángulo de 120 grados con regla y compás. Podemos construir un ángulo de 120 grados a partir del 0 y el 1 por lo tanto debemos poder construir un ángulo de 40 grados desde el 0 y el 1. Intersecando esto con la circunferencia unidad centrada en el origen obtenemos las raíces novenas de la unidad $\zeta_9 = e^{2\pi i/9}$ las cuales deben ser constructibles.

$$x^9 - 1 = (x-1)(x^2+x+1)(x^6+x^3+1), \tag{2.7}$$

donde x^6+x^3+1 es el polinomio mínimo de ζ_9, y por el corolario anterior ζ_9 no es constructible. Por tanto, el ángulo de 120 grados no puede ser dividido en tres usando regla y compás y en general un ángulo cualquiera no puede ser dividido en tres.

Ejemplo 2.7. **Duplicación del cubo**. El problema es a partir de un cubo cualquiera construir uno de exactamente el doble de volumen. Tomemos un cubo cuyos lados midan 1 unidad y por tanto volumen 1. Tenemos que construir un cubo de volumen 2. Para ello los lados deben medir $\sqrt[3]{2}$, pero x^3-2 es el polinomio mínimo de $\sqrt[3]{2}$ sobre $\mathbb{Q}$ y por el corolario 2.2 (pág.26) no es constructible. Por tanto, no es posible obtener la duplicación del cubo con regla y compás.

Ejemplo 2.8. **Cuadratura del círculo**. Aquí el problema es construir un cuadrado cuya área es igual a la dada por el círculo. Tomemos el círculo de radio 1 cuya área será π. Los lados del cuadrado de área π medirán $\sqrt{\pi}$ y por tanto podemos construir $\sqrt{\pi}$. Ademas, como el círculo es de radio 1, podemos asumir la construcción a partir de 0 y 1. Asi, la cuadratura del círculo implica que $\sqrt{\pi}$ es constructible.

Como $\mathscr{C}$ es un cuerpo, la constructibilidad de $\sqrt{\pi}$ implica que π es también constructible. Entonces el corolario 2.2 (pág.26) implicaría que π es algebraico sobre $\mathbb{Q}$. Sin embargo en 1882 Lindemann probo que π es trascendente sobre $\mathbb{Q}$.Una prueba de esto puede ser encontrada en [[4], Seccion 1.7]. Esta contradicción prueba que no se puede obtener la cuadratura del círculo con regla y compás.

2.6 Relacion con teoría de Galois

Ahora nos podemos preguntar si el recíproco del corolario anterior es cierto. En otras palabras ver que si se tiene que $\alpha \in \mathbb{C}$ es algebraico sobre $\mathbb{Q}$ y el grado del polinomio mínimo es una potencia de 2, se tiene que α es constructible. El siguiente resultado resolverá esta pregunta.

Teorema 2.3. *Supongamos que $\alpha \in \mathbb{C}$ es algebraico sobre $\mathbb{Q}$ y que $\mathbb{Q} \subset L$ es el cuerpo de descomposición del polinomio mínimo de α sobre $\mathbb{Q}$. Entonces α es constructible si y solo si $[L:\mathbb{Q}]$ es una potencia de 2*

Demostración. Primero supongamos que $[L:\mathbb{Q}]$ es una potencia de 2. Como $\mathbb{Q} \subset L$ es de Galois, $|\operatorname{Gal}(L/\mathbb{Q})| = [L:\mathbb{Q}]$ es una potencia de 2. Por tanto $\operatorname{Gal}(L/\mathbb{Q})$ es resoluble, lo que significa que tenemos los subgrupos

$$\{e\} = G_m \subset G_{m-1} \subset \cdots \subset G_1 \subset G_0 = \operatorname{Gal}(L/\mathbb{Q}) \tag{2.8}$$

con G_i normal en G_{i-1} de indice 2 (ya que $|\operatorname{Gal}(L/\mathbb{Q})| = 2^m$). Esto nos da:

$$\mathbb{Q} = L_{G_0} \subset L_{G_1} \subset \cdots \subset L_{G_m} = L, \text{ donde } [L_{G_i} : L_{G_{i-1}}] = 2 \ \forall i \tag{2.9}$$

Por el Teorema 2.2 (pág.23), $\alpha \in L$ es constructible.

Probemos ahora la otra implicación. Primero probemos que $\mathbb{Q} \subset \mathscr{C}$ es una extensión normal. Para ello fijemos $\alpha \in \mathscr{C}$ y f tal que sea el polinomio mínimo de α sobre $\mathbb{Q}$. Tenemos que probar que todas las raíces de f pertenecen a $\mathscr{C}$. Como α es constructible el teorema 2.2 (pág.23) nos da las extensiones $\mathbb{Q} = F_0 \subset F_1 \subset \ldots \subset F_n \subset \mathbb{C}$ donde $[F_i : F_{i-1}] = 2$ y $\alpha \in F_n$. Entonces $\mathbb{Q} \subset M$ será el cuerpo de descomposición de $\mathbb{Q} \subset F_n$.

Nótese que todas la raíces de f pertenecen a M, ya que M es normal sobre $\mathbb{Q}$, f es irreducible sobre $\mathbb{Q}$, y $\alpha \in F_n \subset M$ es una raíz de f. Ahora sea $\beta \in M$ una raíz de f. Por la proposición 0.1 (pág.10) tenemos que existe $\sigma \in \operatorname{Gal}(M/\mathbb{Q})$ tal que $\sigma(\alpha) = \beta$. Aplicando σ a los cuerpos $\mathbb{Q} = F_0 \subset F_1 \subset \ldots \subset F_n \subset M$ tenemos:

$$\mathbb{Q} = \sigma(\mathbb{Q}) = \sigma(F_0) \subset \cdots \subset \sigma(F_n) \text{ tal que } [\sigma(F_i) : \sigma(F_{i-1})] = [F_i : F_{i-1}] = 2 \ \forall i \tag{2.10}$$

Por el teorema 2.2 (pág.23) $\beta = \sigma(\alpha) \in \sigma(F_n)$ es constructible. Esto prueba que todas la raíces de f pertenecen a $\mathscr{C}$. Por tanto se tiene que $\mathscr{C}$ contiene un cuerpo de descomposición L de f sobre $\mathbb{Q}$. Por el teorema del elemento primitivo, tenemos que $L = \mathbb{Q}(\gamma)$ para $\gamma \in L$. Como $\gamma \in \mathscr{C}$, el corolario 2.2 (pág.26) implica que $[\mathbb{Q}(\gamma) : \mathbb{Q}] = [L : \mathbb{Q}]$ es una potencia de 2 como queríamos probar.

Podemos usar este teorema para probar que el inverso del corolario 2.2 (pág.26) es falso. Veámoslo con un ejemplo.

Ejemplo 2.9. Sea α una raíz del polinomio

$$f = x^4 - 4x^2 + x + 1. \tag{2.11}$$

Es fácil comprobar que f es irreducible sobre $\mathbb{Q}$, de modo que $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$. Se puede comprobar que el cuerpo de descomposición L de f sobre $\mathbb{Q}$ satisface $[L : \mathbb{Q}] = 24$. Por el teorema 2.3 (pág.28) podemos concluir que α es no constructible. La formula de resolución de una ecuación de cuarto grado implica la resolución previa de una cúbica y como no es posible construir con regla y compás las soluciones de una ecuación cúbica también se tiene que no es constructible.

3 Polígonos regulares y raíces de la unidad

3.1 Primos de Fermat

Nuestro próximo objeto de estudio son los polígonos regulares que se pueden construir con regla y compás. Nuestra principal herramienta será la extensión ciclotómica $\mathbb{Q} \subset \mathbb{Q}(\zeta)$ pero también usaremos los primos de Fermat. Un número primo p es un primo de Fermat si puede ser escrito de la forma:

$$p = 2^{2^m} + 1$$

con $m \geq 0$. Luego nos ayudarán a caracterizar los polígonos regulares a partir de ellos.

Ejemplo 3.1. Supongamos que podemos construir un polígono regular de n lados en el plano. Usando dos vértices consecutivos y el centro del polígono podemos obtener un triángulo. Debemos de tener construido el centro en el proceso de construcción del polígono y si no, el centro es constructible por la intersección de los bisectrices de los ángulos interiores. Se puede ver fácilmente que el ángulo que forman es $\theta = 2\pi/n$. Copiando dicho ángulo n veces y intersecando con el círculo de radio unidad tenemos que la raíz de la unidad $\zeta_n = e^{2\pi i/n}$ es constructible. Por tanto si un polígono de n lados se puede construir con regla y compás el mismo complejo es constructible. En sentido contrario también se tiene ya que si se tienen los puntos constructibles basta unirlos para tener el polígono.

3.2 Caracterización de constructibilidad de un polígono

Veamos antes unos resultados que nos resultaran útiles en el futuro

Lema 3.1. Si n es un entero positivo, entonces:

$$a^n - b^n = (a-b)\sum_{k=0}^{n-1} a^k b^{n-1-k}$$

Demostración.

$$(a-b)\sum_{k=0}^{n-1} a^k b^{n-1-k} = \sum_{k=0}^{n-1} a^{k+1} b^{n-1-k} - \sum_{k=0}^{n-1} a^k b^{n-k} =$$

$$= a^n + \sum_{k=1}^{n-1} a^k b^{n-k} - \sum_{k=1}^{n-1} a^k b^{n-k} - b^n = a^n - b^n$$

Proposición 3.1. Si $2^k + 1$ es primo, entonces k es potencia de 2

Demostración. Supongamos que k no es potencia de 2. Entonces k puede escribirse como $k = r\,s$ con s un primo impar y $1 \leq r \leq k$

Por el lema anterior sabemos que para un entero positivo m:

$$(a-b)|(a^m - b^m).$$

Sustituyendo $a = 2^r, b = -1$ y $m = s$ y sabiendo que s es impar,

$$(2^r + 1)|(2^k + 1)$$

y por tanto

$$(2^r + 1)|(2^k + 1).$$

Entonces como $1 < 2^r + 1 < 2^k + 1$, se tiene que $2^k + 1$ no es primo. Por contraposición k será potencia de 2

Teorema 3.1. *Sea $n > 2$ un entero. Entonces un polígono regular puede ser construido por regla y compás si y solo si:*

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

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

Demostración. En el ejemplo anterior hemos visto que un polígono regular de n lados es constructible si y solo si ζ_n es constructible. Por el teorema 2.3 (pág.28) sabemos que ζ_n es constructible si y solo si $[\mathbb{Q}(\zeta_n) : \mathbb{Q}]$ es potencia de 2 y por el corolario 0.1 (pág.10) $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \phi(n)$ donde $\phi(n)$ es la función de Euler.

De forma que ζ_n es constructible si y solo si $\phi(n)$ es una potencia de 2.

Primero supongamos que $n = 2^s p_1 \cdots p_r$, donde $p_1, \ldots, p_r$ son primos de Fermat todos distintos. Por lema 0.1 (pág.10) apartado (2) tenemos la formula:

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

Por lo que se deduce que $\phi(n)$ es una potencia de 2, cuando cada p_i es un primo de Fermat. En sentido contrario, supongamos que $\phi(n)$ es una potencia de 2, y factoricemos n como $n = q_1^{a_1} \cdots q_s^{a_s}$ donde $q_1, \cdots, q_s$ son primos distintos y los exponentes $a_1, \ldots, a_s$ son todos ≥ 1. Por lema 0.1 (pág.10) apartado (2) tenemos la formula:

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

Si q_i es primo $\neq 2$, entonces debemos tener $a_i = 1$, ya que $\phi(n)$ es una potencia de 2, y podemos concluir que $q_i - 1$ debe ser una potencia de 2. Ademas como sabemos que si un primo q se puede escribir de la forma $2^k + 1$ entonces k será una potencia de 2, es decir, será un primo de Fermat. Esto prueba que los primos que dividen n tienen exponente 1 y son primos de Fermat. Esto completa la prueba del teorema.

Los cinco primos de Fermat conocidos son

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

Se sospecha que F_0, F_1, F_2, F_3, F_4 son los únicos primos de Fermat pero esto no ha sido probado. Si fuera cierto el teorema 3.1 (pág.33) implicaría que un polígono regular de n lados es constructible por regla y compás si y solo si

$$n = 2^s \cdot 3^a \cdot 5^b \cdot 17^c \cdot 257^d \cdot 65537^e,$$

donde $s \geq 0$ y a, b, c, d, e son 0 o 1.

4 Origami

En esta sección nos centraremos en qué es lo que puede aportar el origami en la construcción de elementos en los que solo la regla y compás no son suficientes. Nos centraremos en describir con precisión los números de origami así como a explicar qué nos aporta en el sentido de la teoría de Galois.

4.1 Trisección del ángulo

Para empezar veamos una construcción que con regla y compás demostramos imposible en general, la trisección del ángulo.

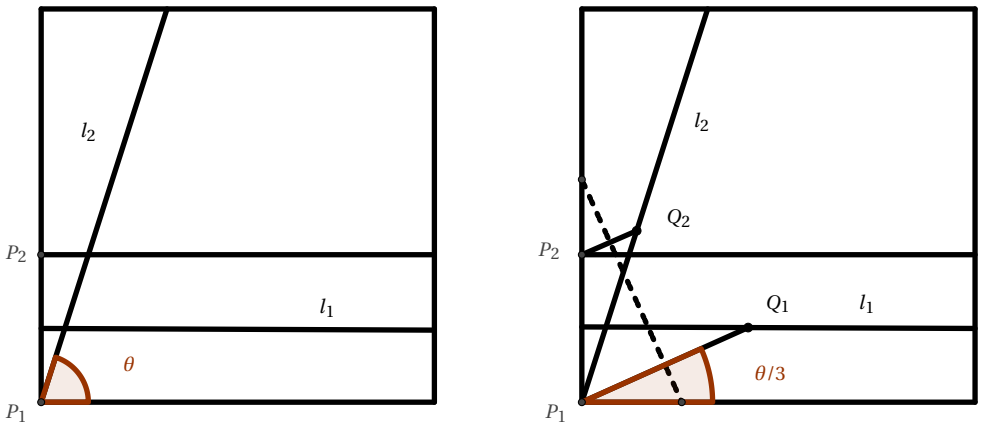


Figura 4.1: Trisección de un ángulo

Tomamos un ángulo arbitrario θ entre $\pi/4$ y $\pi/2$ y lo colocamos en la esquina inferior izquierda de un papel cuadrado de modo que θ es el ángulo entre el fondo del papel y l_2. Después doblamos el papel dos veces como se indica en la imagen de forma que obtenemos dos paralelas a la línea del fondo del papel que serán equidistantes. De las paralelas a la más cercana al fondo la llamaremos l_1, a la esquina inferior izquierda P_1 y a la intersección de la segunda paralela con el fin de la pagina a la izquierda P_2.

Ahora hagamos un doblez de la pagina de forma que superpongamos el punto P_1 con l_1 y el punto P_2 con l_2 generando Q_1 y Q_2 respectivamente. El ángulo formado por $\overline{P_1Q_1}$ será $\theta/3$. Basta doblar dos veces a partir de $\overline{P_1Q_1}$ para comprobar que esta interseca con l_2 y por tanto es un tercio de su ángulo.

Como puede ser un movimiento un tanto complicado de explicar y comprender, en el siguiente video (en el enlace `https://youtu.be/Q8AphvZ2UPU`) hago dicho movimiento, donde puede verse mejor la construcción.

De este modo tenemos que todo ángulo entre $\pi/2$ y $\pi/4$ se puede trisectar y por tanto todo ángulo ya que como todo ángulo es fácilmente duplicable por dobleces y se le puede hallar la bisectriz basta llevarnos el ángulo a trisectar al tramo $\pi/4 \leq \theta \leq \pi/2$ bisectando o duplicando, aplicar la trisección y volviendo a duplicar por cada bisección y viceversa.

También podemos resolver ecuaciones cúbicas usando origami pero antes veamos la geometría que nos aporta la trisección la cual esta asociada al trazado de tangentes a parábolas.

4.2 Resolución de ecuaciones cúbicas

Consideremos la parábola definida como el lugar de los puntos P equidistantes de un punto P_1 (foco) y de una recta l_1 (directriz).

En la figura 4.2 (pág.37) podemos ver que los segmentos $\overline{P_1P}$ y $\overline{PQ_1}$ tienen la misma longitud y $\overline{PQ_1}$ es perpendicular a la directriz l_1. La parte importante es que Q_1 es la reflexión de P_1 a partir de la recta tangente en P. Mediante origami, basta doblar el papel por la tangente para ver que los puntos intersecan. En consecuencia tenemos el siguiente resultado.

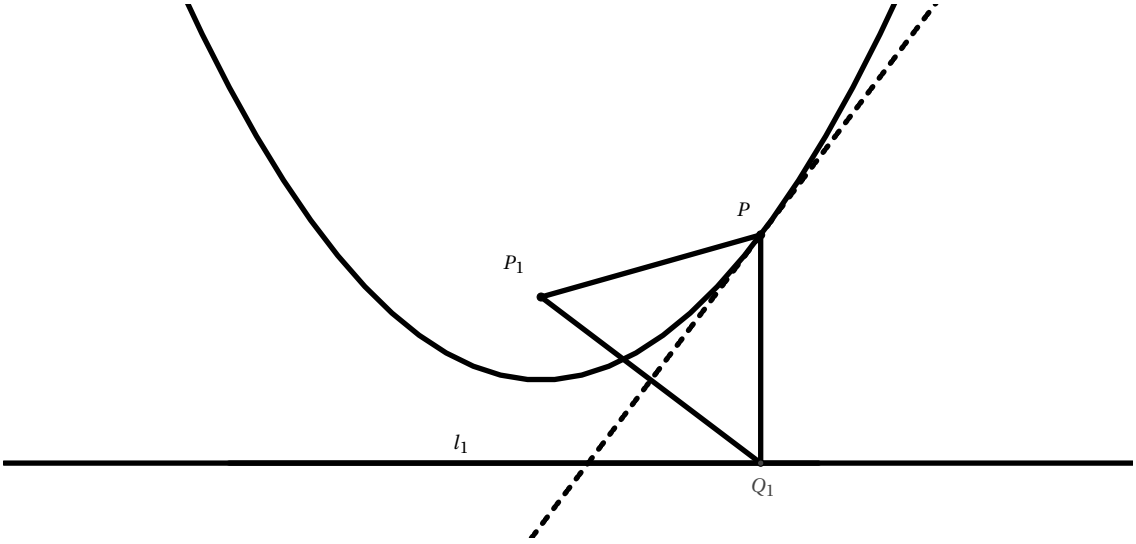


Figura 4.2: Parábola

Lema 4.1. En el plano, tomemos una recta l_1 y un punto P_1 no contenido en ella. Ademas tomemos otra recta l. La reflexión de P_1 a partir de l corta a l_1 si y solo si l es tangente a la parábola de foco P_1 y a la directriz l_1.

Para ver cómo esto se relaciona con origami volveremos a la imagen de la trisección. El movimiento de origami que usamos para llevar P_1 a $Q_1 \in l_1$ y P_2 a $Q_2 \in l_2$ fue el de doblar a partir de una recta cumpliendo unas condiciones. Esto significa que la reflexión de P_1 a partir de la recta generada por el doblez esta en l_1, por lo tanto la recta del doblez es la tangente de la parábola de foco P_1 y directriz l_1 por el lema 4.1 (pág.37). El mismo argumento se tiene para el foco P_2 y la directriz l_2. Por lo tanto podemos concluir que usando origami, se pueden encontrar las tangentes para dos parábolas dadas.

Ejemplo 4.1. Vamos a encontrar las raíces reales de la ecuación cúbica $x^3+ax+b=0$, donde $a, b \in \mathbb{R}$ y $b \neq 0$. Consideremos las parábolas

$$\begin{cases} (y-\frac{1}{2}a)^2 = 2bx, \\ y = \frac{1}{2}x^2. \end{cases}$$

Sea l una recta con pendiente m tal que sea simultáneamente tangente a las dos parábolas, en el punto (x_1, y_1) en la primera y en el punto (x_2, y_2) en la segunda.

Calculemos como sería la forma de la pendiente a la primera parábola. Para ello calculamos la derivada de la parábola lo que nos quedaría

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

Sustituyendo el punto (x_1, y_1) la inversa nos da la pendiente buscada ya que la recta tangente es de la forma $(y - y_0) = m(x - x_0)$ con (x_0, y_0) el punto dado y m la pendiente ya calculada, que será esta

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

Esto implica que $m \neq 0$ y que $y_1 - \frac{1}{2}a = \frac{b}{m}$ de donde podemos concluir fácilmente que

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

Calculando ahora la pendiente a la segunda parábola de la misma forma obtenemos

$$\begin{cases} x_2 = m, \\ y_2 = \frac{m^2}{2} \end{cases}$$

Si sustituimos los valores en $m = (y_2 - y_1)/(x_2 - x_1)$ obtenemos

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

como $m \neq 0$, esto prueba que m satisface la ecuación

$$m^3 + am + b = 0.$$

Por lo tanto las pendiente de las tangentes a las respectivas parábolas son raíces de la ecuación cúbica $m^3 + am + b$.

4.3 Números de Origami

Nuestra siguiente tarea será describir con cuidado cómo serán los números que podemos construir al añadir el movimiento de origami a las construcciones C1 y C2 definidas en la sección 1.

C3. Desde $\alpha_1 \neq \alpha_2$ puntos no contenidos en las rectas $l_1 \neq l_2$ podemos dibujar la recta l que reflecta α_1 en un punto en l_1 y α_2 en un punto en l_2.

La recta del doblez de la trisección es un ejemplo de C3. Se puede ver que hay situaciones donde no existe una recta l (Como por ejemplo en el caso en que l_1 y l_2 sean paralelas) y por lo tanto lo que C3 realmente dice es que podemos usar l siempre que exista. Por el lema 4.1 (pág.37) C3 nos permite dibujar las tangentes para dos parábolas dadas. Hay que tener en cuenta que C3 construye únicamente la recta l. Esto es porque en origami, la recta es un doblez y un punto es una intersección de dobleces. Igualmente una vez obtenido l, podemos construir la reflexión de α_1 y α_2 en l con las construcciones de regla y compás. Las operaciones C1,C2 y C3 crean círculos y rectas, que intersecándose usando P1, P2 y P3 de la sección 2 nos dan nuevos puntos que pueden ser usados para mas construcciones.

Definición 4.1. *Un número complejo α es un **número de origami** si existe una secuencia finita de construcciones usando C1, C2, C3, P1, P2 y P3 tal que comienza con 0 y 1 y termina en α*

Esta definición incluye regla, compás y origami. Sin embargo, en el capitulo 10 del libro de Martin [7] se prueba que todas las construcciones con regla y compás pueden ser reproducidas con ciertas operaciones que solo involucran plegados de papel. En particular se pueden remplazar C1, C2, C3, P1, P2 y P3 por construcciones que solo involucran movimientos de origami y nos darían los mismos números de origami.

4.4 Estructura de cuerpo y extensiones

Para establecer todos los numerosos de origami tenemos la siguiente estructura.

Teorema 4.1. *El conjunto* $\mathcal{O} = \{\alpha \in \mathbb{C} \mid \alpha \text{ es un número de origami}\}$ *es un subcuerpo de* $\mathbb{C}$. *Ademas:*

1. *Sea* $\alpha = a + ib$, *donde* $a, b \in \mathbb{R}$. *Entonces* $\alpha \in \mathcal{O}$ *si y solo si* $a, b \in \mathcal{O}$.
2. $\alpha \in \mathcal{O}$ *implica que* $\sqrt{\alpha}, \sqrt[3]{\alpha} \in \mathcal{O}$.
3. *Un número complejo* α *pertenece a* $\mathcal{O}$ *si y solo si existen los subcuerpos:*

$$\mathbb{Q} = F_0 \subset F_1 \subset \ldots \subset F_n \subset \mathbb{C} \tag{4.1}$$

donde $\alpha \in F_n$ *y* $[F_i : F_{i-1}] = 2$ *o* 3 *con* $1 \leq i \leq n$

Demostración. Tanto la prueba de que $\mathcal{O}$ es un subcuerpo de $\mathbb{C}$ como la prueba de (a) se puede seguir del teorema 2.1 (pág.19).

Para la prueba de (b), primeramente escribiremos α es forma polar $\alpha = re^{i\theta}$ asumiendo que $r > 0$. Usando el compás, podemos enviar r al eje X y con la construcción vista en el teorema 2.1 (pág.19) tenemos que $\sqrt{r} \in \mathcal{O}$. Ya que podemos bisectar θ con regla y compás, se tiene que

$$\sqrt{\alpha} = \pm\sqrt{r}e^{i\theta/2} \in \mathcal{O}.$$

Para la raíz cúbica, podemos trisectar como vimos al principio de la sección . Tomamos la parábolas del ejemplo 4.1 (pág.37) con $a = 0$ y $b = -r$ que serían

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

Dado r es fácil encontrar el foco y la directriz dada la parábola , así que aplicando C3 a los focos y directrices podemos construir varias tangentes a dichas parábolas y nos quedaremos con l que será la que es tangente a ambas simultáneamente. Dicha l tiene de pendiente $m = \sqrt[3]{r}$. Esto implica que $\sqrt[3]{r} \in \mathcal{O}$. Ademas como $w = e^{2\pi i/3} \in \mathcal{O}$ se tiene que

$$\sqrt[3]{\alpha} = w^i \sqrt[3]{r}e^{i\theta/3} \in \mathcal{O},\ i = 0, 1, 2.$$

En la prueba de la parte (c) diremos que los cuerpos $\mathbb{Q} = F_0 \subset F_1 \subset ... \subset F_n \subset \mathbb{C}$ forman una $2-3$ extensión si $[F_i : F_{i-1}] = 2$ o 3 para $1 \leq i \leq n$

Supongamos que $\mathbb{Q} = F_0 \subset F_1 \subset ... \subset F_n \subset \mathbb{C}$ es una $2-3$ extensión. Tenemos que probar que $F_n \subset \mathcal{O}$ por inducción en n. Como $n = 0$ es obvio asumiremos que $F_n \subset \mathcal{O}$. Dado $\alpha \in F_n$, sabemos que α es una raíz de un polinomio $f \in \mathcal{O}[x]$ de grado al menos 3, ya que $[F_n : F_{n-1}] = 2$ o 3. Si f es de grado 1, entonces $\alpha \in \mathcal{O}$ trivialmente y si f tiene grado 2 o 3 con la fórmula de Cardano para ecuaciones cuadráticas, α puede ser expresado en forma de raíces cuadradas, raíces cúbicas y elementos de $\mathcal{O}$. Por (b) se tiene que $\alpha \in \mathcal{O}$.

Probemos ahora el otro sentido. Sea α un número de origami. Tenemos que probar que existe una sucesión de subcuerpos $\mathbb{Q} = F_0 \subset F_1 \subset ... \subset F_n \subset \mathbb{C}$ tal que F_n contiene las partes reales e imaginarias de todos los números constructibles en el proceso de construcción de α. Entonces hay que probar que $\alpha = a + bi$ implica que $a, b \in F_n(i)$. Usaremos la misma estrategia que en la prueba del teorema 2.2 (pág.23).

Vamos a probarlo por inducción sobre N que es el número de veces que usamos P1, P2 o P3 en la construcción de α. Supongamos que es constructible en $N > 1$ pasos y que el último paso usa P1. Entonces α es la intersección de dos rectas l_1 y l_2 distintas, creadas a lo largo de la construcción. Si ambas rectas están generadas por C1, ya lo tenemos, ya que basta con seguir la demostración del teorema 2.2 (pág.23). En cambio si se ha usado C3 para la construcción de alguna de las rectas aún queda trabajo por hacer.

Si l_1 fue creada usando C3, entonces l_1 es simultáneamente tangente a dos parábolas cuyos focos y directrices han sido creados a lo largo de la construcción de α. Primero vamos a probar que l_1 tiene una ecuación cuyos coeficientes están en una $2-3$ extensión. Para ello consideremos el caso especial donde las parábolas son de la forma del ejemplo 4.1 (pág.37) para $a, b \in \mathbb{R}$. Por hipótesis de inducción y por la ecuación de la parábola (se puede calcular la ecuación de la parábola a partir del foco y la directriz) se tiene que a y b están en una $2-3$ extensión. Entonces la pendiente m de l_1 satisface la ecuación cúbica del ejemplo 4.1, y podemos extender la $2-3$ extensión a una que contenga a, b y m. Por el ejemplo 4.1 el punto $(x_1, y_1) \in l_1$ tiene coordenadas en la $2-3$ extensión. Esto prueba que l_1 tiene una ecuación $Ax + By = C$ cuyos coeficientes están en la misma $2-3$ extensión. En el caso general cuando l_1 es creada usando C3 por dos parábola cualesquiera, uno puede argumentar de manera similar que l_1 tiene una ecuación cuyos coeficientes están en una $2-3$ extensión.

Se deduce que si l_1 y/o l_2 han sido creadas a partir de C3, entonces hay una $2-3$ extensión conteniendo los coeficientes de las ecuaciones. Y como probamos en el teorema 2.2 (pág.23) podemos concluir que las coordenadas de la intersección de l_1 y l_2 están en la misma extensión.

Supongamos ahora que el último paso para crear α es P2. Entonces α es creada por la intersección de una circunferencia y una recta. Por la hipótesis de inducción y por el mismo argumento que para P1 se tiene que la circunferencia y la recta están definidas por ecuaciones cuyos coeficientes están en una $2-3$ extensión. Solo basta seguir el mismo argumento que en la demostración del teorema 2.2 (pág.23).

Finalmente si el último paso para generar α es P3, el argumento es idéntico al hecho en la demostración del teorema 2.2 (pág.23), ya que al ser intersección de circunferencias no usa rectas. Y con esto queda probado el teorema.

Ejemplo 4.2. Veamos que podemos construir el heptágono.

$$\mathbb{Q} \subset \mathbb{Q}(2\cos(2\pi/7)) \subset \mathbb{Q}(\zeta_7)$$

Como $[\mathbb{Q}[\cos(2\pi/7)] : \mathbb{Q}] = 3$ y $[\mathbb{Q}[\zeta_7] : \mathbb{Q}[\cos(2\pi/7)]] = 2$ tenemos que ζ_7 es un número de origami ya que es una $2-3$ extensión. Por tanto el heptágono puede ser construido con origami.

4.5 Relación con la teoría de Galois

Vamos a clasificar ahora los números de origami usando la teoría de Galois, pero antes veamos un teorema que nos será de vital importancia.

Teorema 4.2. ***Burnside****: Si p y q son primos distintos, entonces todo grupo de orden $p^n q^m$, $n, m \geq 0$, es resoluble.*

La demostración de este teorema se aleja demasiado del trabajo pero pueden verse dos pruebas en [8] y en [2].

Teorema 4.3. *Sea $\alpha \in \mathbb{C}$ algebraico sobre $\mathbb{Q}$ y sea $\mathbb{Q} \subset L$ el cuerpo de descomposición del polinomio mínimo de α sobre $\mathbb{Q}$. Entonces α es un número de origami si y solo si $[L:\mathbb{Q}] = 2^a 3^b$ para $a, b \geq 0$ enteros.*

Demostración. Primero supongamos que $[L:\mathbb{Q}] = 2^a 3^b$ para $a, b \geq 0$ enteros. Como $\mathbb{Q} \subset L$ es de Galois, $|\mathrm{Gal}(L/Q)| = [L:\mathbb{Q}] = 2^a 3^b$. Por el teorema anterior 4.2 (pág.42) tenemos que resoluble.

$$e = G_m \subset G_{m-1} \subset \cdots \subset G_1 \subset G_0 = \mathrm{Gal}(L/\mathbb{Q})$$

Con G_i normal en G_{i-1} de indice 2 o 3 (ya que $|\mathrm{Gal}(L/\mathbb{Q})$ ya que

$$\mathbb{Q} = L_{G_0} \subset L_{G_1} \subset \cdots \subset L_{G_m} = L, \text{ donde } [L_{G_i} : L_{G_{i-1}}] = 2 \text{ o } 3 \text{ para todo } i$$

Por el teorema 4.1 (pág.40) ,$\alpha \in L$ es constructible.

Probemos ahora la otra implicación. Primero probemos que $\mathbb{Q} \subset \mathcal{O}$ es una extensión normal. Para ello fijemos $\alpha \in \mathcal{O}$ y f tal que sea el polinomio mínimo de α sobre $\mathbb{Q}$. Tenemos que probar que todas las raíces de f pertenecen a $\mathcal{O}$. Como α es constructible el teorema 4.1 (pág.40) nos da las extensiones $\mathbb{Q} = F_0 \subset F_1 \subset \cdots \subset F_n \subset \mathbb{C}$ donde $[F_i : F_{i-1}] = 2$ o 3 y $\alpha \in F_n$. Entonces $\mathbb{Q} \subset M$ será el cuerpo de descomposición de $Q \subset F_n$.

Nótese que todas las raíces de f pertenecen a M, ya que M es normal sobre $\mathbb{Q}$, f es irreducible sobre $\mathbb{Q}$, y $\alpha \in F_n \subset M$ es una raíz de f. Ahora sea $\beta \in M$ una raíz de f. Por la proposición 0.1 (pág.10) tenemos que existe $\sigma \in \mathrm{Gal}(M/Q)$ tal que $\sigma(\alpha) = \beta$. Aplicando σ a los cuerpos $Q = F_0 \subset F_1 \subset \cdots \subset F_n \subset M$ tenemos:

$$\mathbb{Q} = \sigma(\mathbb{Q}) = \sigma(F_0) \subset \cdots \subset \sigma(F_n) \text{ tal que } [\sigma(F_i) : \sigma(F_{i-1})] = [F_i : F_{i-1}] = 2 \text{ o } 3 \text{ para todo } i$$

Por el teorema 4.1 (pág.40) $\beta = \sigma(\alpha) \in \sigma(F_n)$ es constructible. Esto prueba que todas las raíces de f pertenecen a $\mathcal{O}$. Por tanto se tiene que $\mathcal{O}$ contiene un cuerpo de descomposición L de f sobre $\mathbb{Q}$. Por el teorema del elemento primitivo, tenemos que $L = \mathbb{Q}(\gamma)$ para $\gamma \in \mathcal{O}$, el corolario 2.2 (pág.26) implica que $[\mathbb{Q}(\gamma) : \mathbb{Q}] = [L : \mathbb{Q}]$ es una potencia de 2 o 3 como queríamos probar.

Ejemplo 4.3. Sea $\alpha \in \mathbb{C}$ una raíz de $f = x^6 + x + 1$. Se puede comprobar que f es irreducible sobre $\mathbb{Q}$, por tanto $\mathbb{Q} \subset \mathbb{Q}(\alpha)$ es una extensión de grado 6. Sin embargo, aunque $6 = 2 \cdot 3$, α no es un número de origami. Si calculamos el grupo de Galois asociado al cuerpo de descomposición de $\mathbb{Q} \subset L$ obtenemos que $\mathrm{Gal}(L/\mathbb{Q} \cong S_6$. Entonces el teorema 4.3 (pág.43) implica que $\alpha \notin \mathcal{O}$, ya que $[L : \mathbb{Q}] = |\mathrm{Gal}(L/\mathbb{Q})| = 6! = 2^4 \cdot 3^2 \cdot 5$.

4.6 Problemas clásicos

Al comienzo de este capitulo vimos la trisección del ángulo ya que era necesario para la construcción de los números de origami pero no es la única construcción que, a pesar de no poder construirla por regla y compás, podemos realizar. Veamos el caso de la duplicación del cubo.

El problema de construir un cubo tal que tenga el doble de volumen que un cubo dado es equivalente a poder construir $\sqrt[3]{2}$. Ya vimos que con regla y compás es imposible pero por origami es posible por el teorema 4.1 (pág.40). De hecho basta hacer el doblez siguiente para probar que $\sqrt[3]{2}$ es constructible.

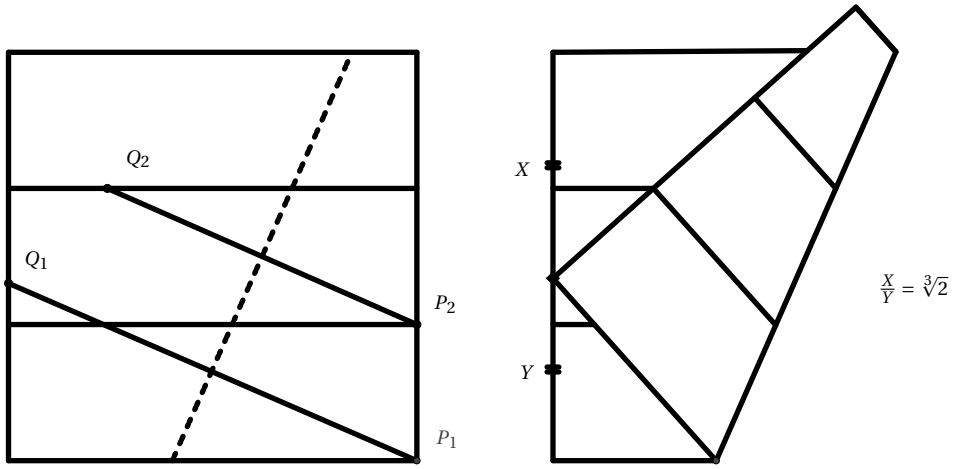


Figura 4.3:

El caso de la cuadratura del círculo sigue siendo imposible por la trascendencia de π.

5 Polígonos regulares por Origami

5.1 Primos de Pierpont

En el capitulo 3 vimos una caracterización de qué polígonos eran constructibles por regla y compás. Lo lógico sería ver si es posible encontrar una nueva caracterización para el caso de Origami. Al igual que con regla y compás nos ayudaremos de unos tipos de números primos que nos serán muy útiles, los primos de Pierpont. Un primo de Pierpont es un primo $p > 3$ de la forma:

$$p = 2^u 3^v + 1, \tag{5.1}$$

con u y v enteros no negativos. Ademas si $v = 0$ y $u > 0$, entonces u será una potencia de 2, y el número primo será por tanto de Fermat.

Los primeros primos de Pierpont serán: $2, 3, 5, 7, 13, 17, 19, 37, 73, 97, 109, 163, 193, 257, 433, 487, 577, 769, \ldots$ y el mayor primo de Pierpont conocido es $3 * 2^{5082306} + 1$ el cual tiene 1529928 dígitos.

5.2 Caracterización de constructibilidad de un polígono con origami

Teorema 5.1. *Un polígono regular de n lados puede ser constructible por origami si y solo si*

$$n = 2^a 3^b p_1 p_2 \cdots p_s,$$

donde $a, b \geq 0$ y $p_1, \ldots, p_s$ son primos de Pierpont distintos.

Demostración. Seguiremos la construcción de la demostración para regla y compás ya que presenta muchas similitudes. Al igual que vimos en el caso de regla y compás un polígono será constructible si y solo si ζ_n es constructible. Por el teorema 4.3 (pág.43) sabemos que ζ_n es constructible si y solo si $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = 2^a 3^b$ con $a.b \geq 0$ enteros y por el corolario 0.1 (pág.10) $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \phi(n)$ donde $\phi(n)$ es la función de euler.

De forma que ζ_n es constructible si y solo si $\phi(n) = 2^a 3^b$.

Primero supongamos que $n = 2^s 3^t p_1 \cdots p_r$, donde $p_1, \ldots, p_r$ son primos de Pierpont distintos. Por el lema 0.1 (pág.10) apartado 2 tenemos la formula:

$$\phi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right) = \begin{cases} 2^{s-1} 3^{t-1} (p_1 - 1) \cdots (p_r - 1), & s > 0 \ t > 0, \\ (p_1 - 1) \cdots (p_r - 1), & s, t = 0. \end{cases}$$

Por lo que se deduce que $\phi(n) = 2^a 3^b$, cuando cada p_i es un primo de Pierpont. En sentido contrario, supongamos que $\phi(n) = 2^a 3^b$, y factoricemos n como $n = q_1^{a_1} \cdots q_s^{a_s}$ donde $q_1, \cdots, q_s$ son primos distintos y los exponentes $a_1, \ldots, a_s$ son todos ≥ 1. Por lema 0.1 (pág.10) apartado (2) tenemos la formula:

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

Si q_i es primo $\neq 2$ o 3, entonces debemos tener $a_i = 1$, ya que $\phi(n) = 2^a 3^b$, y podemos concluir que $q_i - 1 = 2^a 3^b$. Ademas si un primo se puede escribir de la forma $2^k 3^t + 1$ será un primo de Pierpont. Esto prueba que los primos que dividen n tienen exponente 1 y son primos de Pierpont. Esto completa la prueba del teorema.

Gracias a esto podemos afirmar que el heptágono es constructible con origami ya que 7 es un primo de Pierpont, así como otros muchos que con regla y compás sería imposible. En esta lista podemos ver que dicho avance no es pequeño.

1. Polígonos constructibles por regla y compás: 2, 3, 4, 5, 6, 8, 10, 12, 15, 16, 17, 20, 24, 30, 32, 34, 40, 48, 51, 60, 64, 68, 80, 85, 96.

2. Polígonos constructibles por origami: 7, 9, 13, 14, 18, 19, 21, 26, 27, 28, 35, 36, 37, 38, 39, 42, 45, 52, 54, 56, 57, 63, 65, 70, 72, 73, 74, 76, 78, 81, 84, 90, 91, 95, 97.

6 Regla marcada e intersección de cónicas

Los números de origami se pueden construir con regla marcada o con intersección de cónicas. En este capitulo veremos brevemente los métodos de construcción así como comentar qué nos aporta.

6.1 Regla marcada

Una regla marcada es una regla con dos marcas que nos indican la medida de una unidad. De modo que una regla marcada puede construir una recta a partir de dos puntos conocidos como con la regla normal y por otro método alternativo. Dicho método consiste en dado un punto P y las rectas l_1 y l_2 dibujar la recta que pasa por P y y los puntos Q_1 y Q_2 de l_1 y l_2 respectivamente tal que $d(Q_1, Q_2)$ es 1.

Las construcciones con regla marcada comienzan con los puntos $0, 1$ y i. En cada paso, uno puede construir una nueva recta aplicando cualquiera de las dos operaciones descritas antes a rectas y puntos ya construidos de forma que se obtienen nuevas rectas y puntos en $\mathbb{C}$ formados por la intersección de estas.

Ejemplo 6.1. Sea l_1 la recta $y = x$, l_2 la recta $y = -\frac{1}{2}x$ y $P = (\frac{1}{2}, 0)$. Ahora tomamos la recta r con pendiente m que pasa por P. Se puede comprobar que r interseca con l_1 en el punto $Q_1 = (x_1, x_1) \in l_1$, donde $x_1 = \frac{m}{2m-2}$ y con l_2 en el punto $Q_2 = (x_2, -\frac{1}{2}x_2) \in l_2$ donde $x_2 = \frac{m}{2m+1}$.

Si tenemos en cuenta r la construimos con regla marcada la distancia entre Q_1 y Q_2 es 1 y obtenemos la ecuación

$$(\frac{m}{2m-1}-\frac{m}{2m-2})^2+(\frac{-m}{2(2m+1)}-\frac{m}{2m-2})^2=1,$$

que se simplifica en la ecuación de cuarto grado

$$7m^4-16m^3-21m^2+8m+4=0$$

Las raíces de esta ecuación son todas reales y representan las pendientes de las cuatro rectas que pasan por P que han sido construidas con regla marcada con las rectas l_1 y l_2. Se puede comprobar que el grupo de Galois de la ecuación es S_4. Por lo tanto el cuerpo de descomposición es una extensión de $\mathbb{Q}$ de grado 24. Al no ser potencia de 2 estas rectas no son constructibles con regla y compás.

Teorema 6.1. *Sea $\alpha \in \mathbb{C}$. Entonces α puede ser construido usando una regla marcada si y solo si α es un número de origami, es decir, $\alpha \in \mathcal{O}$.*

Una prueba de este resultado se encuentra en [[7],Cap.10]

6.2 Cónicas

Las cónicas pueden ser definidas geométricamente en términos de focos, directrices y excentricidades o algebráicamente tratando las elipses, hipérbolas y parábolas por separado. Para nuestro caso usaremos una tercera forma de definirlas, la cual define una cónica como una curva en el plano definida por una ecuación de la forma

$$F(x,y)=ax^2+bxy+cy^2+dx+ey+f=0$$

donde $a,b,c,d,e,f \in \mathbb{R}$ y $(a,b,c) \neq (0,0,0)$. Asumiremos que tiene, al menos, una solución con x,y reales. Escribiendo la ecuación en la forma matricial tenemos

$$A=\begin{bmatrix} a & \frac{1}{2}b & \frac{1}{2}d \\ \frac{1}{2}b & c & \frac{1}{2}e \\ \frac{1}{2}d & \frac{1}{2}e & f \end{bmatrix}$$

y

$$\mathbf{x} = \begin{bmatrix} x \\ y \\ 1 \end{bmatrix}$$

tal que $F = (x, y) = \mathbf{x}^t A\mathbf{x}$.

Entonces la cónica C definida por F es no degenerada si $\det(A) \neq 0$. Entonces si C es no degenerada

1. $b^2 - 4ac < 0 \Leftrightarrow C$ es una eclipse,
2. $b^2 - 4ac = 0 \Leftrightarrow C$ es una parábola,
3. $b^2 - 4ac > 0 \Leftrightarrow C$ es una hipérbola.

Para hacer construcciones por intersección de cónicas empezamos con $0, 1$ y las posibles construcciones serán una recta que conecte dos puntos ya construidos o una cónica cuyos coeficientes son números reales ya construidos. Entonces podemos obtener nuevos puntos con la intersección de rectas y cónicas

Teorema 6.2. *Sea $\alpha \in \mathbb{C}$. Entonces α es constructible por intersección de cónicas si y solo si α es un número de origami, es decir, $\alpha \in \mathcal{O}$.*

Una prueba de este resultado se encuentra en [1]

Como resultado final tenemos el conjunto de caracterizaciones de un número de origami:

- α es un número de origami $\Leftrightarrow$ α es constructible con regla marcada
- α es un número de origami $\Leftrightarrow$ α es constructible por intersección de cónicas
- α es un número de origami $\Leftrightarrow$ α esta en una $2-3$ extensión $\mathbb{Q} = F_0 \subset \cdots \subset F_n$
- α es un número de origami $\Leftrightarrow$ α es algebraico sobre $\mathbb{Q}$, y el grupo de Galois del polinomio mínimo tiene orden $2^a 3^b$

7 | Axiomas de Lang

Corolario 7.1. Todo elemento constructible por origami es constructible por regla y compás, pero el reciproco no es cierto.

Esta afirmación puede parecer una falsedad, de hecho lo es, pero en el articulo [5] a partir de una serie de pruebas y afirmaciones llega a este resultado. ¿Esta el articulo equivocado? ¿Hay algún error en nuestra construcción? La respuesta a ambas preguntas es no. El problema radica en qué axiomas de origami tomamos en la construcción de elementos. El axioma de origami que nosotros usamos es $\underline{C3}$ pero los autores basan su prueba en otros axiomas con movimientos más básicos.

En 1996 Lang [6] aporto una axiomática de origami que es una de las más usadas en construcciones de origami que contiene los movimientos usados en el articulo [5] asi como el usado en nuestro trabajo. Veámoslos.

$\underline{O1}$. Dados dos puntos p y q podemos doblar el papel por una recta que los conecte.

Figura 7.1:

*O*2. Dados dos puntos p y q podemos doblar el papel tal que se superpongan.

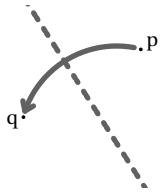


Figura 7.2:

*O*3. Dadas dos rectas r y s podemos doblar el papel tal que se superpongan.

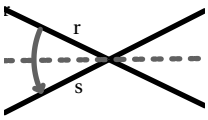


Figura 7.3:

*O*4. Dados un punto p y una recta r podemos doblar el papel por una recta que los conecta perpendicular a r.

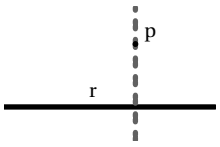


Figura 7.4:

*O*5. Dados dos puntos p y q y una recta r podemos doblar el papel de forma p se superpone con r y q esta contenido en la recta generada por el doblez

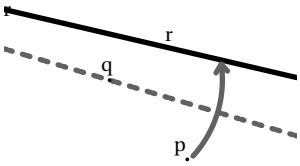


Figura 7.5:

*O*6. Dados dos puntos p y q y dos rectas r y s, podemos doblar el papel de forma que p se superponga con r y q con s

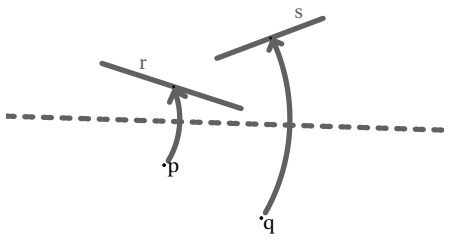


Figura 7.6:

*O*7. Dados un punto p y las rectas r y s, podemos doblar el papel tal que p se superponga con r y la recta generada por el doblez sea perpendicular a s.

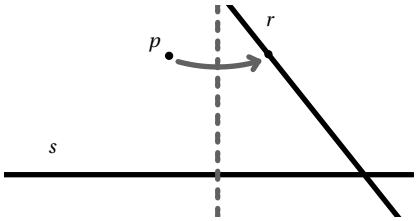


Figura 7.7:

Como podemos ver el axioma que nosotros usamos es el O6 y los usados por los autores de [5] son solo los cinco primeros de forma que es posible llegar al corolario a partir de estos axiomas.

Bibliografía

[1] ALPERIN, R. C. A mathematical theory of origami constructions and numbers. *New York J. Math. 6* (2000), 119–133.

[2] BENDER, H. A group theoretic proof of Burnside's $p^a q^b$-theorem. *Math. Z. 126* (1972), 327–338.

[3] COX, D. A. *Galois theory*, second ed. Pure and Applied Mathematics (Hoboken). John Wiley & Sons, Inc., Hoboken, NJ, 2012.

[4] HADLOCK, C. R. *Field theory and its classical problems*, vol. 19 of *Carus Mathematical Monographs*. Mathematical Association of America, Washington, D.C., 1978.

[5] HULL, T. A note on "impossible" paper folding. *Amer. Math. Monthly 103*, 3 (1996), 240–241.

[6] LANG, R. Origami and geometric constructions. `http://www.langorigami.com/files/articles/origami_constructions.pdf`, 2015.

[7] MARTIN, G. E. *Geometric constructions*. Undergraduate Texts in Mathematics. Springer-Verlag, New York, 1998.

[8] ROTMAN, J. J. *Advanced modern algebra. Part 2*, third ed., vol. 180 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 2017. With a foreword by Bruce Reznick.