UNIVERSIDAD AUTÓNOMA DEL ESTADO DE MÉXICO

FACULTAD DE CIENCIAS

SOBRE LA TRISECTRIZ Y LA IMPOSIBILIDAD DE TRISECTAR EL ÁNGULO CON REGLA Y COMPÁS

TESIS

PARA OBTENER EL TÍTULO DE:

MATEMÁTICA

PRESENTA:

Sarai Vidal Gomez

ASESOR DE TESIS:
Dr. Enrique Castañeda Alvarado

El Cerrillo, Piedras Blancas, México
14 de Julio de 2022.

SOBRE LA TRISECTRIZ Y LA IMPOSIBILIDAD DE TRISECTAR EL ÁNGULO CON REGLA Y COMPÁS

Sarai Vidal Gomez

14 de julio de 2022

Introducción

Platón pensaba que el comienzo es la parte más importante de la obra, y como en esta tesis se hablará de Geometría y en específico de la Geometría Euclidiana empezaremos definiendo la palabra Geometría la cual proviene del griego que significa: “medida de la tierra, medida del terreno”, la geometría tuvo su origen en Mesopotamia y Egipto, como una serie de conocimientos empíricos acerca de longitudes, ángulos, áreas y volúmenes que se usaron para la agrimensura, la construcción y la astronomía. Platón también estableció a la geometría como una disciplina intelectual, separada de cualquier aplicación (ver [9] y [11]).
Después, gracias a la contribución de Euclides con su escrito llamado *Los elementos*, libro que fue considerado durante mucho tiempo el texto más importante de las matemáticas, se establecieron ciertas reglas y definiciones básicas. Él sólo admitía las construcciones geométricas que podían realizarse usando una vara no marcada (regla) y un compás el cual se caracteriza porque si una de sus patas se levanta del papel entonces el compás se cierra inmediatamente (esto es un compás euclidiano), incluso se dice que él hizo de esto un requisito pues esta implícito en sus construcciones.
Con estas restricciones en los instrumentos, existen muchas construcciones geométricas que pueden realizarse. Sin embargo, existen también otras que no se pueden llevar a cabo, de hecho en su momento parecían ser muy fáciles de construir pero con el paso del tiempo los griegos descubrieron que algunas de esas construcciones eran muy difíciles y escaparon completamente de su ingenio, de esta manera existieron tres problemas imposibles, los cuales fueron llamados *los tres problemas griegos* y son los siguientes:

- Es imposible trisecar un ángulo usando sólo regla y compás.
- Es imposible duplicar el volumen de un cubo usando solamente regla y compás.

- Es imposible usando solamente regla y compás, construir un cuadrado cuya área sea la misma de un círculo de radio uno.

Teniendo presente esto, como veremos en este trabajo de tesis, Arquímedes sabía que se puede trisecar un ángulo utilizando una vara recta en la que hay dos marcas fijas y un compás, desde ese entonces se ha supuesto, como los griegos debieron haber sospechado, que una trisección exacta del ángulo con regla (no marcada) y compás es imposible, pero tanto matemáticos como aficionados atraídos a estos intentaban resolverlos, esta sección fue tomada primordialmente de [1] y [4].
Por supuesto, sin las restricciones originales de usar sólo regla y compás todos estos problemas pueden ser resueltos, por ejemplo usando otras herramientas o construcciones para dividir el ángulo en tres, algunas de ellas las abordaremos en esta tesis, un ejemplo es la *trisectriz* y tiene la propiedad de ayudar a trisecar el ángulo y podemos consultarla en [7] y [8], de tal curva en esta tesis haremos un estudio usando polinomios de Chebyshev los cuales se pueden consultar en [5] y [10].
Finalmente, utilizaremos la teoría algebraica de campos para demostrar que es imposible trisecar el ángulo usando sólo regla y compás la cual fue tomada principalmente de [2], [3] y [12], podremos ver como se puede trisecar un ángulo recto con regla y compás. Sin embargo, nuestro principal objetivo es demostrar la imposibilidad de dividir cualquier ángulo dado en tres partes iguales, usando solamente regla y compás.

Índice general

Capítulo 1

Preliminares

En este capítulo presentamos algunas definiciones, proposiciones y resultados básicos de la geometría euclidiana que usaremos en el desarrollo de este trabajo y se pueden consultar en [6], algunas otras serán mencionadas en cuanto se vayan utilizando.

1.1. Definiciones y Proposiciones básicas

Los teoremas geométricos de Euclides se derivan de un pequeño número de supuestos básicos y ampliamente intuitivos, en la literatura se llaman los cinco Postulados de Euclides y son los siguientes (ver [11]):

1. Puedes dibujar un segmento de recta entre cualesquiera dos puntos, es decir, dados dos puntos distintos cualesquiera hay exactamente una recta que los contiene.

2. Una línea recta puede extenderse infinitamente en cualquiera de sus direcciones.

3. Es posible trazar un círculo de cualquier radio en cualquier punto.

4. Todos los ángulos rectos son iguales entre sí.

5. Si una línea recta atraviesa otras dos rectas, y si los ángulos internos formados suman menos que dos ángulos rectos (180^o), las líneas eventualmente se cruzarán. En otras palabras, las líneas paralelas (ver la Definición 1.1.9) nunca se cruzan. Esto se conoció como el postulado de paralelismo de Euclides.

Proposición 1.1.1. *Dos rectas se intersectan en a lo más un punto.*

Demostración. Sean L_1 y L_2 dos rectas que se intersectan en un punto P, el cual supongamos no es el único punto de intersección de las dos rectas dadas, es decir, sea Q un punto en la intersección de L_1 y L_2, entonces P y Q son puntos de L_1 y de L_2, pero esto es falso pues por dos puntos distintos cualesquiera solo puede pasar una línea recta que contenga a los dos por el postulado 1. □

Notación 1.1.2. *Dados dos puntos A y B el segmento de recta que une a A y B lo denotamos por $\overline{AB}$.*

Definición 1.1.3. *Si dos rayos tienen el mismo origen o extremo, pero no están en la misma recta, entonces su reunión es un ángulo como en la Figura 1.1. Los dos rayos se llaman los lados del ángulo y al extremo común se llama vértice. Si los rayos son $\overrightarrow{AB}$ y $\overrightarrow{AC}$, entonces el ángulo se indica con $\angle BAC$ o bien $\angle CAB$.*

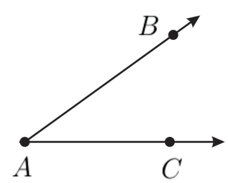

Figura 1.1: Ángulo $\angle BAC$.

Definición 1.1.4. *Si $\overrightarrow{AB}$ y $\overrightarrow{AD}$ son rayos opuestos, y $\overrightarrow{AC}$ es otro rayo cualquiera, entonces $\angle BAC$ y $\angle CAD$ forman un par lineal, véase Figura 1.2.*

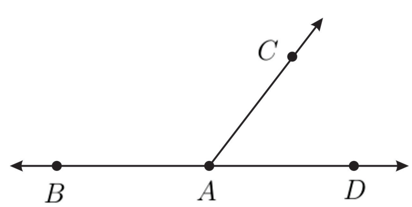

Figura 1.2: Par lineal.

Definición 1.1.5. *Si la suma de las medidas de dos ángulos es* 180^o*, entonces decimos que los ángulos son suplementarios, y que cada uno es el suplemento del otro, véase Figura 1.3.*

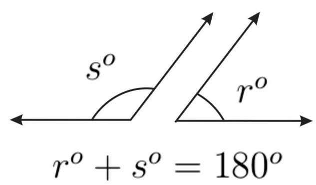

Figura 1.3: Ángulos suplementarios.

Definición 1.1.6. *Si los ángulos de un par lineal tienen la misma medida, entonces cada uno de ellos se llama ángulo recto y su medida es* 90^o*, véase Figura 1.4.*

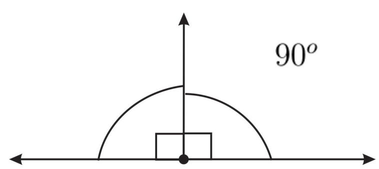

Figura 1.4: Ángulo recto.

Definición 1.1.7. *Si* $\overrightarrow{AB}$ *y* $\overrightarrow{AC}$ *forman un ángulo recto, entonces se llaman perpendiculares, véase Figura 1.5.*

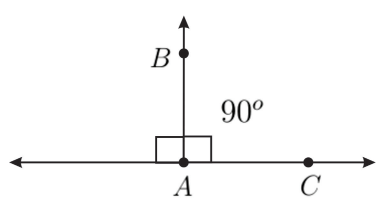

Figura 1.5: Rectas perpendiculares.

Definición 1.1.8. *Una secante* T *a dos rectas coplanares* L_1 *y* L_2 *(rectas que están en el mismo plano) es una recta que las intersecta en dos puntos diferentes, véase Figura 1.6.*

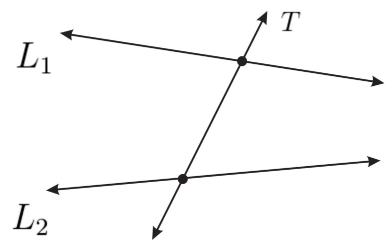

Figura 1.6: Recta secante.

Definición 1.1.9. *Dos rectas son paralelas si están en el mismo plano y nunca se cortan entre sí.*

Definición 1.1.10. *Dos ángulos con la misma medida, se llaman ángulos congruentes.*

Definición 1.1.11. *Sean L_1 y L_2 dos rectas paralelas cortadas por una secante T en los puntos P y Q, respectivamente, como en la Figura 1.7. Sea A un punto de L_1 y B un punto de L_2, tales que A y B están en los lados opuestos de T. Entonces, los ángulos $\angle APQ$ y $\angle PQB$ se dicen alternos internos y además son congruentes.*

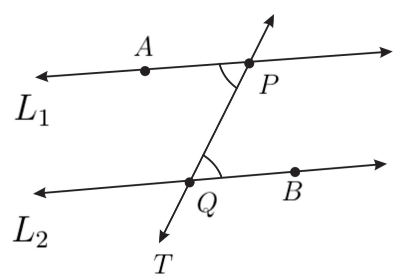

Figura 1.7: Ángulos alternos internos.

Definición 1.1.12. *Dos ángulos son opuestos por el vértice, si sus lados forman dos pares de rayos opuestos y además estos ángulos son congruentes, véase Figura 1.8.*

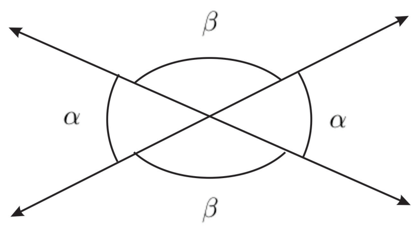

Figura 1.8: Ángulos opuestos por el vértice.

Definición 1.1.13. *Si A, B, C son tres puntos cualesquiera no alineados, entonces la reunión de los segmentos $\overline{AB}$, $\overline{AC}$ y $\overline{BC}$ se llama triángulo como en la Figura 1.9. Los puntos A, B y C se llaman vértices del triángulo, y los segmentos $\overline{AB}$, $\overline{AC}$ y $\overline{BC}$ se llaman lados del triángulo.*

Observación 1.1.14. *Todo triángulo ABC determina tres ángulos: $\angle BAC$, $\angle ABC$ y $\angle ACB$.*

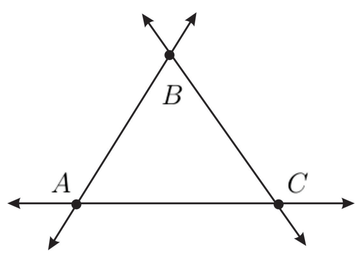

Figura 1.9: Triángulo ABC.

Proposición 1.1.15. *La suma de los ángulos interiores de un triángulo ABC es 180^o.*

Demostración. Sea ABC un triángulo con ángulos interiores $\angle BAC$, $\angle ABC$ y $\angle ACB$. Consideremos la recta $\overleftrightarrow{PQ}$ paralela a $\overline{BC}$ que pasa por el punto A, tal que A está entre P y Q como en la Figura 1.10. Observemos que $\angle QAC = \angle ACB$ y $\angle PAB = \angle ABC$ por ser alternos internos, luego $\angle QAC + \angle BAC + \angle PAB = 180^o$ por ser suplementarios. Por lo tanto $\angle ACB + \angle BAC + \angle ABC = 180^o$ al hacer la sustitución correspondiente. $\square$

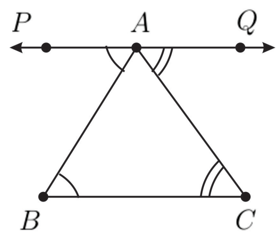

Figura 1.10: Suma de ángulos interiores de un triángulo.

Definición 1.1.16. *Si C está entre A y D como en la Figura 1.11, entonces el $\angle BCD$ es un ángulo externo del triángulo ABC.*

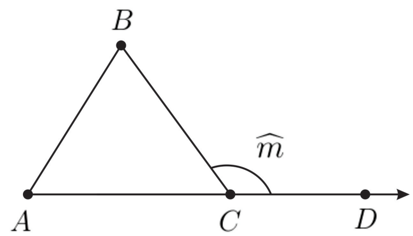

Figura 1.11: Ángulo exterior de un triángulo.

Proposición 1.1.17. *Sea $\widehat{m}$ un ángulo exterior al triángulo ABC como el de la Figura 1.11, entonces $\widehat{m} = \angle BAC + \angle ABC$.*

Demostración. Observemos que $\angle ACB + \widehat{m} = 180^o$ por ser suplementarios. Además, por la Proposición 1.1.15,

$$\angle ACB + \angle BAC + \angle ABC = 180^o \tag{1.1}$$

luego, despejando la primer igualdad tenemos $\angle ACB = 180^o - \widehat{m}$, Entonces al sustituir en (1.1) obtenemos $\angle BAC + \angle ABC + 180^o - \widehat{m} = 180^0$. □

Definición 1.1.18. *Un triángulo con dos lados congruentes se llama isósceles. El otro lado se llama base del triángulo. Los dos ángulos asociados con la base se llaman ángulos en la base.*

Definición 1.1.19. *Un triángulo rectángulo es un triángulo donde uno de sus ángulos es recto. El lado opuesto del ángulo recto se llama hipotenusa, y los otros dos lados son los catetos.*

Definición 1.1.20. *Sea P un punto de un plano dado y sea r un número positivo. La circunferencia con centro P y radio r es el conjunto de todos los puntos del plano que están a distancia r del punto P, véase Figura 1.12.*

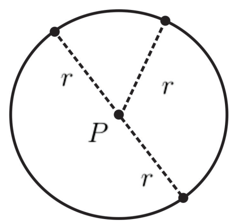

Figura 1.12: Circunferencia de radio r y centro P.

Definición 1.1.21. *La cuerda de una circunferencia es un segmento cuyos extremos están en la circunferencia, en la Figura 1.13 el segmento $\overline{AB}$ es una cuerda.*

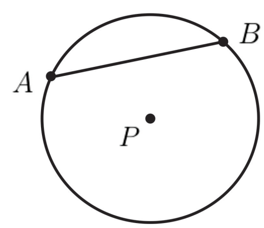

Figura 1.13: Cuerda de una circunferencia.

1.2. Tres construcciones no aceptables

Los griegos consideraron que la medición era simplemente una de tantas artes prácticas, les gustaban las construcciones con una vara (regla) y compás, incluso sabían como sumar, restar y multiplicar con estas construcciones, su interés era tan profundo que se encontraron con problemas que los derrotaron por completo y hasta los fanáticos intentaban encontrar soluciones para poder resolverlos. Con el paso del tiempo estos problemas se hicieron famosos tomando por nombre “Los tres problemas griegos”.

Estos problemas a parte de ser famosos por su imposibilidad, desarrollaron a las mismas matemáticas. Debido a que, si era imposible darles solución, entonces debía ser posible demostrar su imposibilidad. Los tres famosos problemas griegos son los siguientes:

- Trisecar un ángulo usando sólo regla y compás.
- Duplicar el volumen de un cubo usando solamente regla y compás.
- Usando solamente regla y compás, construir un cuadrado cuya área sea la misma de un círculo de radio uno.

El problema que capta el interés en esta tesis es el de la trisección del ángulo, por esta razón a continuación podremos ver tres construcciones en las cuales se puede trisecar el ángulo, evidentemente rompiendo las reglas que los griegos establecieron (usar solo regla y compás).

Primeramente podremos ver como Arquímedes podía trisecar un ángulo utilizando una vara (recta) en la que hay dos marcas fijas y un compás, de modo que la construcción de Arquímedes se extiende a lo que realmente es posible. Sin embargo, como hemos marcado la regla, esto rompe las reglas que los griegos establecieron y por ello esta construcción no puede hacerse con regla y compás.
A continuación mostraremos la construcción de Arquímedes para trisecar un ángulo la cual podemos consultar en [1], véase Figura 1.14.
Sean α el ángulo dado, formado por las rectas ℓ y m, y sea C su vértice.

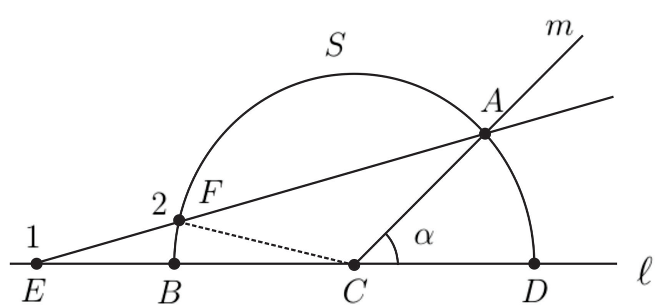

Figura 1.14: Construcción para trisecar un ángulo según Arquímedes.

Construcción:

1. Trazamos un semicírculo S con centro en C y radio arbitrario. Sean B y D las intersecciones de S con la recta ℓ, y sea A la intersección de S con la recta m.
2. En una regla, marcamos la distancia igual al radio CB del semicírculo. Sean 1 y 2 estas marcas.
3. Colocamos la regla de tal modo que 2 coincida con algún punto del semicírculo S, 1 con algún punto de la recta ℓ y que, al mismo tiempo, la regla pase por A. Sean E y F los puntos de ℓ y S que acabamos de localizar con las marcas 1 y 2, respectivamente.

Con la notación anterior, tenemos la siguiente proposición.

Proposición 1.2.1. *El ángulo AEB es un tercio del ángulo α.*

Demostración. Por construcción, $EF = FC$ entonces el triángulo EFC es isósceles. Así,

$$\angle CEF \cong \angle FCE = \gamma.$$

Lo cual implica que $\angle EFC = 180^o - 2\gamma$. Como E, F, A están alineados $\angle CFA = 2\gamma$. Luego, el triángulo FCA es isósceles, porque $FC = CA$. Por lo tanto $\angle AFC = \angle CAF = 2\gamma$. Además,

$$\angle FCA + 2\angle AFC = \angle FCA + 4\gamma = 180^o. \tag{1.2}$$

Como D, C, B están alineados, $\gamma + \angle FCA + \alpha = 180^o$. Por (1.2) tenemos que: $\angle FCA + 4\gamma = \angle FCA + \gamma + \alpha$. Así concluimos que $\alpha = 4\gamma - \gamma = 3\gamma$. Por lo tanto, $\gamma = \frac{\alpha}{3}$. □

La siguiente construcción, hace uso de la curva llamada trisectriz de Hipias (425 a.C.) la cual tambien es llamada Cuadratriz de Dinóstratos. Primeramente definiremos la curva para después ver como se aplica en la trisección del ángulo, véase [4] y [9].

Sean $ABCD$ un cuadrado y $\widehat{BED}$ un arco de un círculo con centro en A y radio $\overline{AD}$ como se muestra en la Figura 1.15. Supongamos que el radio $\overline{AB}$ del círculo se mueve a velocidad uniforme alrededor de A, de la posición $\overline{AB}$ a la posición $\overline{AD}$. También $\overline{BC}$ empieza a moverse en el mismo momento y en su última posición coincide con $\overline{AD}$. En cualquier instante previo, durante el movimiento, la recta $\overline{BC}$ y el radio $\overline{AB}$, determinan con su intersección un punto F o L, véase Figura 1.15. El lugar geométrico de la intersección de estos dos lados genera un curva, la cuadratriz.

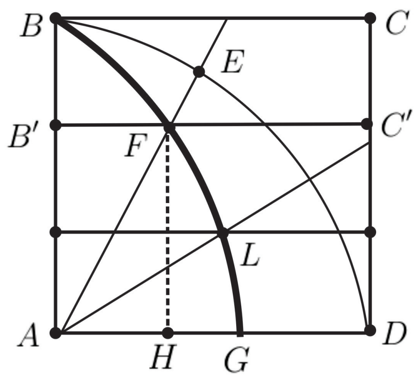

Figura 1.15: Cuadratriz.

Definición 1.2.2. *El lugar geométrico de los puntos B, F, L y G es la cuadratriz, y la propiedad de la curva es:*

$$\frac{\angle BAD}{\angle EAD} = \frac{\widehat{BED}}{\widehat{ED}} = \frac{AB}{FH}.$$

Veamos ahora como la cuadratriz puede trisecar un ángulo.
Sea α el ángulo dado, primero construimos un cuadrado $ABCD$, tal que uno de sus vértices sea el vértice del ángulo α y uno de sus lados esté sobre un lado del ángulo, y construimos la cuadratriz. Sean $\alpha = \angle EAD$ y F el punto de intersección de $\overline{AE}$ con la cuadratriz. Posteriormente trazamos la paralela a $\overline{BC}$ por F. Sean B' y C' los puntos de intersección de ésta con $\overline{AB}$ y $\overline{DC}$, respectivamente. Después, trisectamos el segmento $\overline{AB'}$ con B'' y B''' los puntos de trisección, para trazar paralelas a $\overline{BC}$ por B'' y B'''. Así, $\overline{B''C''}$ y $\overline{B'''C'''}$ son dichas paralelas y F' y F'' sus respectivas intersecciones con la cuadratriz. Finalmente trazamos $\overline{AF'}$ y $\overline{AF''}$.

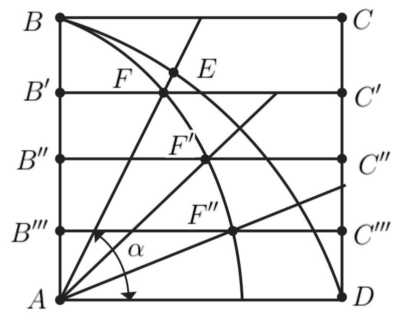

Figura 1.16: Trisección del ángulo con la cuadtratriz.

Afirmación 1.2.3. *Las rectas $\overline{AF'}$ y $\overline{AF''}$ trisecan el ángulo α.*

Demostración. Por la propiedad de la cuadratriz tenemos

$$\frac{B'A}{\angle FAD} = \frac{B''A}{\angle F'AD} = \frac{B'''A}{\angle F''AD}.$$

pero $B'A = 3B'''A$ y $B''A = 2B'''A$, entonces

$$\frac{3}{\angle FAD} = \frac{2}{\angle F'AD} = \frac{1}{\angle F''AD}.$$

De lo cual obtenemos que

$$\begin{aligned} \angle F''AD &= \frac{1}{3}\angle FAD, \\ \angle F'AD &= \frac{2}{3}\angle FAD. \end{aligned}$$

Por lo tanto, las rectas $F'A$ y $F''A$ trisecan el ángulo α. $\square$

Notemos que esta construcción no puede hacerse con regla y compás ya que depende de la construcción de la cuadratriz la cual tendríamos que construir punto por punto lo cual es imposible.

La siguiente y última construcción es la más reciente la cual dío un coronel alemán que participó en la Primera Guerra Mundial y podemos consultar en [4].
Sea α el ángulo dado, ℓ y m sus lados y C su vértice. Primeramente trazamos una serie de semicírculos con centro en C y trisecamos el menor semicírculo de

los trazados, transportando el radio r de éste tres veces. Sean x, y, z los puntos localizados, de esta forma, z estará en ℓ. En cada uno de los semicírculos que hemos trazado, marcamos con la misma abertura r del compás tres arcos. Posteriormente trazamos la curva que una a x con la primera marca de cada semicírculo, y con la segunda, z con la tercera y así obtenemos las curvas I, II y III. Sea E el punto de intersección de III con la recta m. Finalmente trazamos un arco de círculo de radio CE y centro C. Sea F el punto de intersección de éste con ℓ. Sean H y G los puntos de intersección del arco con las curvas I y II, respectivamente.

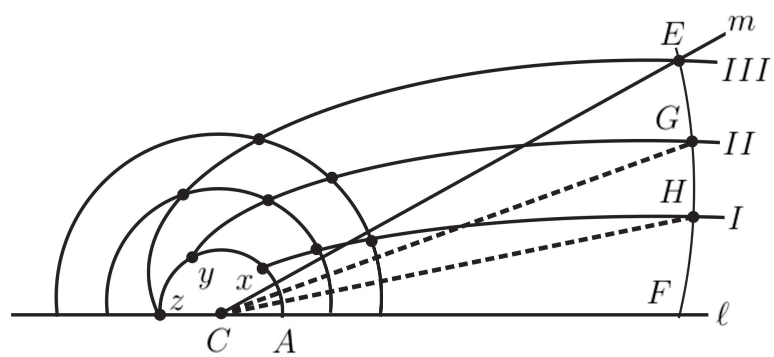

Figura 1.17: Construcción del Coronel Alemán.

Afirmación 1.2.4. *Las rectas CG y CH trisectan al ángulo α.*

Demostración. Las curvas I, II, III son el lugar geométrico de los puntos que determinan arcos iguales en cada semicírculos, en particular G y H dividen el arco $\overline{EF}$ en tres arcos iguales. Por lo tanto, los segmentos $\overline{CG}$ y $\overline{CH}$ trisectan el ángulo α. $\square$

Esta construcción tampoco es aceptable por métodos euclidianos ya que para construir las curvas I, II, III con regla y compás tendríamos que hacerlo punto por punto, lo cual es imposible.

Capítulo 2

Trisectriz: otra forma para trisecar el ángulo

De los trabajos realizados por numerosos matemáticos se descubrieron varias y novedosas curvas. En este capítulo introducimos un tipo de curva derivada de una construcción geométrica, esta curva es importante pues tiene la propiedad de trisecar el ángulo y son la generalización de la llamada Trisectriz de Ceva.

2.1. Construcción

La Trisectriz de Ceva fue estudiada por Giovanni Ceva, matemático italiano (1648-1736). Esta curva se puede describir como sigue y la podemos consultar en [1].
Dados una circunferencia de centro O y radio a, y una recta $\overleftrightarrow{Ox}$ que pasa por O. Consideremos P un punto de la circunferencia, como en la Figura 2.1.

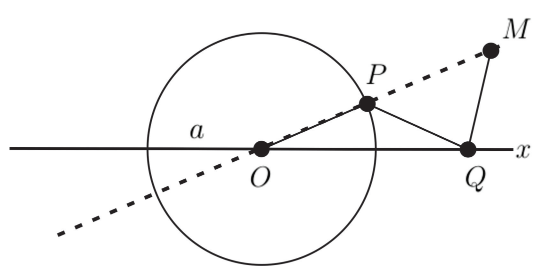

Figura 2.1: Construcción de la Trisectriz de Ceva.

Se construye un punto M tal que $OP = PQ = QM$ y Q se encuentra en la recta $\overleftrightarrow{Ox}$, de manera que los puntos O, P y M sean colineales.
El lugar geométrico de los puntos M cuando P se desplaza en la circunferencia, es la curva llamada *Trisectriz de Ceva*.

Proposición 2.1.1. *El ángulo $\angle xQM$ es el triple del ángulo $\angle xOM$.*

Demostración. El ángulo $\angle POQ = \angle PQO = \alpha$ pues el triángulo OPQ es isósceles. Sea β el ángulo $\angle OPQ$, como $\alpha + \alpha + \beta = 180^o$, por la Proposición 1.1.16, $\angle MPQ = 2\alpha$. Dado que el triángulo PQM es isósceles, entonces el $\angle PMQ = 2\alpha$. Sea $\gamma = \angle PQM$, sabemos que $2\alpha + 2\alpha + \gamma = 180^o$, entonces $\angle xQM = 3\alpha$. $\square$

Proseguimos con el estudio de esta curva, analizando la construcción de la que hemos hablado y dando parametrizaciones con las que podemos visualizarla ([8],[7]). Dada la importancia de la trisectriz de Ceva en lo que sigue de este capítulo determinamos la parametrización de la curva.

Definición 2.1.2. *La Trisectriz de Ceva, véase Figura 2.2, está definida por la siguiente ecuación polar,*

$$\rho = a + 2a\frac{\operatorname{sen} k\varphi \cos(k+1)\varphi}{\operatorname{sen}\varphi}, a > 0, k \in \mathbb{N}, \varphi \in (0, 2\pi). \tag{2.1}$$

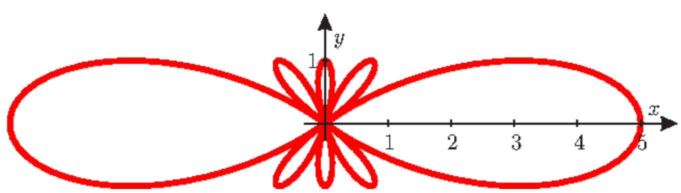

Figura 2.2: Trisectriz de Ceva.

La Figura 2.2 muestra la Trisectriz de Ceva para el caso $a = 1$ y $k = 2$, notemos que tiene dos ejes de simetría perpendiculares.
Si $k = 1$, entonces obtenemos la llamada Cisoide de Ceva la cual fue ideada por Ceva y la llamó Cicloide Anomalorum.

Definición 2.1.3. *La Cisoide de Ceva, véase Figura 2.3, es una curva plana que se define con la ecuación polar*

$$\rho = 1 + 2\cos(2\varphi), \varphi \in (0, 2\pi). \tag{2.2}$$

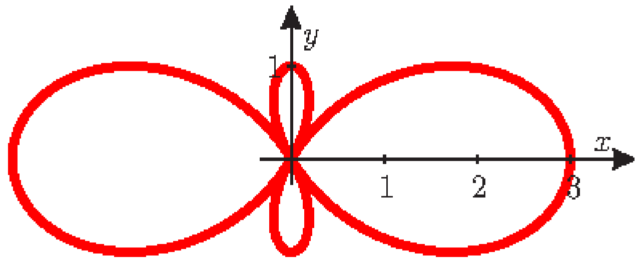

Figura 2.3: Cisoide de Ceva donde $k = 1$.

Notación 2.1.4. *Denotamos la distancia entre dos puntos* A *y* B *como* $d(A, B)$.

Sea e una línea dada por la ecuación $y = x\tan(\alpha)$ donde $0 \leq \alpha \leq \frac{\pi}{2}$. Consideremos A_1 un punto en la línea e tal que su primer coordenada es $x > 0$ y $d(O, A_1) = 1$. Sea A_2 el punto que está en el eje x tal que $d(A_1, A_2) = 1$ y $A_2 \neq O$. Escogemos el nuevo punto A_3 en la línea e tal que $d(A_2, A_3) = 1$ y $A_3 \neq A_2$ véase Figura 2.4. Recursivamente podemos definir el punto A_i (*para* $i \geq 2$) en la línea e o en el eje x, si i es impar o par, respectivamente donde $d(A_i, A_{i-1}) = 1$ y $A_i \neq A_{i-2}$. La Figura 2.4 muestra el caso en el cual los puntos A_i están en la línea e y son impares, y la Figura 2.5 muestra el caso en el cual los puntos A_i están en la línea e y los subíndices son pares.

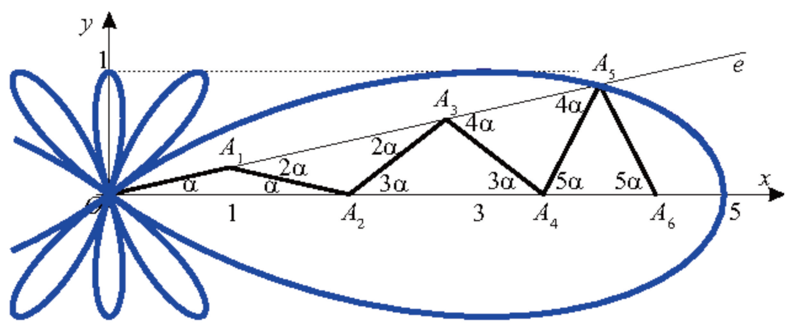

Figura 2.4: Puntos A_i con subíndices impares en la línea e.

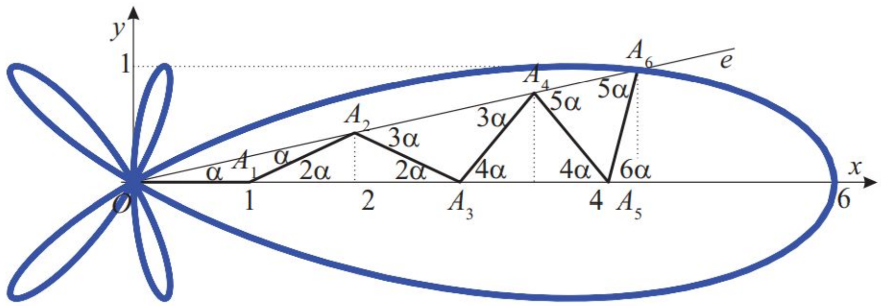

Figura 2.5: Puntos A_i con subíndices pares en la línea e.

Proposición 2.1.5. *Si* $0 < \alpha \leq \frac{\pi}{4}$, *entonces*

a) *A_i está entre los puntos O y A_{i+2}.*

b) *Si el ángulo $\angle OA_{i+1}A_i$ es α_i, entonces $\alpha_i = i\alpha$ para $i \in \mathbb{N}$.*

Demostración. *a*) Como $0 < \alpha \leq \frac{\pi}{4}$, A_i, A_{i+1} y A_{i+2} existen, además observemos que los puntos O, A_i, A_{i+2} son colineales y pertenecen a la recta e o a el eje x como en la Figura 2.4 y la Figura 2.5. Dado que O es el origen se cumple que A_i está entre los puntos O y A_{i+2}.

b) Procederemos de manera inductiva. Dado que el triángulo OA_1A_2 es isósceles con $OA_1 = A_1A_2$ se tiene que $\angle OA_2A_1 = \alpha = \angle A_2OA_1$. Como $\angle OA_1A_2$ es suplemento de $\angle A_2A_1A_3$ (Figura 2.6) y la suma de los ángulos interiores de un triángulo es 180^o, se cumple que $\alpha_2 = \angle A_2A_1A_3 = 2\alpha$.
Supongamos que $\alpha_i = \angle OA_{i+1}A_i = i\alpha$.
Ahora, consideremos el triángulo $A_{i-1}A_iA_{i+1}$ el cual es isósceles con $A_{i-1}A_i = A_iA_{i+1}$. Así, $\angle A_{i+1}A_{i-1}A_i = \alpha_i = \angle A_{i-1}A_{i+1}A_i$. Por la hipótesis de inducción,

$$2\alpha_i + \angle A_{i-1}A_iA_{i+1} = 180^o \text{ y} \tag{2.3}$$

$$\angle OA_iA_{i-1} + \angle A_{i-1}A_iA_{i+1} + \alpha_{i+1} = 180^o. \tag{2.4}$$

Restando las ecuaciones (2.3) y (2.4), y dado que $\angle OA_iA_{i-1} = \alpha_{i-1} = (i-1)\alpha$, obtenemos

$$\alpha_{i+1} + (i-1)\alpha - 2\alpha_i = 0.$$

Por lo tanto,

$$\alpha_{i+1} = (i+1)\alpha.$$

□

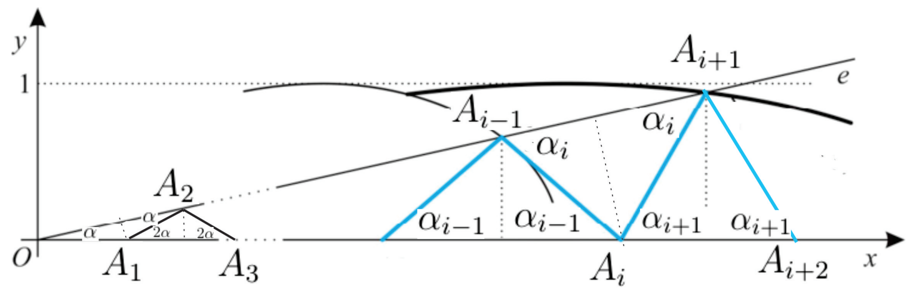

Figura 2.6: Generalización de la trisectriz hasta el punto A_{i+1} en la línea e.

Para que esté bien definida la trisectriz, a continuación determinamos un intervalo para el ángulo α.

Proposición 2.1.6. *Si* $i < \frac{\pi}{2\alpha} + 1$, *y* $i \geq 2$, *entonces los puntos* A_i *existen.*

Demostración. Como $i < \frac{\pi}{2\alpha} + 1$, entonces $2\alpha(i-1) < \pi$. De que $i \geq 2$ el ángulo $2\alpha(i-1)$ existe, es decir, el punto $A_{2(i-1)}$ existe por la Proposición 2.1.5. □

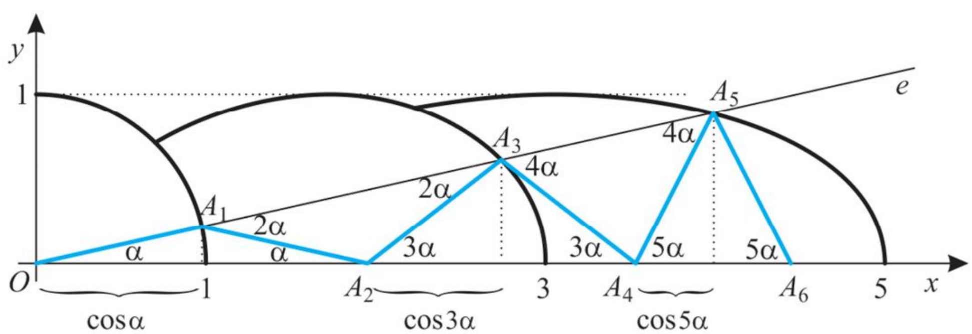

Figura 2.7: Generalización de la trisectriz hasta el punto A_5 en la línea e.

El punto A_1 se mueve en un arco de círculo, véase Figura 2.7, dado por la ecuación

$$\begin{aligned} x_1(\alpha) &= \cos\alpha, \\ y_1(\alpha) &= \operatorname{sen}\alpha. \end{aligned} \quad 0 < \alpha < \frac{\pi}{2}. \tag{2.5}$$

De las coordenadas de A_i (con $i = 2k+1$), obtenemos un sistema de ecuaciones paramétricas dadas por

$$\begin{aligned} x_{2n+1}(\alpha) = &\quad 2(\cos\alpha + cos3\alpha + \cdots + \cos(2n-1)\alpha) + \cos(2n+1)\alpha, \\ y_{2n+1}(\alpha) = &\quad \operatorname{sen}(2n+1)\alpha. \end{aligned} \tag{2.6}$$

Para $n \neq 1$ el punto A_{2n+1} depende del ángulo α, del triángulo $A_{2n-1}A_{2n}A_{2n+1}$, con lo que $2 \cdot 2n\alpha < \pi$, entonces $0 < \alpha < \frac{\pi}{4n}$ véase Figura 2.8.

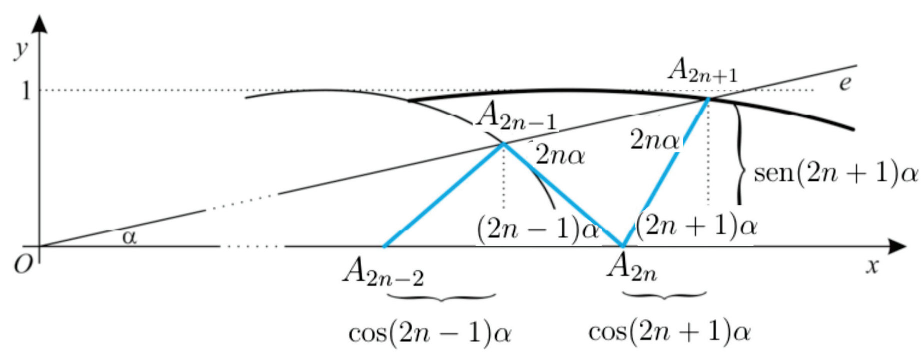

Figura 2.8: Generalización de la trisectriz hasta el punto A_{2n+1} en la línea e.

2.2. Polinomios de Chebyshev

A continuación estudiaremos los polinomios de Chebyshev de los cuales existen varios tipos, sin embargo en esta tesis solo veremos el primer y segundo tipo, $T_n(x)$ y $U_n(x)$, pues son justo los que necesitamos para tener una parametrización de la Trisectriz, una consulta mayor de estos polinomios se puede hacer en [10] y [5].

Definición 2.2.1. *Los polinomios de Chebyshev de primer tipo $T_n(x)$ son polinomios en x de grado n, donde $n \in \mathbb{Z}$ definidos por la siguiente relación*

$$T_n(x) = \cos n\alpha, \; donde \; x = \cos\alpha, \tag{2.7}$$

el valor de la variable x está en el intervalo $[-1, 1]$, y $\alpha \in [0, \pi]$.

Proposición 2.2.2. *Si el grado de los polinomios de Chebyshev es* $n \geqslant 1$ *entonces,* $T_{n+1}(x) = 2xT_n(x) - T_{n-1}(x)$.

Demostración. Por definición sabemos que

$$\begin{aligned} T_{n+1}(\cos\alpha) &= \cos(n+1)\alpha = \cos n\alpha \cos\alpha - \operatorname{sen} n\alpha \operatorname{sen}\alpha, \\ T_{n-1}(\cos\alpha) &= \cos(n-1)\alpha = \cos n\alpha \cos\alpha + \operatorname{sen} n\alpha \operatorname{sen}\alpha. \end{aligned}$$

Entonces,

$$\begin{aligned} T_{n+1}(x) + T_{n-1}(x) &= \cos(n+1)\alpha + \cos(n-1)\alpha \\ &= 2\cos n\alpha\ cos\alpha \\ &= 2xT_n(x). \end{aligned}$$

Despejando se obtiene

$$T_{n+1}(x) = 2xT_n(x) - T_{n-1}(x).$$

□

Ejemplo 2.2.3. *Algunos ejemplos de Polinomios de Chebyshev del tipo* $T_n(x)$ *son:*

$$\begin{aligned} T_0(x) &= \cos 0 \cdot \alpha = 1, \\ T_1(x) &= \cos 1 \cdot \alpha = x, \\ T_2(x) &= 2x^2 - 1, \\ T_3(x) &= 4x^3 - 3x, \\ T_4(x) &= 8x^4 - 8x^2 + 1, \\ T_5(x) &= 16x^5 - 20x^3 + 5x. \end{aligned}$$

Definición 2.2.4. *Los polinomios de Chebyshev de segundo tipo* $U_n(x)$ *son polinomios en* x *de grado* n*, donde* $n \in \mathbb{Z}$ *definidos por*

$$U_n(x) = \frac{\operatorname{sen}(n+1)\alpha}{\operatorname{sen}\alpha},\ donde\ x = \cos\alpha,$$

el valor de la variable x *esta en el intervalo* $[-1, 1]$*, y* $\alpha \in (0, \pi)$.

Ejemplo 2.2.5.

$$\begin{aligned} U_0(x) &= U_0(x) = \frac{\operatorname{sen}\alpha}{\operatorname{sen}\alpha} = 1, \\ U_1(x) &= U_1(x) = \frac{\operatorname{sen}2\alpha}{\operatorname{sen}\alpha} = 2x. \end{aligned}$$

Observación 2.2.6. *Si el grado de los polinomios de Chebyshev de segundo tipo es $n \geqslant 1$, entonces*

$$\begin{aligned} \operatorname{sen}\alpha U_{n-1}(\cos\alpha) &= \operatorname{sen}\alpha \frac{\operatorname{sen}(n-1+1)\alpha}{\operatorname{sen}\alpha} \\ &= \operatorname{sen} n\alpha. \end{aligned}$$

Proposición 2.2.7. *Si el grado de los polinomios de Chebyshev de segundo tipo es $m \geqslant 1$, entonces $U_m(x) = -U_{-m-2}(x)$.*

Demostración. Dado que $\operatorname{sen}(x)$ es una función impar se tiene que:

$$\begin{aligned} -U_{-m-2}(x) &= \frac{-\operatorname{sen}(-m-2+1)\alpha}{\operatorname{sen}\alpha} \\ &= \frac{-\operatorname{sen}(-m-1)\alpha}{\operatorname{sen}\alpha} \\ &= \frac{-\operatorname{sen}(-(m+1))\alpha}{\operatorname{sen}\alpha} \\ &= \frac{\operatorname{sen}(m+1)\alpha}{\operatorname{sen}\alpha} = U_m(x). \end{aligned}$$

□

Proposición 2.2.8. *Si el grado de los polinomios de Chebyshev de segundo tipo es $n = -1$, entonces $U_{-1}(x) = 0$.*

Demostración.

$$U_{-1}(x) = \frac{\operatorname{sen}(-1+1)\alpha}{\operatorname{sen}\alpha} = \frac{\operatorname{sen}0}{\operatorname{sen}\alpha} = 0.$$

□

Proposición 2.2.9. *Si el grado de los polinomios de Chebyshev de segundo tipo es $n = -2$, entonces $U_{-2}(x) = -1$.*

Demostración.

$$U_{-2}(x) = \frac{\operatorname{sen}(-2+1)\alpha}{\operatorname{sen}\alpha} = \frac{\operatorname{sen}-\alpha}{\operatorname{sen}\alpha} = -1.$$

□

Proposición 2.2.10. *Si el grado de los polinomios de Chebyshev de segundo tipo es $n \geqslant 1$ entonces, $U_n(x) = 2xU_{n-1}(x) - U_{n-2}(x)$.*

Demostración. Sabemos que

$$\begin{aligned} \operatorname{sen}(n+1)\alpha &= \operatorname{sen}(n\alpha+\alpha) = \operatorname{sen} n\alpha\cos\alpha + \operatorname{sen}\alpha\cos n\alpha, \\ \operatorname{sen}(n-1)\alpha &= \operatorname{sen}(n\alpha-\alpha) = \operatorname{sen} n\alpha\cos\alpha - \operatorname{sen}\alpha\cos n\alpha. \end{aligned}$$

Entonces,

$$\operatorname{sen}(n+1)\alpha + \operatorname{sen}(n-1)\alpha = 2\cos\alpha\operatorname{sen} n\alpha.$$

Así,

$$\frac{\operatorname{sen}(n+1)\alpha}{\operatorname{sen}\alpha} + \frac{\operatorname{sen}(n-1)\alpha}{\operatorname{sen}\alpha} = \frac{2\cos\alpha\operatorname{sen} n\alpha}{\operatorname{sen}\alpha}.$$

Luego obtenemos,

$$U_n(x) - U_{n-2}(x) = 2xU_{n-1}(x).$$

Finalmente, despejamos y obtenemos la igualdad

$$U_n(x) = 2xU_{n-1}(x) - U_{n-2}(x).$$

□

Ejemplo 2.2.11. *Algunos ejemplos de polinomios de Chebyshev del tipo $U_n(x)$ son:*

$$\begin{aligned} U_2(x) &= 4x^2 - 1, \\ U_3(x) &= 8x^3 - 4x, \\ U_4(x) &= 16x^4 - 12x^2 + 1, \\ U_5(x) &= 32x^5 - 32x^3 + 6x. \end{aligned}$$

Proposición 2.2.12. *Si el grado de los polinomios de Chebyshev de primer y segundo tipo es $n \geqslant 1$, entonces $T_n(x) = \frac{1}{2}(U_n(x) - U_{n-2}(x))$.*

Demostración. Sabemos que

$$\operatorname{sen}(n+1)\alpha - \operatorname{sen}(n-1)\alpha = 2 \operatorname{sen}\alpha \cos n\alpha.$$

Entonces,

$$\frac{\operatorname{sen}(n+1)\alpha}{\operatorname{sen}\alpha} - \frac{\operatorname{sen}(n-1)\alpha}{\operatorname{sen}\alpha} = \frac{2\operatorname{sen}\alpha\cos n\alpha}{\operatorname{sen}\alpha}.$$

Así,

$$U_n(x) - U_{n-2}(x) = 2T_n(x).$$

Por lo tanto,

$$T_n(x) = \frac{1}{2}(U_n(x) - U_{n-2}(x)).$$

□

Proposición 2.2.13. *Si el grado de los polinomios de Chebyshev de primer y segundo tipo es $n \geqslant 1$ con n impar, entonces*

$$U_n(x) = 2\sum_{j \text{ impar}}^{n} T_j(x).$$

Demostración. Sabemos que

$$T_n(x) = \frac{1}{2}(U_n(x) - U_{n-2}(x)).$$

Entonces,

$$\begin{aligned} 2T_1(x) &= U_1(x) - U_{-1}(x), \\ 2T_3(x) &= U_3(x) - U_1(x), \\ 2T_5(x) &= U_5(x) - U_3(x). \end{aligned}$$

Siguiendo el mismo procedimiento hasta n donde n es impar, obtenemos

$$2T_n(x) = U_n(x) - U_{n-2}(x).$$

Por la Proposición 2.2.8, $U_{-1}(x) = 0$. Por lo tanto,

$$U_n(x) = 2\sum_{jimpar}^{k} T_j(x)$$

. □

Proposición 2.2.14. *Si el grado de los polinomios de Chebyshev de primer y segundo tipo es $n \geqslant 1$ con n par, entonces*

$$U_n(x) = 2\sum_{j\ par}^{n} T_j(x) - 1.$$

Demostración. Sabemos que

$$T_n(x) = \frac{1}{2}(U_n(x) - U_{n-2}(x)).$$

Entonces,

$$\begin{array}{rcl} 2T_0(x) & = & U_0(x) - U_{-2}(x), \\ 2T_2(x) & = & U_2(x) - U_0(x), \\ 2T_4(x) & = & U_4(x) - U_2(x). \end{array}$$

Siguiendo el mismo procedimiento hasta n donde n es par, obtenemos

$$2T_n(x) \quad = \quad U_n(x) - U_{n-2}(x).$$

Por la Proposición 2.2.9, sabemos que $U_{-2}(x) = -1$. Así, concluimos que

$$U_n(x) = 2\sum_{j\ par}^{k} T_j(x) - 1.$$

□

Proposición 2.2.15. *Si el grado de los polinomios de Chebyshev de primer y segundo tipo es $n \geqslant 1$, entonces*

$$2\sum_{j=1}^{n} T_{2j-1}(x) + T_{2n+1}(x) = xU_{2n}(x).$$

Demostración. Por la Proposición 2.2.12,

$$xU_n(x) = \frac{1}{2}(U_{n-1}(x) + U_{n+1}(x)).$$

Entonces, obtenemos que

$$\begin{array}{rcl} xU_{2n}(x) & = & \frac{1}{2}(U_{2n-1}(x) + U_{2n+1}(x)) \\ & = & U_{2n-1}(x) + \frac{1}{2}(U_{2n+1}(x) - U_{2n-1}(x)) \\ & = & 2\sum_{j=1}^{n} T_{2j-1}(x) + T_{2n+1}(x). \end{array}$$

□

Proposición 2.2.16. *Si el grado de los polinomios de Chebyshev de primer y segundo tipo es $n \geqslant 1$, entonces*

$$1 + 2\sum_{j=1}^{n-1} T_{2j}(x) + T_{2n}(x) = xU_{2n-1}(x).$$

Demostración.

$$\begin{aligned}
1 + 2\sum_{j=1}^{n-1} T_{2j}(x) + T_{2n}(x) &= -1 + 2\sum_{j=0}^{n-1} T_{2j}(x) + T_{2n}(x) \\
&= U_{2n-2}(x) + \frac{1}{2}(U_{2n}(x) - U_{2n-2}(x)) \\
&= \frac{1}{2}(U_{2n-2}(x) + U_{2n}(x)) = xU_{2n-1}(x).
\end{aligned}$$

$\square$

Proposición 2.2.17. *Usando los Polinomios de Chebishev para $x = \cos\alpha$, las ecuaciones (2.6) se pueden escribir de la siguiente forma*

$$\begin{aligned}
x_{2n+1}(\alpha) &= \cos\alpha U_{2n}(\cos\alpha), \\
y_{2n+1}(\alpha) &= \operatorname{sen}\alpha U_{2n}(\cos\alpha).
\end{aligned} \qquad 0 < \alpha < \frac{\pi}{4n}. \tag{2.8}$$

Demostración. El sistema de ecuaciones (2.6) es

$$\begin{aligned}
x_{2n+1}(\alpha) &= 2(\cos\alpha + cos3\alpha + \cdots + cos(2n-1)\alpha) + cos(2n+1)\alpha, \\
y_{2n+1}(\alpha) &= \operatorname{sen}(2n+1)\alpha.
\end{aligned}$$

Por la Proposición 2.2.15, se cumple

$$2\sum_{j=1}^{n} T_{2j-1}(x) + T_{2n+1}(x) = xU_{2n}(x).$$

Entonces,

$$\begin{aligned}
x_{2n+1}(\alpha) &= 2(\cos\alpha + cos3\alpha + \cdots + cos(2n-1)\alpha) + cos(2n+1)\alpha \\
&= 2\sum_{j=1}^{n} T_{2j-1}(x) + T_{2n+1}(x) \\
&= x\, U_{2n}(x) \\
&= \cos\alpha\, U_{2n}(x).
\end{aligned}$$

Y también,

$$\begin{aligned} y_{2n+1}(\alpha) &= \operatorname{sen}(2n+1)\alpha \\ &= \operatorname{sen}\alpha\left(\frac{\operatorname{sen}(2n+1)\alpha}{\operatorname{sen}\alpha}\right) \\ &= \operatorname{sen}\alpha\, U_{2n}(\cos\alpha). \end{aligned}$$

Por lo tanto,

$$y_{2n+1}(\alpha) = \operatorname{sen}\alpha U_{2n}(\cos\alpha).$$

$\square$

Observemos que las siguientes desigualdades son válidas

$$x_{2n+1}(\frac{\pi}{4n}) < x_{2n+1}(\alpha) < 2n+1, \text{ y}$$
$$0 \leqslant y_{2n+1}(\alpha) \leqslant 1.$$

Además, $y_{2n+1}(0) = 0$ y como $\angle OA_{2n}A_{2n+1} = 90^o$, entonces $\alpha + 2n\alpha = \frac{\pi}{2}$ (ver el triángulo $OA_{2n}A_{2n+1}$ en la Figura 2.9). Despejando a α obtenemos lo siguiente

$$\alpha = \frac{\pi}{4n+2}.$$

Por lo tanto,

$$y_{2n+1}(\frac{\pi}{4n+2}) = 1.$$

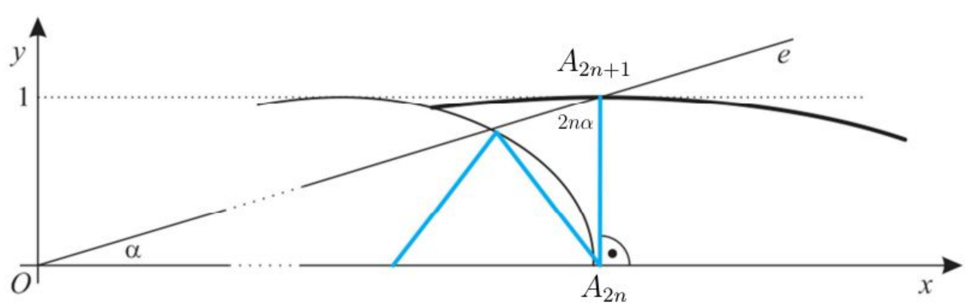

Figura 2.9: Generalización de la trisectriz hasta el punto A_{2n+1} en la línea e.

Corolario 2.2.18. *En caso de vértices A_n (con $n \geqslant 1$) el sistema de ecuaciones paramétricas de las curvas es*

$$\begin{aligned} x_n(\alpha) &= \cos\alpha U_{n-1}(cos\alpha), \\ y_n(\alpha) &= \operatorname{sen}\alpha U_{n-1}(cos\alpha). \end{aligned} \tag{2.9}$$

con $x = cos\alpha$.

Demostración. Por el Teorema 2.2.17 haciendo $n = 2k+1$, obtenemos

$$\begin{aligned} x_n(\alpha) &= x_{2k+1}(\alpha) \\ &= \cos\alpha U_{2k}(cos\alpha) \\ &= \cos\alpha U_{n-1}(cos\alpha) \\ &= \cos\alpha U_{n-1}(cos\alpha) \end{aligned}$$

y también

$$\begin{aligned} y_n(\alpha) &= y_{2k+1}(\alpha) \\ &= sen\alpha U_{2k+1}(\cos\alpha) \\ &= \operatorname{sen}\alpha U_{n-1}(cos\alpha). \end{aligned}$$

□

Definición 2.2.19. *La ecuación polar de A_{2n+1} es*

$$\rho(\alpha) = U_{2n}(\cos\alpha), \quad 0 \leqslant \alpha < \frac{\pi}{4n}. \tag{2.10}$$

Proposición 2.2.20. *La ecuación polar de las curvas cuando $\alpha \in (0, 2\pi)$ es*

$$\rho_n(\alpha) = U_{n-1}(\cos\alpha). \tag{2.11}$$

Demostración. Por Corolario 2.2.18, sabemos que

$$\begin{aligned} x_n(\alpha) &= \cos\alpha U_{n-1}(cos\alpha) \\ y_n(\alpha) &= \operatorname{sen}\alpha U_{n-1}(cos\alpha). \end{aligned}$$

Entonces,

$$\begin{aligned} U_{n-1}^2(cos\alpha) &= \left(\cos^2\alpha + \operatorname{sen}^2\alpha\right) U_{n-1}^2(cos\alpha) \\ &= \cos^2\alpha U_{n-1}^2(cos\alpha) + \operatorname{sen}^2\alpha U_{n-1}^2(cos\alpha) \\ &= x_n^2(\alpha) + y_n^2(\alpha) \\ &= \rho_n(\alpha)^2. \end{aligned}$$

Así, concluimos que $\rho_n(\alpha) = U_{n-1}(\cos\alpha)$. □

Proposición 2.2.21. *Derivado de la Ecuación paramétrica 2.9 tenemos*

$$a) \qquad x_n^2 + y_n^2 = U_{n-1}^2(cos\alpha), \tag{2.12}$$

$$b) \qquad \cos^2\alpha = \frac{x^2}{x^2+y^2}. \tag{2.13}$$

Demostración. De la ecuación (2.9),

a)

$$\begin{aligned} x_n^2 + y_n^2 &= \cos^2\alpha\, U_{n-1}^2(cos\alpha) + \operatorname{sen}^2\alpha\, U_{n-1}^2(cos\alpha) \\ &= U_{n-1}^2(cos\alpha)(\cos^2\alpha + \operatorname{sen}^2\alpha) = U_{n-1}^2(cos\alpha) \end{aligned}$$

b)

$$\frac{x^2}{x^2+y^2} = \frac{\cos^2\alpha U_{n-1}^2(cos\alpha)}{U_{n-1}^2(\cos\alpha)} = \cos^2\alpha.$$

□

Proposición 2.2.22. *La ecuación cartesiana de las curvas definidas por (2.9) es*

$$x^2 + y^2 = U_{n-1}^2\left(\sqrt{\frac{x^2}{x^2+y^2}}\right). \tag{2.14}$$

Demostración. Sabemos por el Corolario 2.2.18 que:

$$\begin{aligned} x_n(\alpha) &= \cos\alpha U_{n-1}(cos\alpha) \\ y_n(\alpha) &= \operatorname{sen}\alpha U_{n-1}(cos\alpha). \end{aligned}$$

Entonces,

$$x^2 + y^2 = \cos^2 x U_{n-1}^2(\cos x) + \operatorname{sen}^2 x U_{n-1}^2(\cos x) = U_{n-1}^2(\cos x).$$

Finalmente por la ecuación (2.13) obtenemos,

$$U_{n-1}^2(\cos x) = U_{n-1}^2\left(\sqrt{\frac{x^2}{x^2+y^2}}\right).$$

□

Teorema 2.2.23. *Si $n = 2k+1$ las curvas definidas por las ecuaciones (2.1) y (2.11) para $a = 1$ son iguales.*

Demostración. Ya que

$$\begin{aligned}
\operatorname{sen}(2k+1)\alpha &= \operatorname{sen}\left(k+(k+1)\right)\alpha \\
&= \operatorname{sen} k\alpha\cos(k+1)\alpha + \cos k\alpha \operatorname{sen}(k+1)\alpha \\
&= \operatorname{sen} k\alpha\cos(k+1)\alpha + \cos k\alpha[\operatorname{sen} k\alpha\cos\alpha + \cos k\alpha \operatorname{sen}\alpha] \\
&= \operatorname{sen} k\alpha\cos(k+1)\alpha + \operatorname{sen} k\alpha\cos k\alpha\cos\alpha + \cos^2 k\alpha \operatorname{sen}\alpha \\
&= 2\operatorname{sen} k\alpha\cos(k+1)\alpha + \operatorname{sen}^2 k\alpha \operatorname{sen}\alpha + \cos^2 k\alpha \operatorname{sen}\alpha \\
&= 2\operatorname{sen} k\alpha\cos(k+1)\alpha + \operatorname{sen}\alpha.
\end{aligned}$$

Si en la ecuación (2.1) hacemos $\varphi = \alpha$ entonces tenemos,

$$\begin{aligned}
U_{2k}(\cos\alpha) &= \frac{\operatorname{sen}(2k+1)\alpha}{\operatorname{sen}\alpha} \\
&= \frac{2\operatorname{sen} k\alpha\cos(k+1)\alpha + \operatorname{sen}\alpha}{\operatorname{sen}\alpha} \\
&= 1 + 2\frac{\operatorname{sen} k\alpha\cos(k+1)\alpha}{\operatorname{sen}\alpha}.
\end{aligned}$$

□

Proposición 2.2.24. *Si $n = -4$ entonces la curva definida por la ecuación (2.11) es la curva de hojas $\rho_n(\alpha) = \cos\varphi(4a\operatorname{sen}^2\varphi - b)$ donde $a = 2$ y $b = 4$.*

Demostración. Sea $n = -4$,

$$\begin{aligned}
\rho_n(\varphi) &= U_{n-1}(\cos\varphi) = U_{-5}(\cos\varphi) \\
&= -U_3(\cos\varphi) = -U_{2+1}(\cos\varphi) \\
&= -(2\cos\varphi U_2(\cos\varphi) - U_1(\cos\varphi) \\
&= -(2\cos\varphi(2xU_1(x) - U_0(x)) - U_1(\cos\varphi)) \\
&= -(2\cos\varphi(2\cos\varphi(2\cos\varphi) - 1) - 2\cos\varphi) \\
&= -8\cos^3\varphi + 2\cos\varphi + 2\cos\varphi \\
&= -8\cos^3\varphi + 4\cos\varphi = -4\cos\varphi(2\cos^2\varphi - 1) \\
&= \cos\varphi(-8\cos^2\varphi + 4) \\
&= \cos\varphi(-8(1-\operatorname{sen}^2\varphi) + 4) = \cos\varphi(-8(1-\operatorname{sen}^2\varphi) + 4) \\
&= \cos\varphi(-8 + 8\operatorname{sen}^2\varphi + 4) = \cos\varphi(8\operatorname{sen}^2\varphi - 4).
\end{aligned}$$

Por lo que $\rho_n(\varphi) = \cos\varphi(4a\operatorname{sen}^2\varphi - b)$ con $a = 2$ y $b = 4$. □

Las siguientes ecuaciones cartesianas las podemos consultar en [8, p. 44].

Proposición 2.2.25. *Las ecuaciones cartesianas para (2.14) son las siguientes.*

a) $x^2 + y^2 = 1$ *para* $|n| = 1$ *(Círculo, Figura 2.10);*

b) $(x^2 + y^2)^2 = 4x^2$ *para* $|n| = 2$ *(Dos círculos tangentes, Figura 2.11);*

c) $(x^2 + y^2)^3 = (3x^2 - y^2)^2$ *para* $|n| = 3$ *(Cisoide de Ceva, Figura 2.12);*

d) $(x^2 + y^2)^4 = 16x^2(x^2 - y^2)^2$ *para* $|n| = 4$ *(Unión de la Curva de hojas, Figura 2.13);*

e) $(x^2 + y^2)^5 = (5x^4 - 10x^2y^2 + y^4)^2$ *para* $|n| = 5$ *(Sectriz de Ceva, Figura 2.14);*

Demostración. a)

$$x^2 + y^2 = U_{1-1}^2\left(\sqrt{\frac{x^2}{x^2+y^2}}\right) = U_0^2(x) = (1)^2 = 1.$$

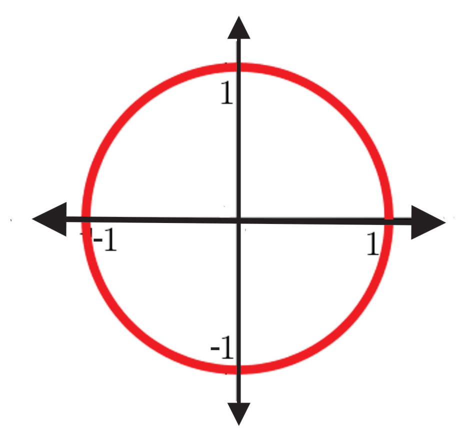

Figura 2.10: Círculo.

b)

$$\begin{aligned}(x^2+y^2)^2 &= \left(U_{n-1}^2\left(\sqrt{\frac{x^2}{x^2+y^2}}\right)\right)^2\\ &= \left(U_{2-1}^2\left(\sqrt{\frac{x^2}{x^2+y^2}}\right)\right)^2\\ &= \left(2\left(\sqrt{\frac{x^2}{x^2+y^2}}\right)\right)^4\\ &= \left(4\frac{x^2}{x^2+y^2}\right)^2\\ &= \frac{(4x^2)^2}{(x^2+y^2)^2}.\end{aligned}$$

Entonces,

$$((x^2+y^2)^2)^2 = (4x^2)^2.$$

Así, $(x^2+y^2)^2 = 4x^2$.

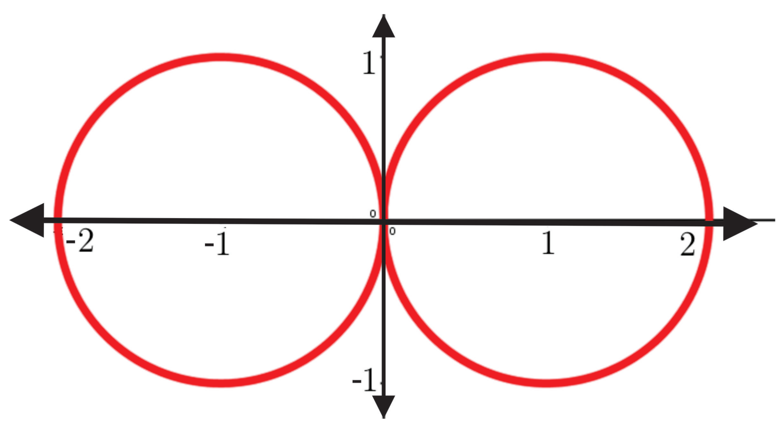

Figura 2.11: Dos circulos tangentes.

c)

$$
\begin{aligned}
(x^2+y^2)^3 &= \left(U_{n-1}^2\left(\sqrt{\frac{x^2}{x^2+y^2}}\right)\right)^3 \\
&= \left(U_{3-1}^2\left(\sqrt{\frac{x^2}{x^2+y^2}}\right)\right)^3 \\
&= \left(\left(4\left(\sqrt{\frac{x^2}{x^2+y^2}}\right)^2-1\right)^2\right)^3 \\
&= \left(\left(4\frac{x^2}{x^2+y^2}-1\right)^2\right)^3 \\
&= \left(\left(\frac{3x^2-y^2}{x^2+y^2}\right)\left(\frac{3x^2-y^2}{x^2+y^2}\right)\right)^3 \\
&= \left(\frac{(3x^2-y^2)^2}{(x^2+y^2)^2}\right)^3.
\end{aligned}
$$

Entonces,

$$
\begin{aligned}
(x^2+y^2)^3 &= \left(\frac{(3x^2-y^2)^2}{(x^2+y^2)^2}\right)^3, \\
(x^2+y^2)^3((x^2+y^2)^2)^3 &= ((3x^2-y^2)^2)^3, \\
((x^2+y^2)^3)^3 &= ((3x^2-y^2)^2)^3, \\
(x^2-y^2)^3 &= (3x^2-y^2)^2.
\end{aligned}
$$

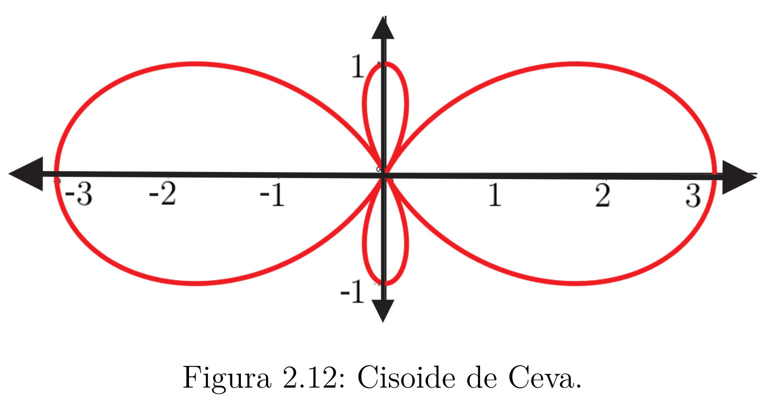

Figura 2.12: Cisoide de Ceva.

d)

$$
\begin{aligned}
(x^2+y^2)^4 &= \left(U_3^2\left(\sqrt{\frac{x^2}{x^2+y^2}}\right)\right)^4\\
&= \left(\left(8\left(\sqrt{\frac{x^2}{x^2+y^2}}\right)^3 - 4\left(\sqrt{\frac{x^2}{x^2+y^2}}\right)\right)^2\right)^4\\
&= \left(64\left(\sqrt{\frac{x^2}{x^2+y^2}}\right)^3 - 64\left(\sqrt{\frac{x^2}{x^2+y^2}}\right)^2 + 16\left(\sqrt{\frac{x^2}{x^2+y^2}}\right)\right)^4\\
&= \left(64\frac{(x^2)^3}{(x^2+y^2)^3} - 64\frac{(x^2)^2}{(x^2+y^2)^2} + 16\frac{(x^2)^2}{(x^2+y^2)}\right)^4\\
&= \left(64\frac{(x^2)^3}{(x^2+y^2)^3} - 64\frac{(x^2)^2(x^2+y^2)^2}{(x^2+y^2)^3} + 16\frac{(x^2)^2(x^2+y^2)}{(x^2+y^2)^3}\right)^4
\end{aligned}
$$

$$
\begin{aligned}
&= \left(\frac{64x^6 - 64x^6 - 64x^4y^2 + 16x^6 + 32x^4y^2 + 16x^2y^4}{(x^2+y^2)^3}\right)^4\\
&= \left(\frac{16x^6 - 32x^4y^2 + 16x^2y^4}{(x^2+y^2)^3}\right)^4.
\end{aligned}
$$

Así,

$$
\begin{aligned}
(x^2+y^2)^4(x^2+y^2)^14 &= (16x^6 - 32x^4y^2 + 16x^2y^4)^4,\\
((x^2+y^2)^4)^4 &= (16x^6 - 32x^4y^2 + 16x^2y^4)^4,\\
((x^2+y^2)^4)^4 &= (16x^2(x^4 - 2x^2y^2 + y^4))^4,\\
(x^2+y^2)^4 &= 16x^2(x^2-y^2)^2.
\end{aligned}
$$

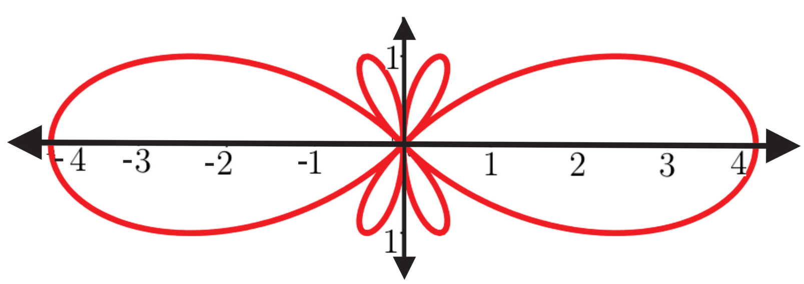

Figura 2.13: Unión de la curva de hojas.

e)

$$\begin{aligned}
(x^2+y^2)^5 &= \left(U_{5-1}^2\left(\sqrt{\frac{x^2}{x^2+y^2}}\right)\right)^5 \\
&= \left(U_4^2\left(\sqrt{\frac{x^2}{x^2+y^2}}\right)\right)^5 \\
&= \left(\left(16\left(\sqrt{\frac{x^2}{x^2+y^2}}\right)^4 - 12\left(\sqrt{\frac{x^2}{x^2+y^2}}\right)^2 + 1\right)^2\right)^5 \\
&= \left(\left(16\left(\frac{x^2}{x^2+y^2}\right)^2 - 12\left(\frac{x^2}{x^2+y^2}\right) + 1\right)^2\right)^5
\end{aligned}$$

$$\begin{aligned}
&= \left(256\left(\frac{x^2}{x^2+y^2}\right)^4 - 384\left(\frac{x^2}{x^2+y^2}\right)^3 + \cdots + \left(\frac{x^2+y^2}{x^2+y^2}\right)\right)^5 \\
&= \left(256\frac{(x^2)^2}{(x^2+y^2)^4} - 384\frac{(x^2)^3(x^2+y^2)}{(x^2+y^2)^4} + \cdots + \frac{x^2+y^2}{x^2+y^2}\right)^5 \\
&= \left(\frac{25x^8 - 100x^6y^2 + 110x^4y^4 - 20x^2y^6 + y^8}{(x^2+y^2)^4}\right)^5.
\end{aligned}$$

Entonces,

$$\begin{aligned}
(x^2+y^2)^5(x^2+y^2)^{20} &= (25x^8 - 100x^6y^2 + 110x^4y^4 - 20x^2y^6 + y^8)^5, \\
((x^2+y^2)^5)^5 &= (25x^8 - 100x^6y^2 + 110x^4y^4 - 20x^2y^6 + y^8)^5, \\
(x^2+y^2)^5 &= 25x^8 - 100x^6y^2 + 110x^4y^4 - 20x^2y^6 + y^8, \\
(x^2+y^2)^5 &= (5x^4 - 10x^2y^2 + y^4)^2.
\end{aligned}$$

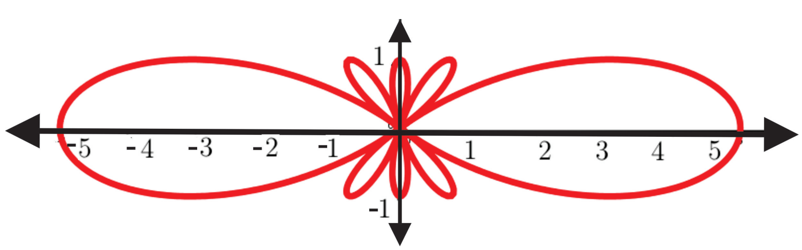

Figura 2.14: Trisectriz de Ceva.

□

Por lo tanto, para $n = 5$, $(x^2 + y^2)^5 = (5x^4 - 10x^2y^2 + y^4)^2$.

Capítulo 3

Haciendo Álgebra con regla y compás

Por razones estéticas, matemáticas o filosóficas, los matemáticos griegos consideraron a la *recta* y al *círculo* como las únicas figuras geométricas perfectas. De hecho, la regla debería ser una regla sin marcas y de un solo lado. En la primera sección de este capítulo veremos una serie de definiciones y proposiciones necesarias para poder demostrar la imposibilidad de los tres problemas griegos, las cuales podemos consultar en [3].

3.1. Extensión de Campos

Definición 3.1.1. *Un campo F es un conjunto en el cual se definen dos operaciones $+$, $\cdot$ (llamadas adición y multiplicación, respectivamente) de modo que para cualquier par de elementos a, b en F, existen elementos únicos $a+b$ y $a \cdot b$ en F tales que se cumplen las siguientes condiciones, para todos los elementos a, b, c en F.*

1. $a + b = b + a$ *y* $a \cdot b = b \cdot a$.
   (Conmutatividad de la adición y la multiplicación).

2. $(a + b) + c = a + (b + c)$ *y* $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.
   (Asociatividad de la adición y la multiplicación).

3. *Existen elementos distintos* 0 *y* 1 *en* F *tales que*

$$0 + a = a \quad y \quad 1 \cdot a = a.$$

(Existencia de elementos identidad para la adición y la multiplicación).

4. *Para cada elemento a en F y cada elemento no nulo b en F, existen elementos c y d en F tales que*

$$a + c = 0 \quad y \quad b \cdot d = 1.$$

   (Existencia de inversos para la adición y la multiplicación).

5. $a \cdot (b + c) = a \cdot b + a \cdot c$.
   (Distributividad de la multiplicación sobre la adición).

Definición 3.1.2. *Un espacio vectorial V sobre un campo F es un grupo abeliano respecto a la adición " + " tal que para todo $\alpha \in F$ y todo $v \in V$, existe un elemento $\alpha v \in V$ de tal modo que:*

1. $\alpha(v_1 + v_2) = \alpha v_1 + \alpha v_2$, *para* $\alpha \in F$, $v_1, v_2 \in V$.
2. $(\alpha + \beta)v = \alpha v + \beta v$, *para* $\alpha, \beta \in F$, $v \in V$.
3. $\alpha(\beta v) = (\alpha\beta)v$, *para* $\alpha, \beta \in F$, $v \in V$.
4. $1v = v$ *para todo* $v \in V$, *donde* 1 *es el elemento identidad de* F.

Definición 3.1.3. *Dados K y F dos campos tales que $K \supset F$, en tal situación se dice que K es una extensión (o campo extensión) de F y a F un subcampo de K.*

Ejemplo 3.1.4. *Denotamos el campo de los números complejos por $\mathbb{C}$, el de los números reales por $\mathbb{R}$ y el de los números racionales por $\mathbb{Q}$.*

- $\mathbb{R}$ *es una extensión de* $\mathbb{Q}$.
- $\mathbb{C}$ *es una extensión de* $\mathbb{Q}$ *y de* $\mathbb{R}$.

Definición 3.1.5. *Sean V un espacio vectorial y F un campo, la dimensión de V sobre F es el número de elementos de cualquier base de V sobre F.*

Definición 3.1.6. *El grado de K sobre F es la dimensión de K como espacio vectorial sobre F y se denota $\dim_F(K)$.*

Definición 3.1.7. *Se dice que K es una extensión finita de F si considerado como espacio vectorial sobre F, $\dim_F(K)$ es finita. Se expresará $\dim_F(K)$ como $[K : F]$ y se le llamará grado de K sobre F.*

Notación 3.1.8. *Denotamos por* $\mathbb{K}[x]$ *al conjunto de los polinomios en* x *sobre* K.

Definición 3.1.9. *Sean* K *un campo y* $f(x) \in \mathbb{K}[x]$, *no constante. El polinomio* $f(x)$ *es irreducible sobre* K *o es un polinomio irreducible en* $\mathbb{K}[x]$ *si* $f(x)$ *no puede expresarse como el producto* $g(x)h(x)$ *de dos polinomios* $g(x)$ *y* $h(x)$ *en* $\mathbb{K}[x]$ *ambos de grado menor que el grado de* $f(x)$.

Ejemplo 3.1.10.

- $p(x) = x^2 - 2$ *es un polinomio irreducible en* $\mathbb{Q}$, *pues* $p(x) = x^2 - 2 = (x + \sqrt{2})(x - \sqrt{2})$ *y* $\sqrt{2} \notin \mathbb{Q}$.
- $p(x) = x^2 + 1$ *es un polinomio irreducible en* $\mathbb{R}$, *pues* $p(x) = x^2 + 1 = (x + i)(x - i)$ *y* $i \notin \mathbb{R}$.

Las siguientes definiciones se pueden consultar en [2, p. 37-38].

Definición 3.1.11. *Un subconjunto* S *de un espacio vectorial* V *es linealmente dependiente si existe un número finito de vectores distintos*

$$x_1, x_2, \ldots, x_n \text{ en } S$$

y escalares $a_1, a_2, \ldots, a_n$ *en* F, *no todos cero, tales que*

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = 0.$$

También se puede describir esta situación diciendo que los elementos de S *son linealmente dependientes.*

Definición 3.1.12. *Se dice que un subconjunto* S *de un espacio vectorial, que no es linealmente dependiente, es linealmente independiente.*

Teorema 3.1.13. *Sean* $L \supset K \supset F$, *tres campos tales que ambos* $[L : K]$ *y* $[K : F]$ *son finitos. Entonces* L *es una extensión finita de* F *y satisface,*

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

Demostración. Escribiremos explícitamente una base de L sobre F. Supongamos que $[L : K] = m$ y que $[K : F] = n$. Sea $\{v_1, v_2, ..., v_m\}$ una base de L sobre K y $\{w_1, w_2, ..., w_n\}$ una base de K sobre F. Mostraremos que los elementos de la forma v_iw_j donde $i \in \{1, 2, ..., m\}$ y $j \in \{1, 2, ..., n\}$, son base de L sobre F. Nótese que al menos tal colección tiene el número exacto de elementos.

Afirmación. El conjunto $\{v_iw_j : i \in \{1, 2, ..., m\}$ y $j \in \{1, 2, ..., n\}\}$ forma una base de L sobre F.
Primero veremos que todo elemento de L es combinación lineal de estos mn elementos con coeficientes en F, posteriormente mostraremos que estos mn elementos son linealmente independientes. Sea l un elemento cualquiera de L. Como todo elemento de L es combinación lineal de $v_1, v_2, ..., v_m$ con coeficientes en K, el elemento l debe ser en particular de la forma $l = k_1v_1 + k_2v_2 + \cdots + k_mv_m$ donde los elementos $k_1, ..., k_m \in K$. Como todo elemento de K es una combinación lineal de $w_1, w_2, ..., w_n$ con coeficientes en F. Entonces,

$$k_i = f_{11}w_1 + \cdots + f_{in}w_n$$

donde todos los f_{ij} están en F para todos $i \in \{1, 2, ..., m\}$ y $j \in \{1, 2, ..., n\}$. Sustituyendo las expresiones de los k_i en $l = k_1v_1 + \cdots + k_mv_m$ obtenemos, $l = (f_{11}v_1 + f_{12}v_2 + \cdots + f_{1n}v_n)w_1 + \cdots + (f_{m1}w_1 + \cdots + f_{mn}v_n)w_m$, efectuando las operaciones indicadas usando las propiedades distributiva y asociativa, tenemos $l = f_{11}v_1w_1 + f_{12}v_2w_1 + \cdots + f_{ij}v_jw_i + \cdots + f_{mn}v_nw_m$, como los f_{ij} están en F, hemos expresado a l como combinación lineal sobre F de los elementos v_iw_j. De esta manera, los elementos v_iw_j generan ciertamente a L sobre F. Por lo tanto, $[L : F]$ es finito.

Ahora veamos que los elementos v_iw_j son linealmente independientes sobre F. Supongamos que $f_{11}v_1w_1 + f_{12}v_1w_1 + \cdots + f_{1n}v_1w_n + f_{21}v_2w_1 + \cdots + f_{2n}v_2w_n + \cdots + f_{m1}v_mw_1 + \cdots + f_{mn}v_mw_n = 0$, donde los f_{ij} están todos en F. Reagrupando la expresión anterior, se tiene que $c_1v_1 + c_2v_2 + \cdots + c_mv_m = 0$ donde $c_i = f_{i1}w_1 + \cdots + f_{in}w_n$ puesto que los elementos c_i están en K y los elementos $v_1, v_2, ..., v_n$ de L son linealmente independientes sobre K se tiene que $c_1 = c_2 = \cdots = c_m = 0$. Recordando que $c_i = f_{i1}w_1 + \cdots + f_{in}w_n$ donde los f_{ij} están en F y $w_1, w_2, ..., w_n \in K$ son linealmente independientes sobre F, se deduce que $f_{ij} = 0$ para todo $i \in \{1, 2, ..., m\}$ y $j \in \{1, 2, ..., n\}$. Por consiguiente solo la combinación lineal trivial con todos los coeficientes cero de los elementos v_iw_j sobre F pueden ser cero. Por lo tanto, los v_iw_j son linealmente independientes sobre F. Hemos probado que los mn elementos v_iw_j forman una base de L sobre F. Luego $[L : F] = mn$, como $m = [L : K]$ y $n = [K : F]$ hemos obtenido el resultado buscado, es decir, $[L : F] = [L : K][K : F]$. □

Las demostraciones de los siguientes Teoremas se pueden consultar en [3, p. 187–188].

Teorema 3.1.14. *Supóngase que V es dimensionalmente finito sobre F, entonces dos bases cualesquiera de V sobre F deben tener el mismo número de elementos y este número es exactamente $dim_F(V)$.*

Teorema 3.1.15. *Sea V un espacio vectorial sobre F tal que la $dim_F(V) = n$. Si $m > n$ entonces m elementos cualesquiera de V son linealmente dependientes sobre F.*

Corolario 3.1.16. *Si $F \subset K \subset L$ son tres campos tales que $[L : F]$ es finito, entonces $[K : F]$ es finito y divide a $[L : F]$.*

Demostración. Como $K \subset L$ no puede tener mas elementos linealmente independientes sobre F que L. Por el Teorema 3.1.15, $[L : F]$ es el tamaño del mayor conjunto de elementos linealmente independientes de L sobre F. En consecuencia $[K : F] \leq [L : F]$, así debe ser finito. Dado que L es finito dimensional sobre F y puesto que K contiene a F, L debe ser finito dimensional sobre K. De esta manera se satisfacen todas las condiciones del Teorema 3.1.13 y se cumple que $[L : F] = [L : K][K : F]$, de donde $[K : F]$ divide a $[L : F]$. □

Teorema 3.1.17. *Supóngase que K es una extensión finita de F de grado n. Entonces, dado cualquier elemento u en K existen elementos $a_0, a_1, ..., a_n$ en F, no todos cero, tales que $a_0 + a_1u + \cdots + a_nu^n = 0$.*

Demostración. Dado que $[K : F] = dim_F(K) = n$ y $\{1, u, u^2, ..., u^n\}$ tiene $n + 1$ elementos, por el Teorema 3.1.15, deben ser linealmente dependientes sobre F, de esta manera se pueden encontrar $a_0, a_1, ..., a_n$ en F, no todos cero, tales que $a_0 + a_1u + \cdots + a_nu^n = 0$. □

Dado $p(x) = \alpha_0x^n + \alpha_1x^{n-1} + \cdots + \alpha_n$, $p(a)$ se entiende por el elemento $\alpha_0a^n + \alpha_1a^{n-1} + \cdots + \alpha_n$ de K.

Definición 3.1.18. *Si $K \supset F$ son campos, entonces se dice que $a \in K$ es algebraico sobre F si existe un polinomio $p(x) \neq 0$ en $\mathbb{F}[x]$ tal que $p(a) = 0$.*

La conclusión del Teorema 3.1.17 quiere decir que, si K es una extensión finita de F, entonces todo elemento de K es algebraico sobre F.

Definición 3.1.19. *Si K es una extensión de F tal que todo elemento de K es algebraico sobre F se dice que K es una extensión algebraica de F.*

En estos terminos el Teorema 3.1.17 se puede reformular como sigue:

Teorema 3.1.20. *Si K es una extensión finita de F entonces K es una extensión algebraica de F.*

Definición 3.1.21. *Un elemento de K que no es algebraico sobre F se dice que es trascendente sobre F.*

Ejemplo 3.1.22. *Considérese $\mathbb{C}$ el campo complejo como una extensión del campo de los racionales $\mathbb{Q}$. El número complejo $a = 1 + i$ es algebraico sobre $\mathbb{Q}$, ya que satisface $a^2 - 2a + 2 = 0$ sobre $\mathbb{Q}$ de manera semejante, el número real $b = \sqrt{1 + \sqrt[3]{1 + \sqrt{2}}}$ es algebraico sobre $\mathbb{Q}$ puesto que $b^2 = 1 + \sqrt[3]{1 + \sqrt{2}}$. Así, desarrollando $\left((b^2 - 1)^3 - 1\right)^2 = 2$ se obtiene que $\left((b^2 - 1)^3 - 1\right)^2 - 2 = b^{12} - 6b^{10} + 15b^8 - 22b^6 + 21b^4 - 12b^2 - 6 = 0$ una expresión polinómica no trivial en b con coeficientes racionales, que es igual a cero y por consiguiente b es algebraico sobre $\mathbb{Q}$.*

Es posible obtener números racionales que sean trascendentes sobre $\mathbb{Q}$ muy fácilmente sin embargo, el establecer la trascendencia de ciertos números conocidos requiere un esfuerzo real. Se sabe que los números π y e son trascendentes sobre $\mathbb{Q}$.

Definición 3.1.23. *Se dice que un número complejo es un número algebraico si es algebraico sobre $\mathbb{Q}$.*

Se verá pronto que los números algebraicos forman un campo, el cual es un subcampo de $\mathbb{C}$. Recordando lo visto en el Teorema 3.1.17, si K es una extensión finita de F, entonces todo elemento de K es algebraico sobre F con base a esta afirmación nos preguntamos ahora ¿se puede producir de algún modo una extensión finita de F usando a? la respuesta es si y es consecuencia del siguiente teorema, el cual se demuestra en un contexto mas general de lo que en verdad se requiere sin embargo daremos una serie de definiciones y proposiciones antes de proseguir.

Definición 3.1.24. *Se dice que un conjunto no vacío R es un anillo si tiene dos operaciones " $+$ " y " $\cdot$ " tales que*

1. *$a,b \in R$ implica que $a + b \in R$.*

2. *$a + b = b + a$ para $a,\ b \in R$.*

3. $(a+b)+c = a+(b+c)$ *para* $a, b, c \in R$.

4. *Existe un elemento* $0 \in R$ *tal que* $a + 0 = a$ *para todo* $a \in R$.

5. *Dado* $a \in R$, *existe un* $b \in R$ *tal que* $a + b = 0$. *(*b *se expresará como* $-a$*).*

Nótese que se ha dicho hasta ahora que R *un grupo abeliano respecto a* $+$. *Ahora se expresan las reglas de la multiplicación en* R.

6. a,$b \in R$ *implica que* $a \cdot b \in R$.

7. $a \cdot (b \cdot c) = (a \cdot b) \cdot a$ *para* $a,\ b, c \in R$.

Esto es todo lo que se exige por lo que se refiere a la multiplicación sola. Mas no se dejan las operaciones $+$ *y* $\cdot$ *aisladas entre sí, sino que se entrelazan mediante las dos leyes distributivas:*

8. $a \cdot (b+c) = (a \cdot b) + (a \cdot c)$ *para* $a, b, c \in R$.

9. $(b+c) \cdot a = (b \cdot a) + (c \cdot a)$ *para* $a, b, c \in R$.

Definición 3.1.25. *Un anillo conmutativo* R *es un dominio entero si* $ab = 0$ *en* R *implica que* $a = 0$ *o bien* $b = 0$.

Definición 3.1.26. *Un anillo con unidad* R, *es un anillo con división si para* $a \neq 0$ *en* R, *existe un elemento* $b \in R$ *(que normalmente se expresa como* a^{-1}*) tal que* $a \cdot a^{-1} = a^{-1} \cdot a = 1$.

Observación 3.1.27. *Un campo es un anillo conmutativo con división.*

Definición 3.1.28. *Si* $p(x) = a_0 + a_1x + \cdots + a_nx^n$ *y* $a_n \neq 0$, *entonces el grado de* $p(x)$, *denotado por grd* $p(x)$, *es* n.

Teorema 3.1.29. *Si* D *es un dominio entero con unidad* 1 *que es un espacio vectorial finito-dimensional sobre un campo* F, *entonces* D *es un campo.*

Demostración. Para demostrar el teorema, dado $a \neq 0$ en D debemos encontrar un elemento a^{-1} en D tal que $aa^{-1} = 1$. Como en la demostración del Teorema 3.1.17, si $dim_F(D) = n$ entonces $1, a, a^2, \ldots, a^n$ en D son linealmente dependientes en D sobre F. De manera que para ciertos $\alpha_0, \alpha_1, \ldots, \alpha_n$ en F apropiados, no todos ellos cero, $\alpha_0a^n + \alpha_1a^{n-1} + \cdots + \alpha_n = 0$. Sea $p(x) = \beta_0x^r + \beta_1x^{r-1} + \cdots + \beta_r \neq 0$ un polinomio en $F[x]$ de grado mínimo

tal que $p(a) = 0$.
Afirmación. $\beta_r \neq 0$.
Supongamos que $\beta_r = 0$, entonces

$$\begin{aligned} 0 &= \beta_0 a^r + \beta_1 a^{r-1} + \cdots + \beta_{r-1} a + 0 \\ &= \left(\beta_0 a^{r-1} + \beta_1 a^{r-2} + \cdots + \beta_{r-1}\right) a \end{aligned}$$

Como D es un dominio entero y $a \neq 0$ se concluye que $\beta_0 a^{r-1} + \beta_1 a^{r-2} + \cdots + \beta_{r-1} = 0$. Por consiguiente $q(a) = 0$, donde $q(x) = \beta_0 x^{r-1} + \beta_1 x^{r-2} + \cdots + \beta_{r-1}$ en $F[x]$ es de grado menor que $p(x)$, pero esto es una contradicción pues $p(x)$ era el de grado mínimo con $p(a) = 0$. De esta manera $\beta_r \neq 0$.
Por lo tanto β_r^{-1} esta en F y

$$\frac{a\left(\beta_0 a^{r-1} + \beta_1 a^{r-2} + \cdots + \beta_{r-1}\right)}{\beta_r} = -1,$$

lo cual da lugar a,

$$\frac{-\left(\beta_0 a^{r-1} + \beta_1 a^{r-2} + \cdots + \beta_{r-1}\right)}{\beta_r},$$

el cual está en D es el a^{-1} requerido en D. □

Definición 3.1.30. *Se dice que un elemento a en la extensión K de F es algebraico de grado n si existe un polinomio $p(x)$ en $F[x]$ de grado n tal que $p(a) = 0$ y ningún polinomio no cero de grado menor en $F[x]$ tiene esta propiedad.*

Definición 3.1.31. *El polinomio $f(x)$ en $F[x]$ es mónico si el coeficiente de su potencia más alta es 1. Así que, si $f(x)$ es mónico significa que $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$.*

Ejemplo 3.1.32. *Los siguientes son ejemplos de polinomios mónicos en $F[x]$*

- $f(x) = x^3 - 6x^2 + 2x + 100$
- $f(x) = x^{100} - 1$
- $f(x) = 100x^{99} + x^{100}$

Se puede suponer que el polinomio $p(x)$ en la Definición 3.1.30 es mónico, ya que se podría dividir dicho polinomio entre su coeficiente de la potencia mayor para obtener un polinomio mónico $q(x)$ en $F[x]$ de igual grado que $p(x)$ y tal que $q(a) = 0$, de ahora en adelante se supone que el polinomio $p(x)$ es mónico y se le llama polinomio mínimo de a sobre F.

Proposición 3.1.33. *Sea $a \in K$ algebraico sobre F con polinomio mínimo $p(x)$ en $F[x]$. Entonces $p(x)$ es irreducible en $F[x]$.*

Demostración. Supongamos que $p(x)$ no es irreducible en $F[x]$; entonces $p(x) = f(x)g(x)$, donde $f(x)$ y $g(x)$ están en $F[x]$ y cada uno tiene grado positivo. Puesto que $0 = p(a)$ entonces $p(a) = f(a)g(a)$ y dado que $f(a)$ y $g(a)$ están en el campo K, se concluye que $f(a) = 0$ o bien $g(a) = 0$, lo cual es imposible, ya que ambos $f(x)$ y $g(x)$ son de grado menor que $f(x)$. Por lo tanto $p(x)$ es irreducible en $F[x]$. □

Definición 3.1.34. *Se dice que un subgrupo N de G es un subgrupo normal de G si $a^{-1}Na \subset N$ para todo $a \in G$.*

Definición 3.1.35. *Sea G un grupo y N un subgrupo normal el grupo factor o grupo cociente de G por N, es $M = \{[a] | a \in G\}$, donde*

$$[a] = \left\{ x \in G | xa^{-1} \in N \right\} = Na,$$

el símbolo que se emplea para M es G/N (léase G sobre N o G mód N).

El siguiente Teorema se puede consultar en [3, p. 155]

Teorema 3.1.36. ***(ALGORITMO DE LA DIVISIÓN)***
Dados los polinomios $f(x)$, $g(x) \in F[x]$, con $g(x) \neq 0$, existen $q(x)$, $r(x) \in F[x]$ tales que

$$f(x) = q(x)g(x) + r(x),$$

donde $r(x) = 0$ o bien grd $r(x) <$ grd $g(x)$.

Sea $a \in K$ algebraico de grado n sobre F y $p(x) \in F[x]$ su polinomio mínimo sobre F. Si $f(x) \in F[x]$, entonces $f(x) = q(x)p(x) + r(x)$ donde $q(x)$, $r(x)$ están en $F[x]$ y $r(x) = 0$ o bien $grd(r(x)) < grd(p(x))$, en virtud del algoritmo de la división. Por lo tanto $f(a) = q(a)p(a) + r(a) = r(a)$ ya que $p(a) = 0$. En forma breve, cualquier expresión polinómica en a sobre F se puede expresar como un polinomio en a de grado $n-1$ a lo sumo.

El siguiente lema se puede consultar en [3, p. 153].

Lema 3.1.37. *Si $p(x)$, $q(x)$ son elementos de $F[x]$ distintos de cero, entonces $grd(p(x)q(x)) = grd(p(x)) + grd(q(x))$.*

Proposición 3.1.38. *Si $F[a] = \{f(a)|f(x) \in F[x]\}$ entonces $F[a]$ es un subcampo de K que contiene tanto a $F[a]$ como a y $[F[a] : F] = n$, con a algebraica de grado n.*

Demostración. Como cualquier expresión polinómica en a sobre F se puede expresar como un polinomio en a de grado $n-1$, $F[a]$ es generado sobre F por $1, a, a^2, \ldots, a^{n-1}$. Por lo tanto es dimensionalmente finito sobre F.
Afirmación. $F[a]$ es un subanillo de K y como tal, $F[a]$ es un dominio entero.
En efecto, pues $K \supset F$ y al ser K una extensión finita de F y al saber que $F[x]$ es el anillo de polinomios en x sobre F, $F[a]$ hereda todas las propiedades que $F[x]$ cumple como anillo, con esto concluimos la demostración de la afirmación.
Para ver que $F[a]$ es un dominio entero, procederemos por contradicción. Si $p(a) \neq 0$ y $q(a) \neq 0$, entonces $grd(p(a)) \geq 0$ y $grd(q(a)) \geq 0$. Por el Lema 3.1.37 $grd(p(a)q(a)) = grd(p(a)) + grd(q(a)) \geq 0$. Por lo tanto, $p(a)q(a)$ tiene grado mayor a 0 y no puede ser 0 (el cual no tiene grado asignado). Por consiguiente, $F[a]$ es un dominio entero.

Por la afirmación anterior y por el Teorema 3.1.29, $F[a]$ es un campo, puesto que es generado sobre F por $1, a, a^2, ..., a^{n-1}$.
Afirmación. $[F[a] : F] = n$.
Para probar esta afirmación se debe probar que $1, a, a^2, ..., a^{n-1}$ son linealmente independientes sobre F. Si $\alpha_0 + \alpha_1 a + \cdots + \alpha_{n-1}a^{n-1} = 0$ con los α_i en F, entonces $q(a) = 0$ donde $q(x) = \alpha_0 + \alpha_1 x + \cdots + \alpha_{n-1}x^{n-1}$ esta en $F[x]$. Puesto que $q(x)$ es de grado menor que $p(x)$, el cual es el polinomio mínimo de a en $F[x]$ se concluye que $q(x) = 0$. Así, $\alpha_0 = \alpha_1 = \cdots = \alpha_{n-1} = 0$. Por lo tanto, $1, a, a^2, ..., a^{n-1}$ son linealmente independientes sobre F y forman una base de $F[a]$ sobre F y $[F[a] : F] = n$. $\square$

Dado que $F[a]$ es un campo se denotará por $F(a)$, obsérvese además que si M es cualquier campo que contiene a ambos F y a, entonces M contiene todas las expresiones polinómicas en a sobre F. Por consiguiente, $F(a) \subset M$ y $F(a)$ es el menor subcampo de K que contiene a ambos F y a.

Definición 3.1.39. *Se llama $F(a)$ al campo o extensión obtenida al agregar a al campo F.*

Definición 3.1.40. *Sea R un anillo. Un subconjunto no vacío I de R se llama ideal de R si:*

1. *I es un subconjunto aditivo de R.*
2. *Dados $r \in R$, $a \in I$, entonces $ra \in I$ y $ar \in I$.*

Definición 3.1.41. *Una aplicación $\psi : R \to R'$ de un anillo R en un anillo R' es un homomorfismo si*

(a) $\psi(a+b) = \psi(a) + \psi(b)$,

(b) $\psi(ab) = \psi(a)\psi(b)$ *para todo* $a, b \in R$.

La demostración del siguiente Teorema se puede consultar en [3, p. 159]

Teorema 3.1.42. *Si $p(x) \in F[x]$, entonces el ideal $\langle p(x) \rangle$ generado por $p(x)$ en $F[x]$ es un ideal máximo de $F[x]$ si y sólo si $p(x)$ es irreducible en $F[x]$.*

La demostración del siguiente Teorema se puede consultar en [3, p. 148]

Teorema 3.1.43. *Sea R un anillo conmutativo con unidad 1 y M un ideal máximo de R. Entonces R/M es un campo.*

Teorema 3.1.44. *Supóngase que $K \supset F$ y que $a \in K$ es algebraico sobre F de grado n. Entonces $F(a)$ el campo obtenido agregando a F el elemento a, es una extensión finita de F y $[F(a) : F] = n$.*

Demostración. Sean $F[x]$ el anillo de los polinomios en x sobre F y $M = \langle p(x) \rangle$ el ideal de $F[x]$ generado por $p(x)$ el polinomio mínimo de a en K sobre F. Por la Proposición 3.1.33, $p(x)$ es irreducible en $F[x]$, y por el Teorema 3.1.42, M es un ideal máximo de $F[x]$. Así, por el Teorema 3.1.43, $F[x]/(p(x))$ es un campo.
Afirmación. La función $\psi : F[x] \to K$ dada por $\psi(f(x)) = f(a)$ es un

homomorfismo.
Dado que

$$\begin{aligned}\psi(f(x)+g(x)) &= \psi((f+g)(x)), \text{ donde } f(x), g(x) \in F[x] \\ &= (f+g)(a) \\ &= f(a)+g(a) \\ &= \psi(f(x))+\psi(g(x)).\end{aligned}$$

Y también,

$$\begin{aligned}\psi(f(x)g(x)) &= \psi((fg)(x)), \text{ donde } f(x), g(x) \in F[x] \\ &= (fg)(a) \\ &= f(a)g(a) \\ &= \psi(f(x))\psi(g(x)).\end{aligned}$$

Se tiene que ψ es un homomorfismo.
Como ψ es un homomorfismo de $F[x]$ en K y la imagen de $F[x]$ en K es simplemente $F(a)$. El núcleo de ψ es $J = \{f(x) \in F[x] : \psi(f(x)) = 0\}$. como se sabe que $\psi(f(x)) = f(a)$, se tiene que $J = \{f(x) \in F[x] : f(a) = 0\}$. Dado que $p(x)$ está en J y es el polinomio mínimo de a sobre F, $p(x)$ es del grado mínimo posible entre los elementos de J. De esta manera $J = (p(x))$ usando la demostración del Teorema 4.5.6 de [3] se tiene que $J = M$. Por el primer Teorema de homomorfismos para anillos (Teorema 4.3.3 en [3]), $F[x]/M = \psi(F[x]) = (F(a))$. Dado que $F[x]/M$ es un campo, se tiene que $F(a)$ es un campo. □

3.2. Extensiones Finitas

Denotamos por $E(K)$ el conjunto de los elementos de K y que son algebraicos sobre F, desde luego $F \subset E(K)$. Nuestro objetivo es probar que $E(K)$ es un campo.

Teorema 3.2.1. *El conjunto $E(K)$ es un subcampo de K.*

Demostración. Lo que probaremos es que si a y $b \in K$ son algebraicos sobre F, entonces $a \pm b$, ab, y a/b (si $b \neq 0$) son algebraicos sobre F. Esto garantizará que $E(K)$ es un subcampo de K.
Sea $K_0 = F(a)$ el subcampo de K que se obtiene agregando a a F. Como a es

algebraico sobre F digamos de grado m, por el Teorema 3.1.44, $[K_0 : F] = m$. Dado que b es algebraico sobre F se tiene que b es algebraico sobre K_0. Si b es algebraico sobre F de grado n, entonces es algebraico sobre K_0 y de grado a lo sumo n. De esta manera $K_1 = K_0(b)$, el subcampo de K obtenido agregando b a K_0, es una extensión finita de K_0 y $[K_1 : K_0] \leqslant n$. Por consiguiente, por el Teorema 3.1.13, $[K_1 : F] = [K_1 : K_0][K_0 : F] \leqslant mn$ y por el Teorema 3.1.17, K_1 es una extensión finita de F. Así, todos sus elementos son algebraicos sobre F. Puesto que $a \in K_0 \subset K_1$ y $b \in K_1$, entonces todos los elementos $a \pm b,\ ab,\ a/b$ están en K_1 y son algebraicos sobre F. □

Teorema 3.2.2. *Si u en K es algebraico sobre $E(K)$, entonces u está en $E(K)$.*

Demostración. Todo lo que se debe hacer es demostrar que u es algebraico sobre F esto colocará a u en $E(K)$ y habremos terminado. Puesto que u es algebraico sobre $E(K)$ existe un polinomio no trivial $f(x) = x^n + a_1x^{n-1} + a_2x^{n-2} + \cdots + a_n$ donde $a_1, a_2, ..., a_n$ están en $E(K)$, tal que $f(u) = 0$. Dado que $a_1, a_2, ..., a_n$ están en $E(K)$ son algebraicos sobre F, supongamos que sus grados son $m_1, m_2, ..., m_n$, respectivamente.
Afirmación. $[F(a_1, ..., a_n) : F] = m_1m_2 \cdots m_n$.
Para tal fin, simplemente se llevará a cabo n aplicaciones sucesivas del Teorema 3.1.13 a la sucesión $K_1, K_2, ..., K_n$ de campos. De esta manera, dado que u es algebraico sobre el campo $K_n = F(a_1, a_2, ..., a_n)$, (después de todo, el polinomio que u satisface es $p(x) = x^n + a_1x^{n-1} + \cdots + a_n$, el cual tiene todos sus coeficientes en $F(a_1, a_2, ..., a_n)$), el campo $K_n(u)$ es una extensión finita de K_n y puesto que K_n es una extensión finita de F se tiene de nuevo por el Teorema 3.1.13 que $K_n(u)$ es una extensión finita de F. Como $u \in K_n(u)$, del Teorema 3.1.17 se obtiene que u es algebraico sobre F. Esto situa a u en $E(K)$ por la misma definición de $E(K)$. □

3.3. Construcciones con regla y compás

Como ya mencionamos en el capítulo 1, el problema de la trisección del ángulo (dividir un ángulo dado en tres partes iguales) junto con la duplicación del cubo (construir un cubo cuyo volumen sea el doble del de un cubo dado) y la cuadratura del círculo (construir un cuadrado con la misma área de un círculo dado) forman un grupo de problemas imposibles, llamados “los tres problemas griegos”.

Proposición 3.3.1. *Podemos construir con regla y compás, una recta perpendicular ℓ' a una recta dada ℓ.*

Demostración. Sea ℓ una recta construible que pasa por los puntos A y B, y sea P un punto en ℓ distinto de B. Luego, se puede construir una circunferencia (con compás) de radio PB tal que corte a ℓ en B y B', después construimos dos circunferencias (con compás) de radio BB' con centro en B' y B las cuales se intersectan en dos puntos Q y S. Por lo tanto la recta que une a Q y S llamada ℓ' es perpendicular a ℓ y además es construible con regla y compás véase Figura 3.1. □

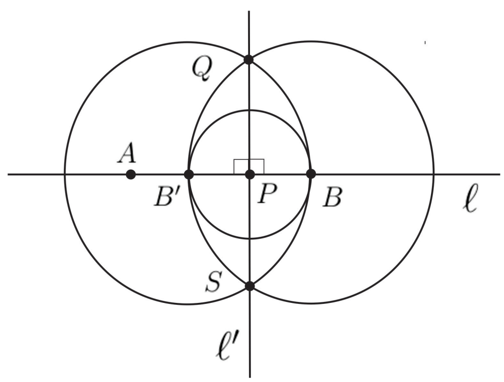

Figura 3.1: Construcción de una recta perpendicular a ℓ.

Teorema 3.3.2. *Podemos construir con regla y compás, una recta paralela ℓ' a una recta dada ℓ que pase por un punto dado P.*

Demostración. Sea ℓ una recta construible, P un punto en la recta ℓ y Q un punto exterior a la recta. Luego con el compás trazamos la circunferencia S de radio PQ y centro en P, la cual corta a la recta ℓ en dos puntos A y A'. Después, trazamos una circunferencia S' de radio AQ con centro en A' la cual cortará a S en el punto O. Así, concluimos que la recta ℓ' que pasa por el punto Q y O es paralela a la recta ℓ que pasa por el punto A y A' véase Figura 3.2. □

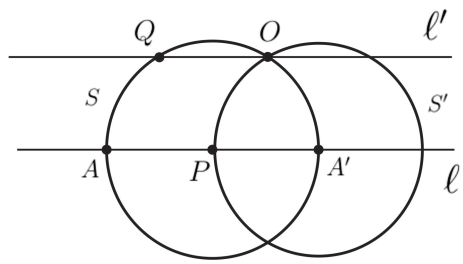

Figura 3.2: Construcción de una recta paralela a una recta dada.

Definición 3.3.3. *Un número α se dice que es un número construible si únicamente usando la regla y el compás podemos construir un segmento rectilíneo de longitud α.*

Teorema 3.3.4. *Si α y β son construibles entonces también lo son:*

a) $\alpha + \beta$ *es construible,*

b) $\alpha - \beta$ *es construible,*

c) $\alpha\beta$ *es construible,*

d) $\frac{\alpha}{\beta}$ *es construible si* $\beta \neq 0$.

Demostración. a) Por hipótesis tenemos un segmento $\overline{AB}$ de longitud α, y también otro segmento $\overline{CD}$ de longitud β como en la Figura 3.3. Construimos primero la recta que contiene al segmento $\overline{AB}$ y luego el círculo con centro B y radio $\beta = CD$. Sea E el punto de intersección de la recta L_{AB} con este círculo y tal que la longitud orientada de BE es β. Se tiene que $AE = AB + BE = \alpha + \beta$.

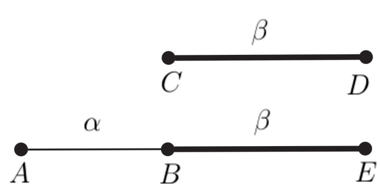

Figura 3.3: $\alpha + \beta$ es construible.

b) Sea ℓ una recta en la cual encontramos al segmento $\overline{AE}$ de longitud α y también otro segmento $\overline{CD}$ de longitud β. Construyamos primero la recta que contiene al segmento $\overline{AE}$ y luego el círculo con centro en E y radio $\beta = CD$. Sea B el punto de intersección de la recta L_{AB} con este círculo tal que la longitud orientada de BE es β. Se tiene que: $AE - BE = \alpha - \beta = BA$, véase Figura 3.4.

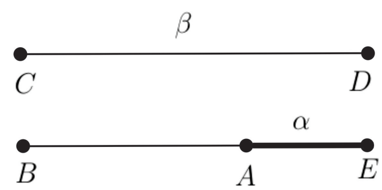

Figura 3.4: $\alpha - \beta$ es construible.

c) Construyamos primero la recta ℓ que pasa por A y B, luego la recta ℓ' perpendicular a ℓ por el punto A. Como se puede elegir una unidad de longitud, se puede escoger un punto U en ℓ tal que $AU = 1$, usando compás. Marquemos los puntos A y B en ℓ tales que $AB = \alpha$. Tracemos ahora el círculo de centro A y radio β con C el punto de intersección de este círculo con la perpendicular ℓ', tal que la longitud orientada $AC = \beta$. Construyase la recta $\overleftrightarrow{CU}$ y la recta paralela a $\overleftrightarrow{CU}$ por el punto B (usando regla y compás), sea D el punto de intersección de esta paralela con ℓ' y sea $AD = \gamma$, se sigue que $\gamma = AD = AB \cdot AC = \alpha\beta$. Por semejanza de triángulos se tienen las siguientes razones de semejanza $\frac{AB}{AU} = \frac{AD}{AC}$, entonces $\frac{AB}{1} = \frac{AD}{AC}$. Así, $AD = AB \cdot AC = \alpha\beta$, véase Figura 3.5.

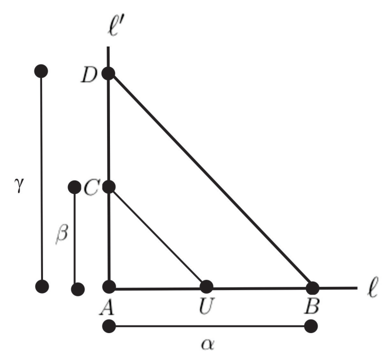

Figura 3.5: $\alpha\beta$ es construible.

d) Construyamos la recta ℓ que pasa por A y B tal que $AB = \alpha$ luego la recta ℓ' perpendicular a ℓ por el punto A y sea C en ℓ' tal que $AC = \beta \neq 0$.

Como se puede elegir una unidad de longitud se puede escoger un punto U en ℓ' tal que $AU = 1$ (usando compás). Construyamos la recta $\overleftrightarrow{CB}$ y la recta paralela a $\overleftrightarrow{CB}$ por el punto U. Sea D el punto de intersección de esta recta paralela con ℓ. Entonces, por semejanza de triángulos obtenemos que $\frac{AB}{AD} = \frac{AC}{AU}$, de modo que $\frac{AB}{AD} = AC$. Así, $\frac{\alpha}{AD} = \beta$ y $\frac{\alpha}{\beta} = AD$, véase Figura 3.6. $\square$

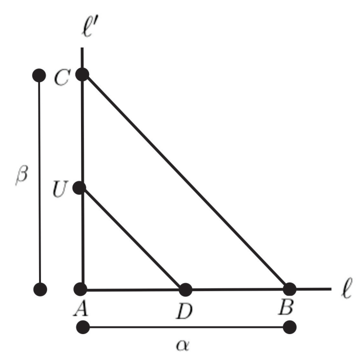

Figura 3.6: $\frac{\alpha}{\beta}$ es construible.

Teorema 3.3.5. *Podemos sacar la raíz cuadrada con regla y compás de un número construible.*

Demostración. Primeramente trazamos un segmento $\overline{AB}$ de longitud a en una recta dada ℓ, es decir de longitud igual al número del cual queremos sacar su raíz cuadrada. Posteriormente extendemos el segmento $\overline{AB}$ una unidad en dirección opuesta, luego trazamos un círculo que tenga como diámetro el segmento $\overline{AC}$. Finalmente, en el punto B (donde se empieza la extensión de longitud 1) trazamos una línea perpendicular a $\overline{AC}$ la cual corta a la circunferencia en dos puntos H y P, véase Figura 3.7.

Afirmación. El segmento BH es la raíz cuadrada de a.

Observemos que el triángulo ABH es semejante al triángulo HBC, entonces $\frac{BC}{BH} = \frac{BH}{AB}$, pero $BC = 1$ de lo que se tiene que $\frac{1}{BH} = \frac{BH}{AB}$. Entonces $(AB) = (BH)^2$. Así, $BH = \sqrt{a}$. $\square$

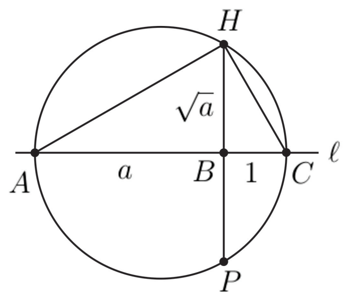

Figura 3.7: Raíz cuadrada de un número construible a.

Definición 3.3.6. *Sea F un subcampo cualquiera del campo de los números reales, consideremos todos los puntos (x, y) en el plano real euclidiano cuyas coordenadas x e y están en F; llamamos al conjunto de estos puntos el plano de F.*

El siguiente teorema lo podemos consultar en [12, p. 135].

Teorema 3.3.7. *Sea $P \subseteq \mathbb{R}^2$ un conjunto con al menos dos puntos. Si α, β son números reales construibles a partir de P, entonces también $\alpha + \beta, \alpha - \beta, \alpha \cdot \beta, \alpha/\beta$ (cuando $\beta \neq 0$) son construibles a partir de P. Se sigue que el conjunto K de números reales construibles a partir de P forma un subcampo K de $\mathbb{R}$. Más aún, $\mathbb{Q} \subseteq K \subseteq \mathbb{R}$.*

Ahora nos interesa saber la condición necesaria para que un número real sea construible. Sea K el campo de números construibles y K_0 un subcampo de K. Dado que se entiende por el plano de K_0 el conjunto de todos los puntos (a, b) en el plano euclidiano real cuyas coordenadas a y b están en el plano de K_0. Si (a, b) y (c, d) están en el subcampo K_0, entonces la recta que los une tiene la ecuación $\frac{(y-b)}{(x-a)} = \frac{(b-d)}{(a-c)}$, de manera que es de la forma $ux + vy + w = 0$ donde u, w, v están en K_0.

Recordemos que de geometría analítica se tienen los siguientes resultados:

Proposición 3.3.8. *Dadas dos rectas de la forma $u_1x + v_1y + w_1 = 0$ y $u_2x + v_2y + w_2 = 0$, donde $u_1, u_2, v_1, v_2, w_1, w_2$ están todos en K_0, entonces son paralelas o bien su punto de intersección es un punto del plano de K_0.*

Proposición 3.3.9. *Dada una circunferencia cuyo radio r está en K_0 y cuyo centro (a, b) está en el plano de K_0, su ecuación es $(x-a)^2 + (y-b)^2 = r^2$ la cual al desarrollarse es de la forma $x^2 + y^2 + dx + ey + f = 0$ donde d, e y f están en K_0.*

Ahora para ver dónde intersecta una recta de la forma $ux + vy + w = 0$ a una circunferencia de la forma $x^2 + y^2 + dx + ey + f = 0$ contenida en el plano de K_0, se resuelve simultáneamente las ecuaciones de la recta y la circunferencia.

Si $v \neq 0$, entonces $y = -\frac{(ux+w)}{v}$, sustituyendo y en la ecuación $x^2 + y^2 + dx + ey + f = 0$ se tiene

$$\begin{aligned}
0 &= x^2 + \left(-\frac{ux+w}{v}\right)^2 + dx + e\left(-\frac{ux+w}{v}\right) + f \\
&= x^2 + \left(-\frac{(ux+w)(ux+w)}{v^2}\right) + dx + \left(\frac{eux - ew}{v}\right) + f \\
&= x^2 + \frac{u^2x^2}{v^2} + 2\frac{uxw}{v^2} + w^2 + dx - \frac{eux}{v} - \frac{ew}{v} + f \\
&= x^2\left(1 + \frac{u^2}{v^2}\right) + x\left(\frac{2uw}{v^2} + d - \frac{eu}{v}\right) + w^2 - \frac{ew}{v} + f.
\end{aligned}$$

La cual es una ecuación cuadrática en la abscisa c de la forma $c^2+s_1c+s_2 = 0$ con s_1 y s_2 en K_0. Por la fórmula cuadrática $c = \frac{-s_1 \pm \sqrt{s_1^2 - 4s_2^2}}{2}$ y si la recta y la circunferencia se cortan en el plano real, entonces $s_1^2 - 4s_2^2 \geq 0$ y si $K_1 = K_0(\sqrt{s})$ entonces se ve que la abscisa c se encuentra en K_1. Si $\sqrt{s} \in K_0$ resulta que $K_1 = K_0$ de lo contrario $[K_1 : K_0] = 2$. Puesto que la ordenada $d = \frac{-(uc+w)}{v}$, se tiene que también $d \in K_1$. Por consiguiente, el punto de intersección (c, d) se encuentra en el plano de K_1 donde $[K_1 : K_0] = 1$ *o* 2.
Finalmente, para obtener la intersección de las circunferencias $x^2 + y^2 + dx + ey + f = 0$ y $x^2 + y^2 + gx + hy + k = 0$ en el plano de K_0 restando una de estas ecuaciones de la otra, resulta $(d-g)x + (e-h)y + (f-k) = 0$ la cual es la ecuación de la recta en el plano de K_0. Por tanto, encontrar los puntos de intersección de las dos circunferencias en el plano K_0 es lo mismo que hallar los puntos de intersección de una recta en el plano de K_0 con una circunferencia en este plano. Ésta es precisamente la situación de que se dispuso anteriormente, por tanto si las dos circunferencias se cortan en el plano real, sus puntos de intersección se encuentran en el plano de una extensión de K_0 de grado 1 o 2.

Teorema 3.3.10. *Para que un número real a sea construible es necesario que $[\mathbb{Q}(a) : \mathbb{Q}]$ sea una potencia de 2. En forma equivalente, el polinomio mínimo de a sobre $\mathbb{Q}$ debe tener grado igual a una potencia de 2.*

Demostración. Para producir una longitud construible a se empieza en el plano de $\mathbb{Q}$, la regla proporciona rectas en el plano de $\mathbb{Q}$ y el compás circunferencias en el plano de $\mathbb{Q}$. Por tanto, estas se intersectan en un punto del plano de una extensión de grado 1 o 2 de $\mathbb{Q}$. Para llegar a a, se va por este procedimiento del plano de $\mathbb{Q}$ al de L_1, digamos donde $[L_1 : \mathbb{Q}] = 1$ *o* 2, luego al de L_2, donde $[L_2 : L_1] = 1$ *o* 2 y se continua un número finito de veces. De esta forma se obtiene una sucesión finita $\mathbb{Q} = L_0 \subset L_1 \subset L_2 \subset \cdots \subset L_n$ de campos donde cada $[L_i : L_{i-1}] = 1$ *o* 2 y donde a está en L_n. Por el Teorema 3.1.13 se tiene

$$[L_n : \mathbb{Q}] = [L_n : L_{n-1}][L_{n-1} : L_{n-2}] \cdots [L_1 : \mathbb{Q}].$$

Dado que cada $[L_i : L_{i-1}] = 1$ *o* 2 se ve que $[L_n : \mathbb{Q}]$ es una potencia de 2. Puesto que $a \in L_n$, se tiene que $\mathbb{Q}(a)$ es un subcampo de L_n. Por consiguiente, por el Corolario 3.1.16, $[\mathbb{Q}(a) : \mathbb{Q}]$ debe dividir a una potencia de 2. Por lo tanto $[\mathbb{Q}(a) : \mathbb{Q}] = 2^m$ para algún entero no negativo m. En forma equivalente por el Teorema 3.1.44, el polinomio mínimo de a sobre $\mathbb{Q}$ debe tener un grado igual a una potencia de 2. Esta es una condición necesaria para que a sea construible. □

Antes de proseguir con la demostración de la imposibilidad con regla y compás para trisecar un ángulo, veremos que un ángulo recto se puede trisecar.

Sea $\angle A$ un ángulo recto. Trazamos un círculo con centro en A, con cualquier radio a, que intersecta los lados de $\angle A$ en los puntos B y C. Luego trazamos un círculo con centro en B, que contenga a A. Los dos círculos se intersectan en dos puntos, uno de los cuales será un punto D en el interior de $\angle A$. Ahora el triángulo es equilátero y, por lo tanto, equiangular. Por lo tanto $\angle BAD = 60^o$ y $\angle DAC = 90^o - 60^o = 30^o = \frac{1}{3}90^o$. Es decir, $\angle DAC$ es un tercio del ángulo $\angle BAC$.

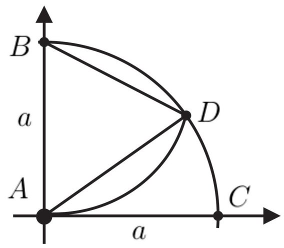

Figura 3.8: Trisección de un ángulo recto.

Teorema 3.3.11. *Es imposible trisecar un ángulo de* 60^o *usando sólo regla y compás.*

Demostración. Si se pudiera trisecar el ángulo particular de 60^o se podría construir el triángulo de la Figura 3.9.

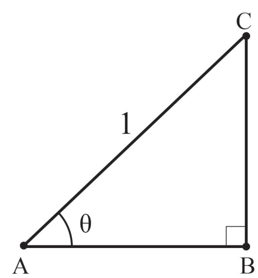

Figura 3.9: Triángulo rectángulo.

Donde $\theta = 20^o$ y $AC = 1$, usando solo regla y compás puesto que AB es de longitud $\cos 20^o$, debido a que $\cos\theta = \frac{cateto\ adyacente}{hipotenusa} = \frac{AB}{1} = AB$ por las propiedades antes mencionadas se tendría que probar que $\cos 20^o = AB$ es un número construible.

Afirmación. El $\cos 20^o$ no es un número construible.

Produciendo su polinomio mínimo sobre $\mathbb{Q}$ y demostrando que este polinomio es de grado 3. Para tal fin recordemos que

$$\begin{aligned}
\cos(3\phi) &= \cos(2\phi+\phi) = cos(2\phi)cos\phi - \sin(2\phi)\phi\sin\phi \\
&= \cos(\phi+\phi)\cos\phi - \sin(\phi+\phi)\sin\phi \\
&= (\cos^2\phi - \sin^2\phi)\cos\phi - (2\sin\phi\cos\phi)\sin\phi \\
&= \cos^3\phi - \sin^2\phi\cos\phi - 2\sin^2\phi\cos\phi \\
&= \cos^3\phi - 3(1-\cos^2\phi)\cos\phi \\
&= \cos^3\phi - 3\cos\phi + 3\cos^3\phi \\
&= 4\cos^3\phi - 3\cos\phi.
\end{aligned}$$

Sea $\cos\phi = q$, donde $\phi = 20^o$ y usamos el hecho de que $\cos(3{\cdot}20^o) = \cos 60^o = \frac{1}{2}$, así la fórmula $\cos(3\phi) = 4\cos^3\phi - 3\cos\phi$ se convierte en $4q^3 - 3q = \frac{1}{2}$ y de esta manera $2(4q^3 - 3q = \frac{1}{2})$ se convierte en $8q^3 - 6q - 1 = 0$, si $s = 2q$ esta se transforma en $4s^3 - 3s - 1 = 0$, por las propiedades de los números construibles si q es construible entonces s también lo es, pero $p(s) = 0$ donde $p(x) = 4x^3 - 3x - 1$ el cual es un polinomio irreducible sobre $\mathbb{Q}$ pues

$$\begin{aligned}
4x^3 - 3x - 1 &= x - x(4x^2 - 3) - 1 \\
&= x(2x+\sqrt{3})(2x-\sqrt{3}) - 1 \\
&= 0.
\end{aligned}$$

pero $\sqrt{3} \notin \mathbb{Q}$. Así, $p(x)$ es el polinomio mínimo de s sobre $\mathbb{Q}$, debido a que $p(x)$ es de grado 3 y 3 no es una potencia de 2, así por los teoremas 3.3.7 y 3.3.10 se tiene que s no es construible, Por lo tanto, no se puede trisecar un ángulo de 60^o usando solo regla y compás. $\square$

Observación 3.3.12. *El polinomio $p(x)$ en la demostración anterior es una combinación de polinomios de Chebyshev de tipo I Y II, es decir, $p(x) = T_3(x) + U_{-2}(x)$.*

Para finalizar este trabajo y aprovechando la teoría desarrollada en él demostraremos la imposibilidad de duplicar el volumen de un cubo y de construir un cuadrado con la misma área que un círculo dado.

Para demostrar el siguiente Teorema, necesitaremos saber el *Criterio de Eisenstein* y la definición de Divisibilidad los cuales podemos revisar en [3, p. 23, 169].

Definición 3.3.13. *Dados m, n números enteros, $m \neq 0$, se dice que m divide a n, escrito como $m \mid n$, si $n = cm$ para algún entero c.*

Teorema 3.3.14. *Sea* $f(x) = x^n + a_1x^{n-1} + \cdots + a_n$ *un polinomio con coeficientes enteros. Supóngase que existe algún primo* p *tal que* $p \mid a_1, p \mid a_2, ..., p \mid a_n$ *pero* $p^2 \nmid a_n$*, entonces* $f(x)$ *es irreducible en* $\mathbb{Q}[x]$*.*

Teorema 3.3.15. *Es imposible duplicar el cubo de volumen* 1 *usando solamente regla y compás.*

Demostración. Duplicar un cubo de lado 1, por lo tanto de volumen 1, mediante regla y compás, requeriría construir un cubo cuyos lados miden b y su volumen fuera 2. Pero el volumen de tal cubo seria b^3, así que se tendría que encontrar un número construible b tal que $b^3 = 2$. Dado un número real b tal que $b^3 = 2$, entonces su polinomio mínimo sobre $\mathbb{Q}$ es $p(x) = x^3 - 2$.
Afirmación. El polinomio $p(x) = x^3 - 2$ es irreducible en $\mathbb{Q}$.
Usando el criterio de Eisenstein, con $p = 2$ y sabiendo que $a_n = -2$, se tiene que $p \mid a_n = -2$ pero $p^2 \nmid -2$ pues $-2 = (4)\left(-\frac{1}{2}\right)$ y $-\frac{1}{2} \notin \mathbb{Z}$. Así, $p(x) = x^3 - 2$ es irreducible sobre $\mathbb{Q}$ y además $p(b) = 0$ y $p(x)$ es de grado 3, puesto que 3 no es una potencia de 2 por el Teorema 3.3.10 no existe tal b construible.
Por lo tanto, la duplicación del cubo mediante regla y compás no es posible. □

Para la demostración del siguiente Teorema, es necesario saber que Lindemann demostró en 1882 que π es un número trascendente y como lo mencionamos anteriormente en la Definición 3.1.21 también se puede entender como número trascendente a los números que no pueden ser obtenidos mediante procesos de resolver ecuaciones algebraicas.

Teorema 3.3.16. *Es imposible usando regla y compás, hallar el área de un círculo dado.*

Demostración. Podemos pensar al radio del círculo como la unidad y al círculo unitario centrado en el origen de $\mathbb{R}^2$. El área de este círculo es π y así el cuadrado cuya área es igual a la π tiene lados igual a $\sqrt{\pi}$ pero si fuera posible construir este cuadrado entonces π sería construible y $[\mathbb{Q}(\sqrt{\pi}) : \mathbb{Q}]$ sería potencia de 2 y entonces π sería algebraico sobre $\mathbb{Q}$ pero eso es una contradicción al Teorema de Lindemann. Por lo tanto, es imposible usando solo regla y compás hallar el área de un círculo dado. □

Bibliografía

[1] J. Contreras y C. Del Pino, *Acerca del problema de la trisección de un ángulo*, Instituto de Matemáticas y Física Universidad de Talca.

[2] S. H. Friedberg y A. J. Insel, *Linear Algebra*, Cuarta Edición. Prentice Hall, Nueva Jersey, (2003).

[3] I. N. Herstein, *Álgebra Abstracta*, Grupo Editorial Iberoaméricana, (1986).

[4] N. Martínez de la Escalera, *Construcciones con regla y compás*, México. D. F., UNAM, (1979).

[5] J. C. Mason y D. C. Handscomb, *Chebyshev Polynomials*, CHAPMAN & HALL\CRC, (1990).

[6] E. Moise y F. Downs, *Geometría Moderna*, Addison Wesley Iberoaméricana, (1989).

[7] L. Németh, *A new type of lemniscate*, NymE SEK Tudományos Kozlemények XX. Természettudományok **15**, (2014), 9-16.

[8] L. Németh, *Sectrix Curves on the Sphere*, KoG Scientific Professional Journal of Croatian Society for Geometry and Graphics **19**, (2015), 42-47.

[9] A. Ortiz, *Historia de la Matemática*, Pontificia Universidad Católica de Peru, (1936).

[10] T. J. Rivlin, *Chebyshev Polynomials*, New York, Wiley, (1990).

[11] I. Stewart, *Historia de las Matemáticas en los últimos 10,000 años*, Crítica Barcelona, (2007).

[12] F. Zaldívar, *Teoría de Galois*, Universidad Autónoma Metropolitana - Iztapalapa, (1996).