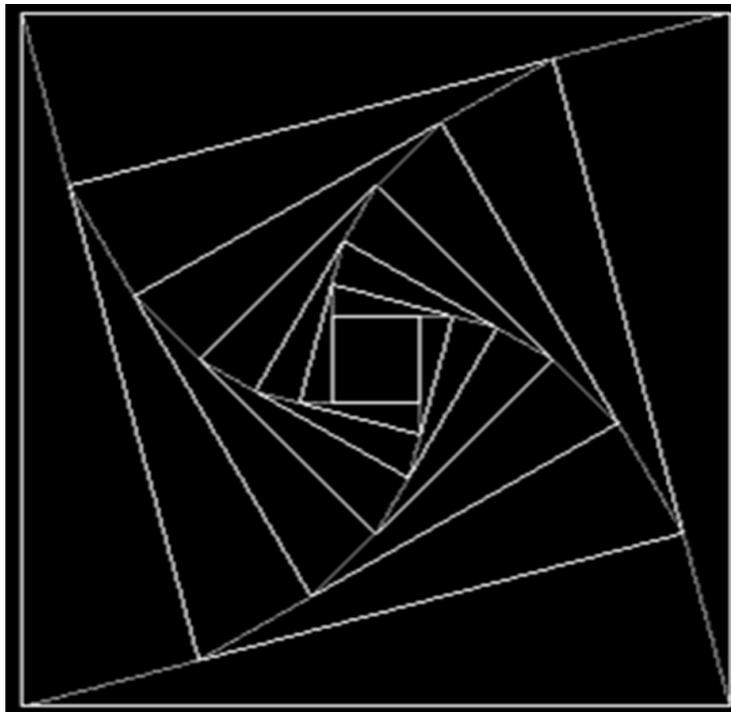


**SOCIEDAD «PUIG ADAM»  
DE PROFESORES DE MATEMÁTICAS**



**BOLETÍN N.º 111  
ABRIL DE 2021**

## ÍNDICE

	<i>Págs.</i>
Sociedad “Puig Adam” de Profesores de Matemáticas .....	2
Edición del Boletín y Comité Editorial .....	4
Cancelación de la Asamblea General Ordinaria de 2021 .....	6
Cancelación del Concurso Intercentros “Joaquín Hernández” de Matemáticas de la Comunidad de Madrid .....	6
Convocatoria del XXXVIII Concurso de Resolución de Problemas .....	7
Inventando teoremas con GeoGebra: un nuevo Teorema de la Altura, por <i>Fernando Etayo Gordejuela, Nicolás de Lucas Sanz,</i> <i>Tomás Recio y M<sup>a</sup> Pilar Vélez</i> .....	8
Sobre una familia de curvas asociadas a un cuadrado, por <i>Ricardo Moreno Castillo</i> .....	28
Una familia de polinomios de grado 8 cuyo grupo de Galois es el grupo cuaternión $Q_8$ , por <i>Arturo Rodríguez y M<sup>a</sup> Belén Rodríguez</i> .....	40
Kepler y el dodecaedro rómbico, por <i>Roberto Cardil Ricol</i> .....	59
Espirales primas como una herramienta para el análisis de conjuntos en $N$ , por <i>Darwin Méndez Contreras</i> .....	76
Reseña de libros .....	92
Instrucciones para el envío de originales .....	93
Adquisición de números atrasados de nuestro Boletín .....	95
Boletín de inscripción en la Sociedad “Puig Adam” .....	96

## **SOCIEDAD "PUIG ADAM" DE PROFESORES DE MATEMATICAS**

SEDE: Facultad de Educación. Despacho 3215  
Rector Royo Villanova, s/n 28040 – Madrid  
Correo electrónico: puigadam@mat.ucm.es

-----

### **Junta Directiva de la Sociedad "Puig Adam"**

*Presidente:* José Javier Etayo Gordejuela

*Vicepresidentes:*

Eugenio Roanes Macías

María Gaspar Alonso-Vega

Juan Jesús Donaire Moreno

*Vocales:*

Enrique Rubiales Camino (Relaciones Institucionales)

Eugenio Roanes Lozano (Gestión de publicaciones)

Ricardo Moreno Castillo (Redacción de Publicaciones)

Javier Soler Areta (Actividades y concursos)

*Secretario:* José María Sordo Juanena

*Vicesecretaria:* Carmen Escribano Ródenas

*Tesorero:* José Manuel Gamboa Mutuberría

*Bibliotecaria:* Angélica Martínez Zarzuelo

-----

### **Boletín de la Sociedad "Puig Adam"**

ISSN: 1135-0261 Depósito Legal: M-7762-1995

Gráficas Loureiro, S.L.- San Pedro, 23 bis - 28917 Leganés (Madrid).

Tel.: 91 611 59 88 loureiro@graficasloureiro.es

El Boletín se distribuye gratuitamente a nuestros socios. Las instrucciones para hacerse socio aparecen en la página 96 del mismo.

Las instrucciones para publicar en el Boletín aparecen en las páginas 93-94 del mismo. Las propuestas de publicación de artículos, reseñas, etc., deben hacerse a través del correo electrónico de la Sociedad: puigadam@mat.ucm.es

En la portada aparece la figura adoptada como logotipo de la Sociedad "Puig Adam". Se trata de la figura de portada de uno de los libros más emblemáticos de D. Pedro Puig Adam, el titulado "La Matemática y su enseñanza actual".

## **Página web de la Sociedad**

<http://www.sociedadpuigadam.es>

### Contenido:

Nuestra web contiene varias secciones: *Historia* de la Sociedad, *Boletín* de la Sociedad y *Concursos* de Problemas (el Concurso “Puig Adam” y otros concursos en que colaboran miembros de nuestra Junta Directiva).

### Sobre la publicación del Boletín en nuestra web:

Nuestro Boletín se ha publicado ininterrumpidamente desde 1983 en que se fundó nuestra Sociedad. Muchos de los números antiguos están agotados y, con frecuencia se nos pide información sobre artículos publicados en ellos. La incomodidad de copiar reiteradamente dichos artículos por escaneo y de enviarlos nos ha llevado a adoptar la solución indicada a continuación.

Teniendo en cuenta la información solicitada a la Sociedad y, particularmente a algunos de nuestros socios, por parte de profesores y entidades (españolas y también de países sudamericanos) sobre artículos aparecidos en nuestro Boletín, varios de nuestros socios han propuesto incorporar parcialmente el Boletín a nuestra web, al igual que se está haciendo en otras Sociedades Matemáticas que publican revistas.

En respuesta a esta propuesta, se ha acordado que sean colgados en nuestra web en formato pdf los contenidos íntegros de los números de nuestro Boletín con más de cinco años de antigüedad y el índice de contenidos de los números publicados en los cinco últimos años. Ya se ha concluido esa tarea, de modo que los interesados pueden encontrar todos los Boletines en nuestra web.

### Cómo acceder a los Boletines

Nuestra pág. web cuelga de la pág. de la Universidad Complutense de Madrid ([www.ucm.es](http://www.ucm.es)) y se puede entrar directamente en nuestra pág., por ejemplo, desde *Google*, tecleando *Sociedad Puig Adam*, seleccionando *Todos los Boletines* y eligiendo *Índices de los Boletines de los últimos cinco años*, o bien *Boletines completos de más de cinco años*.

### Mantenedoras de la página web:

Beatriz Barrero Díaz y Carolina Bravo Sanz, bajo la dirección del Secretario de nuestra Sociedad.

### **Comité Editorial del Boletín**

Gabriel Aguilera Venegas, Universidad de Málaga  
José Antonio Alonso, Universidad de Sevilla  
Francisco Baena Muñoz, Profesor de Instituto  
Bärbel Barzel, University of Duisburg-Essen (Alemania)  
Michel Beaudin, École de Technologie Supérieure, Montreal (Canadá)  
Josef Böhm, Profesor de Instituto (Austria)  
Joaquín Borrego, Universidad de Sevilla  
Francisco Botana, Universidad de Vigo  
Justo Cabezas, Profesor de Instituto y Univ. de Extremadura  
Agustín Carrillo de Albornoz Torres, Profesor de Instituto y Univ. de Córdoba  
Juan Carlos Cortés López, Universidad Politécnica de Valencia  
Juan Jesús Donaire Moreno, Profesor del Instituto “Ramiro de Maeztu”, Madrid  
Fernando Etayo Gordejuela, Universidad de Cantabria  
José Javier Etayo Gordejuela, Universidad Complutense de Madrid  
Sergio Falcón, Universidad de las Palmas de Gran Canaria  
Jose Luis Galán García, Universidad de Málaga  
José Manuel Gamboa, Universidad Complutense de Madrid  
José Alberto García Suárez, Profesor de Instituto y Univ. Santiago Compostela  
María Gaspar Alonso-Vega, Profesora de Instituto y Univ. Complutense Madrid  
Francisco González Redondo, Universidad Complutense de Madrid  
Gregorio Hernández Peñalver, Universidad Politécnica de Madrid  
Antonio Hernando Esteban, Universidad Politécnica de Madrid  
David J. Jeffrey, University of Western Ontario (Canadá)  
Nuria Joglar Prieto, Universidad Complutense de Madrid  
Wolfram Koepf, Universität Kassel (Alemania)  
Zoltán Kovács, The Private University College of Education, Linz (Austria)  
Ricardo Luengo González, Universidad de Extremadura  
Edgar Martínez Moro, Universidad de Valladolid  
Angélica Martínez Zarzuelo, Universidad Complutense de Madrid  
Ricardo Moreno Castillo, Profesor de Instituto y Univ. Complutense Madrid  
Aleksandr Myllari, St. George’s University (Grenada)

John Olive, The University of Georgia (USA)  
Pavel Pech, University of South Bohemia (República Checa)  
Pedro Quaresma, Universidade de Coimbra (Portugal)  
Antonio Quesada, Akron University (USA)  
Tomás Recio, Universidad de Cantabria  
Luis Rico, Universidad de Granada  
Eugenio Roanes Lozano, Universidad Complutense de Madrid  
Eugenio Roanes Macías, Universidad Complutense de Madrid  
Ana Romero, Universidad de La Rioja  
Enrique Rubiales Camino, Profesor de Instituto y Univ. Complutense Madrid  
Julio Rubio, Universidad de La Rioja  
José Luis Ruiz Reina, Universidad de Sevilla  
Eduardo Sáenz de Cabezón, Universidad de La Rioja  
Fernando Sánchez Fernández, Universidad de Extremadura  
Tomás Sánchez Giralda, Universidad de Valladolid  
Javier Soler Areta, Catedrático de Instituto  
José María Sordo Juanena, Universidad Complutense de Madrid  
Jon R. Star, Harvard Graduate School of Education (USA)  
Stanly Steinberg, University of New Mexico (USA)  
Elena Varbanova, Technical University of Sofia (Bulgaria)  
Nikolay N. Vassiliev, Russian Academy of Sciences (Rusia)  
M. Pilar Vélez, Universidad Nebrija  
Michael J. Wester, Cotopaxi and University of New Mexico (USA)

### Edición de este número 111

La coordinación de la edición ha estado a cargo de Eugenio Roanes Macías.

### Menciones de los artículos del Boletín

- 1) Recensiones de los artículos publicados en el Boletín aparecen en “MathEduc”, lo que antes era Zentralblatt für Didaktik der Mathematik (ZDM).
- 2) Los abstracts de los artículos están accesibles en el portal Dialnet.
- 3) El Boletín aparece en las bases de datos de publicaciones periódicas: Google Académico, UlrichsWeb y WorldCat.

## Cancelación de la Asamblea General Ordinaria de 2021

Las circunstancias sanitarias, de todos conocidas, obligan a cancelar la *Asamblea General Ordinaria* de nuestra Sociedad de este año 2021, que cada año se celebra en el mes de abril.

En el próximo número 112 de nuestro Boletín daremos cuenta de las decisiones tomadas, en consecuencia, por la Junta Directiva de la Sociedad.

## Cancelación del XX Concurso Intercentros

### “Joaquín Hernández”

Así mismo, las circunstancias sanitarias obligaron a cancelar el *XX Concurso Intercentros de la Comunidad de Madrid*, que debía haberse celebrado el pasado otoño.

Por ello, este número de abril de nuestro Boletín no incluye la Crónica de dicho Concurso, con la colección de enunciados de los ejercicios propuestos, así como la lista de alumnos y centros ganadores, como venía siendo habitual.

**XXXVIII Concurso de Resolución de Problemas**  
convocado por la Sociedad "Puig Adam" de Profesores de Matemáticas  
(con la colaboración del Colegio de Doctores y Licenciados)

**BASES DEL CONCURSO**

**Primera:** Los alumnos podrán participar en el Concurso en tres niveles:

- a) *Primer nivel:* alumnos de 3º de E.S.O.
- b) *Segundo nivel:* alumnos de 4º de E.S.O.
- c) *Tercer nivel:* alumnos de 1º Bachillerato

**Segunda:** Las pruebas consistirán en la resolución de Problemas de Matemáticas (los mismos para todos los concursantes de un mismo nivel) y se realizarán en la mañana del *sábado 22 de mayo de 2021* a partir de las 10 horas en la Facultad de Matemáticas de la Universidad Complutense de Madrid.

**Tercera:** A los mejores de cada nivel, se concederán diplomas y premios.

**Cuarta:** Los Centros que deseen presentar alumnos (hasta un máximo de seis) deberán realizar la preinscripción preferiblemente antes del día 11 de mayo, dirigiéndose por correo electrónico, carta o fax al presidente de nuestra Sociedad:

*Prof. Javier Etayo Gordejuela*  
*Departamento de Álgebra, Geometría y Topología*  
*Facultad de Ciencias Matemáticas*  
*28040-Madrid      Fax: 91 394 4662*  
*Correo electrónico: jetayo@mat.ucm.es*

En la preinscripción no es preciso hacer constar los nombres de los alumnos seleccionados. Si algún centro desea presentar más de seis alumnos, debe solicitarlo antes de la fecha mencionada anteriormente.

**Quinta:** Los centros entregarán a los alumnos que envíen, credenciales individuales en las que se haga constar que han sido seleccionados por su excepcional aprovechamiento en Matemáticas, así como el curso en que están matriculados en el curso académico 2020-2021.

**AVISO MUY IMPORTANTE:** A la vista de la situación sanitaria existente en el momento de cerrar este Boletín, se recomienda encarecidamente que se consulte la página web de nuestra Sociedad, por si se hace necesario modificar la fecha del Concurso o cancelarlo.

# Inventing theorems with GeoGebra: a new Altitude Theorem

# Inventando teoremas con GeoGebra: un nuevo Teorema de la Altura

**Fernando Etayo Gordejuela<sup>a</sup>**  
**Nicolás de Lucas Sanz<sup>b</sup>**

Departamento de Matemáticas, Estadística y Computación,  
Universidad de Cantabria

**Tomás Recio<sup>c</sup>**  
**M. Pilar Vélez<sup>d</sup>**

Grupo de Investigación Matemáticas y sus Aplicaciones,  
Universidad Antonio de Nebrija

<sup>a</sup>fernando.etayo@unican.es,

<sup>b</sup>nicolas.delucas@alumnos.unican.es,

<sup>c</sup>trecio@nebrija.es, <sup>d</sup>pvelez@nebrija.es

## **Abstract**

*The Altitude Theorem states that, in a right triangle, the altitude drawn from the right angle to the hypotenuse divides the hypotenuse into two segments, the length of the altitude is the geometric mean of these two segments. A generalization of this classical theorem is discovered and proved here through the interaction of automated and human reasoning. GeoGebra automated reasoning tools reveal the existence of a larger family of triangles (right and pseudo-right) that verify the thesis of the theorem. Then human reasoning leads to the characterization of pseudo-right triangles from euclidean and lorentzian geometries. Some reflections of educational nature about the development of human reasoning supported by technological tools arise naturally.*

## Introducción: Descubrimiento Automático de teoremas con GeoGebra

El Teorema de la Altura de un triángulo rectángulo, también llamado Teorema de la Media Geométrica, establece que el cuadrado de la altura  $l$ , medida desde el vértice opuesto a la hipotenusa, es igual al producto de las proyecciones  $j, k$ , de los catetos sobre la hipotenusa. Ver Figura 1. También suele considerarse en su enunciado, recíprocamente, que esta igualdad, entre la altura trazada desde un vértice al lado opuesto y el producto de las proyecciones de los lados adyacentes, implica que el triángulo es rectángulo.

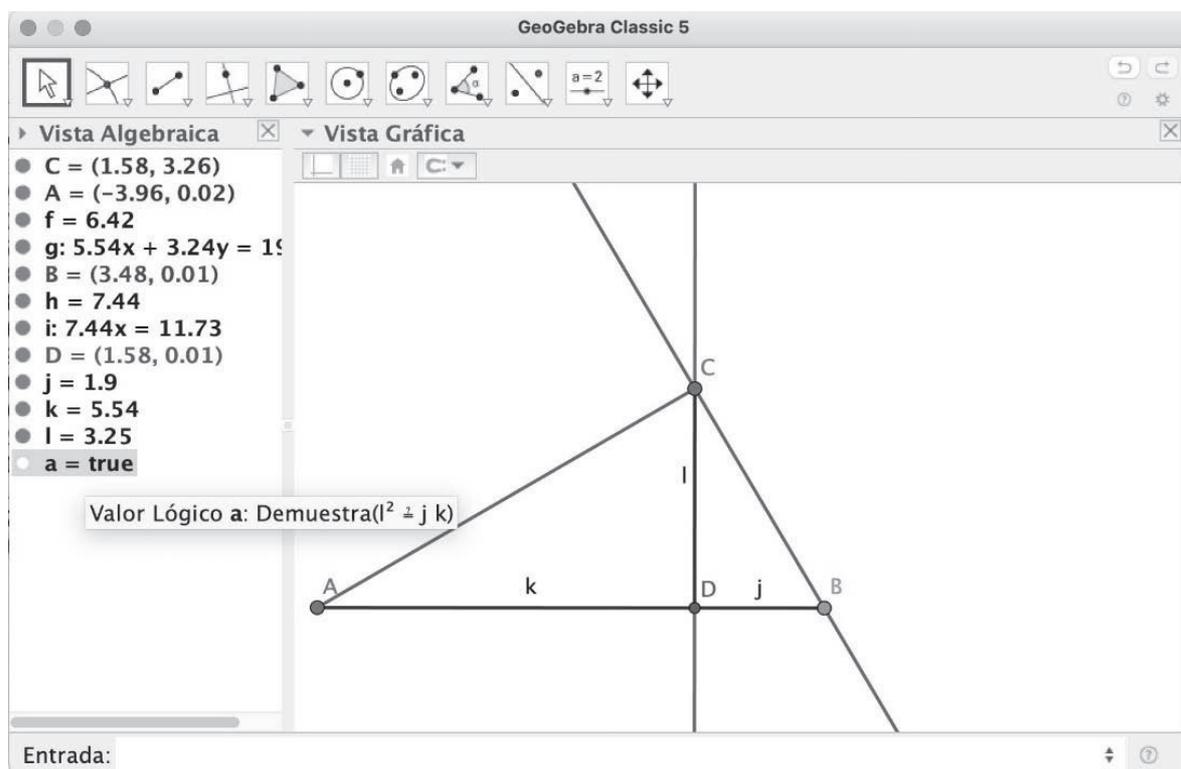


Figura 1: *El Teorema de la Altura verificado con GeoGebra.*

Es un resultado bien conocido, incluido en los Elementos de Euclides ([https://es.wikipedia.org/wiki/Teorema\\_de\\_la\\_media\\_geométrica](https://es.wikipedia.org/wiki/Teorema_de_la_media_geométrica)), que se trabaja ya en los primeros años del currículum de la ESO en relación con los teoremas de Tales y Pitágoras (ver: <https://zagan.unizar.es/record/58769?ln=es>), aunque no aparece explícitamente mencionado en el currículo oficial.

El otro ingrediente esencial de este artículo es el programa de matemática y geometría dinámica, GeoGebra (<http://www.geogebra.org>) que permite, desde hace años, la verificación automática y rigurosa de la verdad o falsedad de proposiciones de geometría. Véase, por ejemplo, la detallada descripción de las herramientas de razonamiento automático en GeoGebra que aparece en [5]. Así, en la Figura 1 se ha recogido la comprobación, a través de GeoGebra, de la validez del Teorema de la Altura.

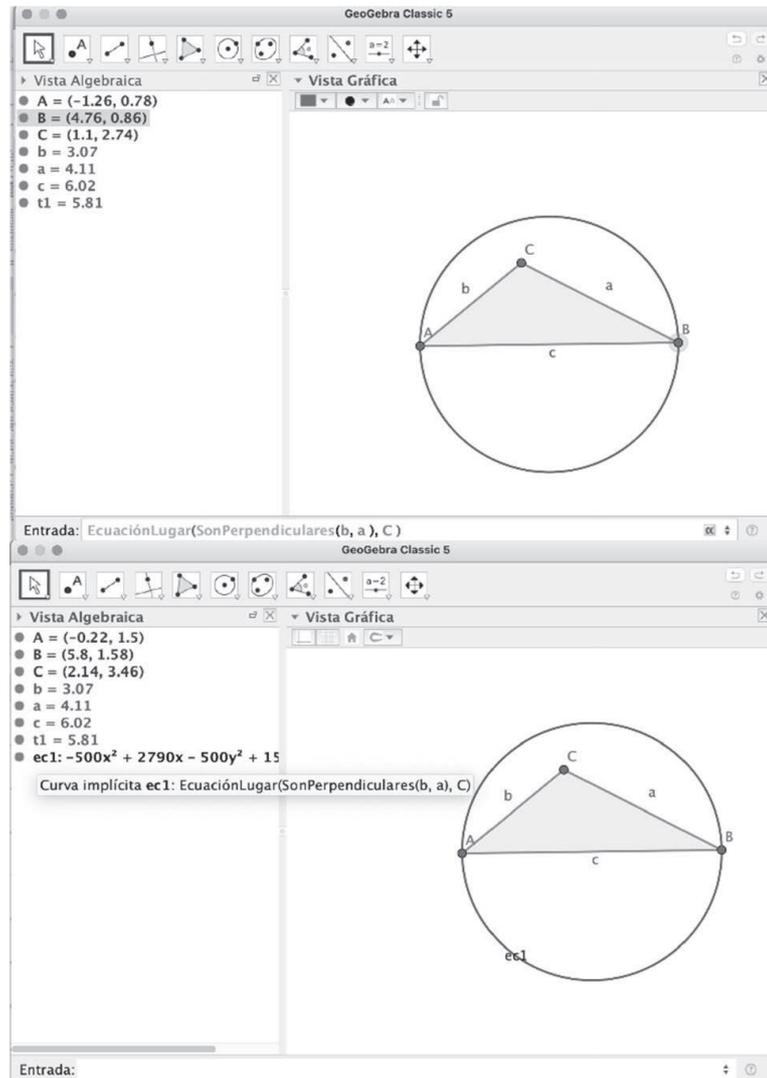


Figura 2: Arriba, en la Entrada, se plantea la búsqueda de las condiciones para que los lados  $b$  y  $a$  sean perpendiculares. Abajo, la respuesta de GeoGebra:  $C$  ha de estar en la circunferencia de ecuación  $ec1$ .

Una de las características más notables de tales herramientas es, sin duda, la posibilidad de contribuir al descubrimiento automático de nuevos teoremas, como pretendemos conseguir en este artículo en relación con el Teorema de la Altura.

El planteamiento de GeoGebra en relación con el descubrimiento automático consiste en tratar de hallar posibles hipótesis complementarias, i.e. condiciones necesarias  $H$ , que conduzcan a la verificación de cierta tesis  $T$  que establezcamos de antemano, es decir, obtener  $H$  para que  $H \Rightarrow T$ .

La Figura 2 muestra un sencillo ejemplo. Supongamos que trazamos un triángulo  $ABC$  cualquiera y que deseamos saber qué propiedad ha de verificar  $C$  para que el triángulo sea rectángulo en  $C$ . Es decir, tratamos de enunciar un teorema que afirme: si  $C$  verifica  $H$  (hipótesis buscada), entonces se tiene  $ABC$  rectángulo en  $C$  (tesis). La respuesta, como puede verse en la Figura 2, es el grafo y ecuación de una circunferencia. Se trata de una respuesta dinámica, esto es, automáticamente modificable en función de los valores de  $A$ ,  $B$  establecidos por el usuario en la figura, y que pueden cambiar si el usuario los arrastra por la Vista Gráfica.

Como limitaciones de esta herramienta señalemos que las propiedades definitorias de la curva obtenida (por ejemplo, que se trata de una circunferencia que tiene su centro en el punto medio del lado  $AB$  y que pasa por  $A$  y por  $B$ ) habrán de ser deducidas por el usuario a partir de estos datos, quien deberá, además, comprobar que estas condiciones necesarias son, además, suficientes para la validez de la tesis.

Esto no siempre ocurre. Por ejemplo, en la Figura 3, arriba, aparece una curva de grado 12 (producto de los dos ejes y de una curva de grado 10) en la que es necesario ubicar el vértice  $C$  para que los bisectores  $h$  e  $i$  de los ángulos  $\widehat{BAC}$  y  $\widehat{ABC}$ , respectivamente, sean de igual longitud (véase, [8] para más detalles). Dejando a un lado los casos degenerados, es decir, la ubicación del vértice  $C$  en el eje horizontal, aun así es fácil ver (Figura 3, abajo) que no se verifica la igualdad de longitud de los bisectores cuando situamos ese vértice en cualquier punto de la curva de grado 10; y que sólo se cumple la tesis requerida cuando se coloca  $C$  en el eje vertical.

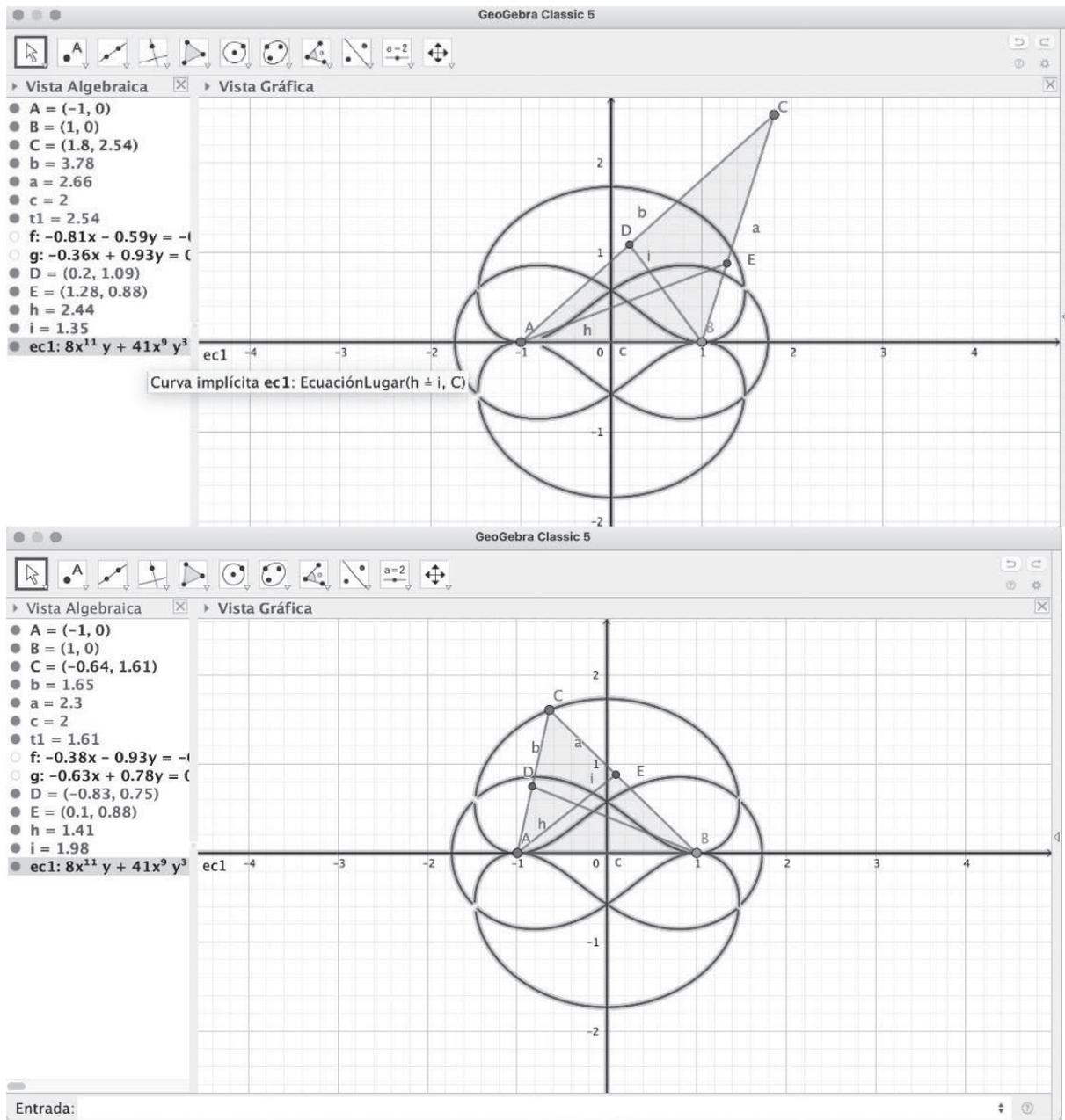


Figura 3: Arriba, obtención del lugar geométrico para que los bisectores  $h, i$  sean iguales. Abajo, verificación numérica y visual (valores en rojo de  $h, i$ ) de que no todos los puntos del lugar geométrico verifican la tesis buscada.

Por tanto, si bien el lugar geométrico encontrado en la Figura 3 contiene el conjunto de puntos donde se verifica la conclusión propuesta por el usuario, esta inclusión puede ser muy estricta, como en este ejemplo. Remitimos al lector al artículo [6] para un estudio detallado, desde la perspectiva de la geometría algebraica, de esta complicada situación.

Es necesario advertir al lector, como una última característica –tal vez inesperada– de este mecanismo automático de generación de hipótesis, de que el lugar geométrico obtenido a partir de una tesis  $T$ , arbitraria, puede ser vacío, degenerado o limitado a un número pequeño de casos, como ejemplifican las Figuras 4 y 5. Tales respuestas pueden ser muy útiles, por ejemplo, para advertir al usuario de que la tesis que plantea no se verifica nunca, como en el ejemplo de la Figura 4. O pueden complicar la interpretación de los resultados, como en la Figura 5. En efecto, reescribir una ecuación  $ec1$ , dependiente de  $A$  y  $B$ , como producto de sumas de cuadrados no es trivial; y es aún más complicado deducir, a partir de esta descomposición, la ubicación espacial de los puntos definidos por tales sumas de cuadrados, en función de la posición de  $A$  y  $B$ .

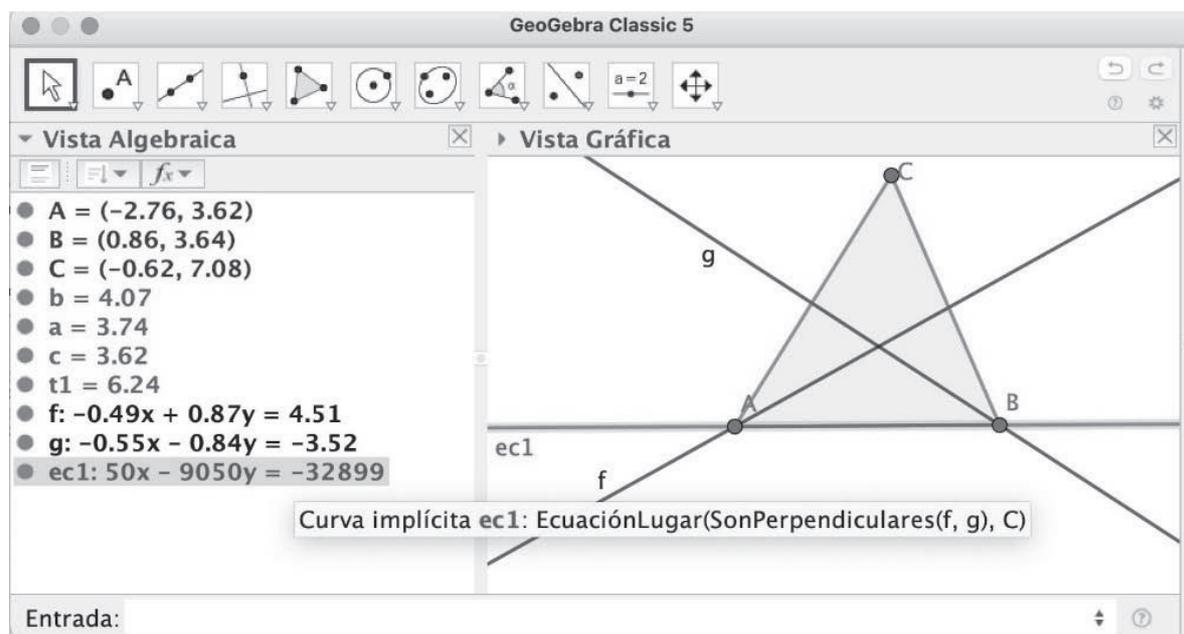


Figura 4: En línea gruesa, ubicación del vértice  $C$  para que las bisectrices  $f, g$  de los ángulos  $\overline{CAB}$  y  $\overline{ABC}$  sean perpendiculares. En todos los casos se obtienen triángulos degenerados, dado que la hipótesis obtenida es que  $A, B$  y  $C$  han de estar alineados.

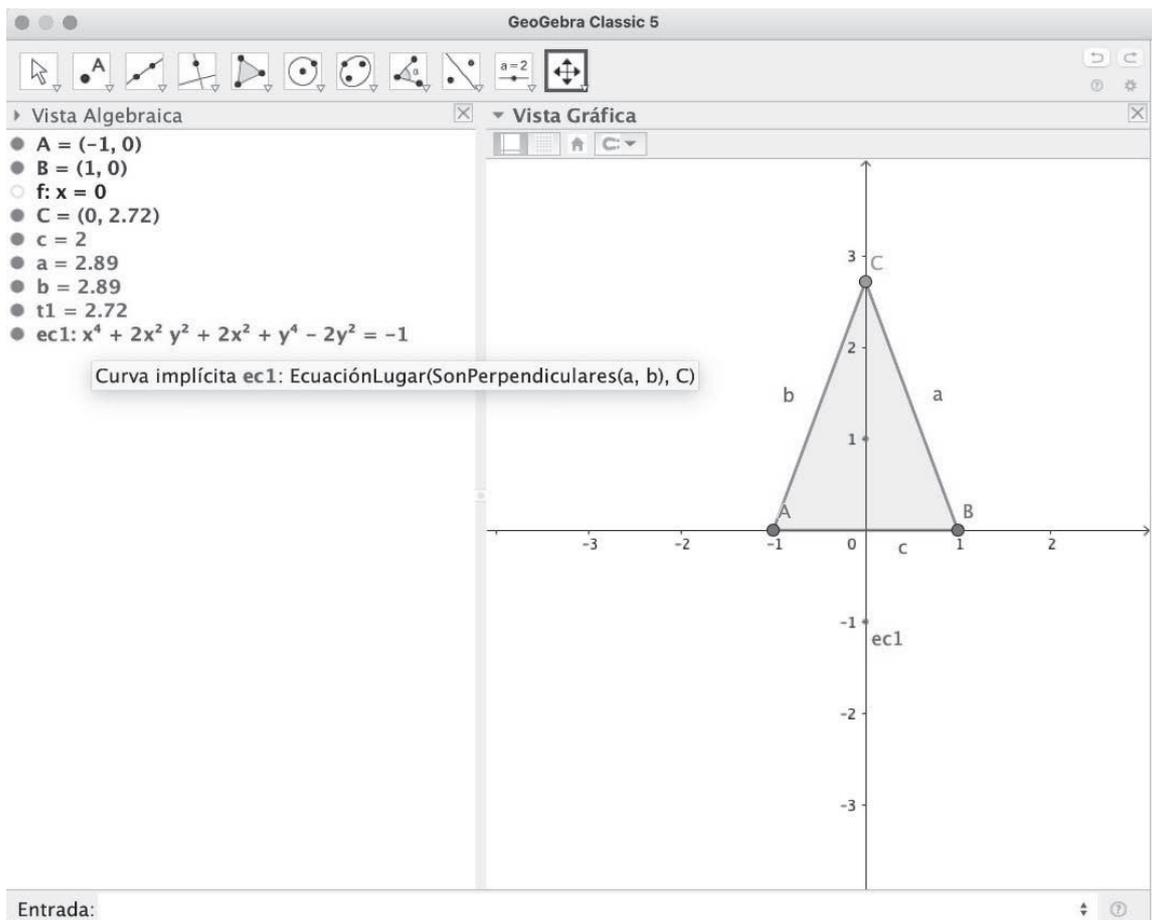


Figura 5: Dado un triángulo isósceles (el vértice  $C$  está construido sobre la mediatriz del lado  $AB$ ), buscamos una hipótesis que implique que sea rectángulo en  $C$ . La respuesta son los puntos  $(0,1)$  y  $(0,-1)$  descritos en  $ec1$  mediante el producto de sumas de cuadrados  $(x^2 + (y - 1)^2)(x^2 + (y + 1)^2)$ .

En resumen: la herramienta *EcuaciónLugar* de razonamiento automático, implementada en GeoGebra, es, en nuestra opinión, extraordinariamente atractiva y útil para la exploración e invención de nuevos resultados, pero en la mayoría de los casos su respuesta requiere altas dosis de tratamiento y reflexión por parte del usuario.

Por eso, en este contexto de descubrimiento automático de teoremas, nuestro objetivo es completar, a través de la interacción hombre-máquina, los resultados descritos en [1], relativos a la generalización del Teorema de la Altura.

En efecto, en esa nota se describe, esencialmente, la ecuación de la curva –obtenida de modo automático por GeoGebra– que ha de verificar el vértice  $C$  para que sea cierta la tesis de dicho teorema. Pero no se traduce esa condición en términos geométricos, sin coordenadas, como es tradicional en geometría elemental.

Para lograr este objetivo en la Sección 1 siguiente desarrollaremos en detalle los resultados ya obtenidos en dicho artículo, haciendo hincapié, sobre todo, en las distintas carencias que supone el mero conocimiento de la ecuación del lugar en ese caso particular. Y, en la Sección 2 trataremos de paliar –con razonamiento humano– dichas carencias, alcanzando finalmente un enunciado sintético de un nuevo Teorema de la Altura. En la breve sección tres daremos otra interpretación del resultado obtenido y concluiremos el artículo con unas reflexiones de carácter educativo que surgen, de manera natural, cuando se desarrolla el razonamiento humano apoyado con herramientas tecnológicas.

## 1. Generalizando el Teorema de la Altura: la aportación de la máquina

Existen diversas generalizaciones de este Teorema de la Altura (véase [4] y las referencias que allí se incluyen), aunque todas las que recopila este autor se refieren, más bien, a diversas extensiones de la tesis.

Por el contrario, en [1] se describe, *grosso modo*, un enunciado del Teorema de la Altura en el que se relajan las hipótesis, conservando la tesis habitual. Es decir, se pretende ampliar el tipo de triángulos  $ABC$  que verifican que el cuadrado de la altura medida sobre un vértice  $C$  respecto de la recta  $AB$  es igual al producto de las proyecciones de los lados  $AC$  y  $BC$  sobre dicha recta.

Realmente esa breve nota era sólo una introducción y resumen de una presentación de software que los autores de la nota realizaron en el *International Symposium on Symbolic and Algebraic Computation (ISSAC) 2016*, y por la que recibieron el *Distinguished Software Demonstration Award*. En particular, en dicho trabajo se mostraba cómo una de las herramientas de razonamiento automático que los autores estaban implementando en el programa de matemática y geometría dinámica, GeoGebra, era capaz de obtener el lugar geométrico del vértice  $C$  de modo que se verifique que  $g^2 = hi$ , donde  $g$  es la altura de  $C$  sobre el lado opuesto y  $h$  e  $i$  son las proyecciones de los lados adyacentes sobre la recta  $AB$ , véase Figura 6.

Dicho lugar geométrico, tal como lo presenta GeoGebra, se describe mediante la ecuación implícita (ítem  $d$  en la Vista Algebraica que aparece en la Figura 6) de la curva de grado 4, con coeficientes de 10 dígitos, correspondiente a los valores numéricos concretos de  $A$  y  $B$  que se visualicen en la pantalla (por ejemplo,  $A = (-2.96, 0.38)$  en este caso), así como su representación gráfica.

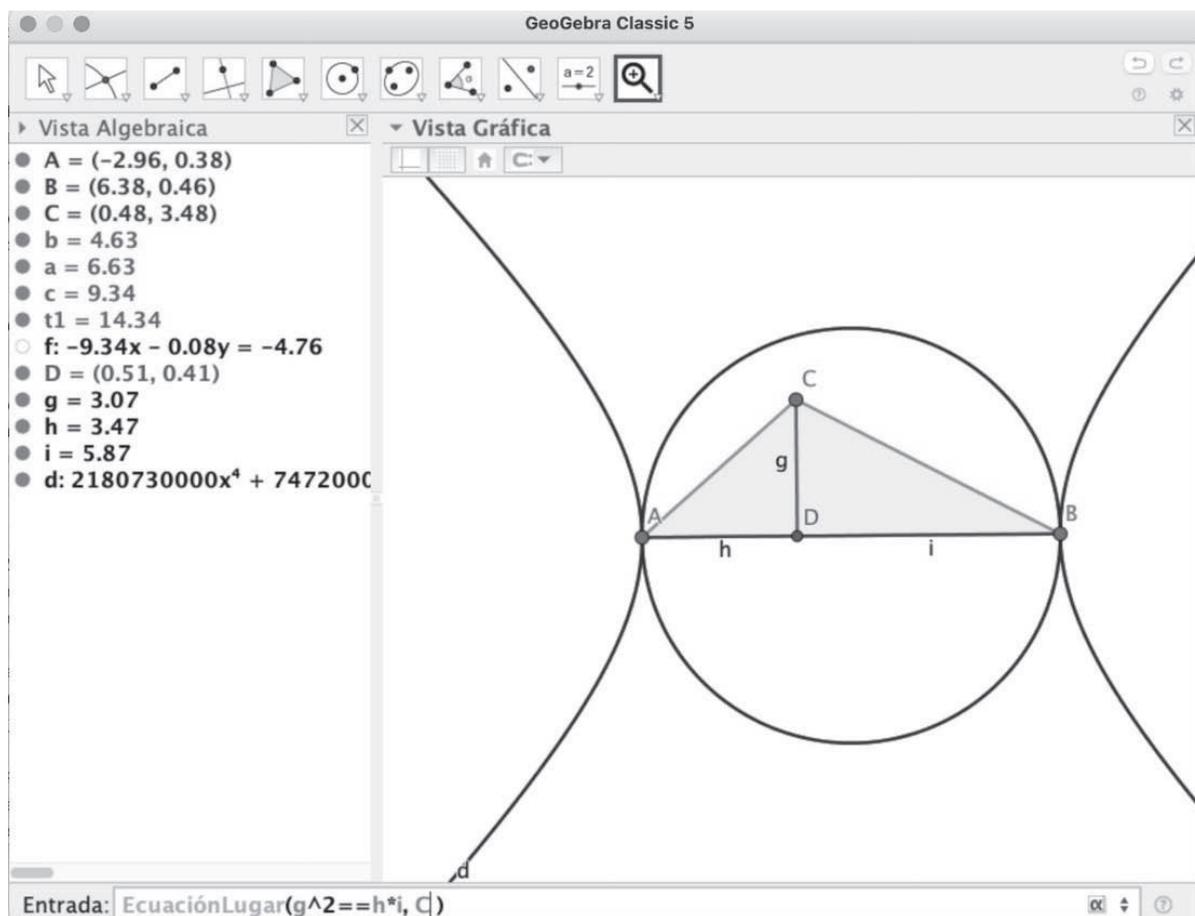


Figura 6: Lugar geométrico del vértice  $C$ , tal que  $g^2 = hi$

Es decir, el resultado obtenido tras el cálculo del lugar geométrico por GeoGebra no puede considerarse directamente como el enunciado de una generalización del Teorema de la Altura, sino, simplemente, una sugerencia. Y esto por varias razones, que hemos pergeñado en la Introducción y que resumimos, teniendo en cuenta el contexto particular de este teorema, aquí:

- i. Porque, por definición, el lugar geométrico sólo proporciona condiciones necesarias (pero tal vez no suficientes) para que se verifique la tesis del Teorema de la Altura. Para verificar la generalización de dicho teorema tendríamos que probar que, ubicando  $C$  en cualquier punto de esa curva, se cumple la tesis.
- ii. Porque como se señala en [5], en relación con otra situación diferente, en la que el lugar geométrico obtenido era un círculo  $c$ : “...in GeoGebra this implicit curve is a numerical object, it does not have a symbolic representation as the result of a construction in terms of the free given points  $A, B, C$ . GeoGebra does not know that  $c$  is a circle...”. Por tanto, del cálculo del lugar geométrico no se puede deducir, automáticamente, la relación geométrica entre la curva obtenida y el triángulo dado, en términos generales, simbólicos (por ejemplo: es un círculo que tiene el lado  $AB$  como diámetro y una hipérbola que tiene  $A, B$  como vértices y sus focos están en la recta  $AB$ , a distancia  $d(A, B) \frac{\sqrt{2}-1}{2}$  de  $A$  y  $B$ , respectivamente).
- iii. Y, en consecuencia, no podemos describir, como sería necesario para formular el nuevo teorema, qué propiedades caracterizan a los triángulos cuyo vértice  $C$  se ubique en ese lugar geométrico (digamos: si un triángulo es rectángulo o tiene una propiedad concreta, entonces, y sólo entonces, se tiene  $g^2 = hi$ ). Se trata de un paso más, porque, aunque supiéramos relacionar la curva lugar geométrico y el triángulo de manera general (como hemos enunciado en el punto anterior de manera hipotética), no parece razonable enunciar un teorema que diga: dado un triángulo  $ABC$ , entonces se tiene  $g^2 = hi$  si  $C$  está en un círculo que tiene el lado  $AB$  como diámetro y una hipérbola que tiene  $A, B$  como vértices y sus focos están en la recta  $AB$ , a distancia  $d(A, B) \frac{\sqrt{2}-1}{2}$  de  $A$  y  $B$ , respectivamente. Por ejemplo, con tal descripción no sabríamos si, tal vez, todos los triángulos cumplen tal condición, módulo traslación, rotación, simetría, homotecia... . O cómo comprobar si un triángulo dado verifica tales condiciones...

Sin embargo, se trata de una *sugerencia* que tiene una utilidad inmediata: la de ilustrar que no se verifica el recíproco del Teorema de la Altura. Es fácil, arrastrando  $C$  sobre la hipérbola, comprobar que no todo triángulo que verifica la tesis ha de ser rectángulo, contradiciendo, en cierto modo la afirmación de Josefsson [4] y otras similares, que señalan que la tesis del teorema es condición necesaria y suficiente para que el triángulo sea rectángulo. Tal vez estos autores se refieren,

implícitamente, sólo al caso en el que la proyección de  $C$  caiga dentro del lado  $AB$ , una restricción que nosotros no imponemos en nuestra construcción.

## 2. Generalizando el Teorema de la Altura: el factor humano.

Como se ha indicado anteriormente, la Figura 6 muestra, en la ventana gráfica, el lugar geométrico como una curva cuya ecuación tiene grado 4 y coeficientes de bastantes dígitos. Es, por tanto, una tarea complicada la de tratar de extraer información de dicha ecuación, buscando algunas propiedades de la curva que representa. Sin embargo, es fácil observar, como se hizo ya en [1], que si se supiera resolver el caso particular  $A(-1,0), B(1,0)$ , se podría generalizar a cualquier otra posición de estos vértices, mediante movimiento y homotecia, manteniendo la igualdad  $g^2 = hi$  puesto que es una fórmula homogénea (y por tanto invariante si cada cantidad se multiplica por una constante de homotecia) involucrando longitudes (y, por tanto, invariantes por movimiento).

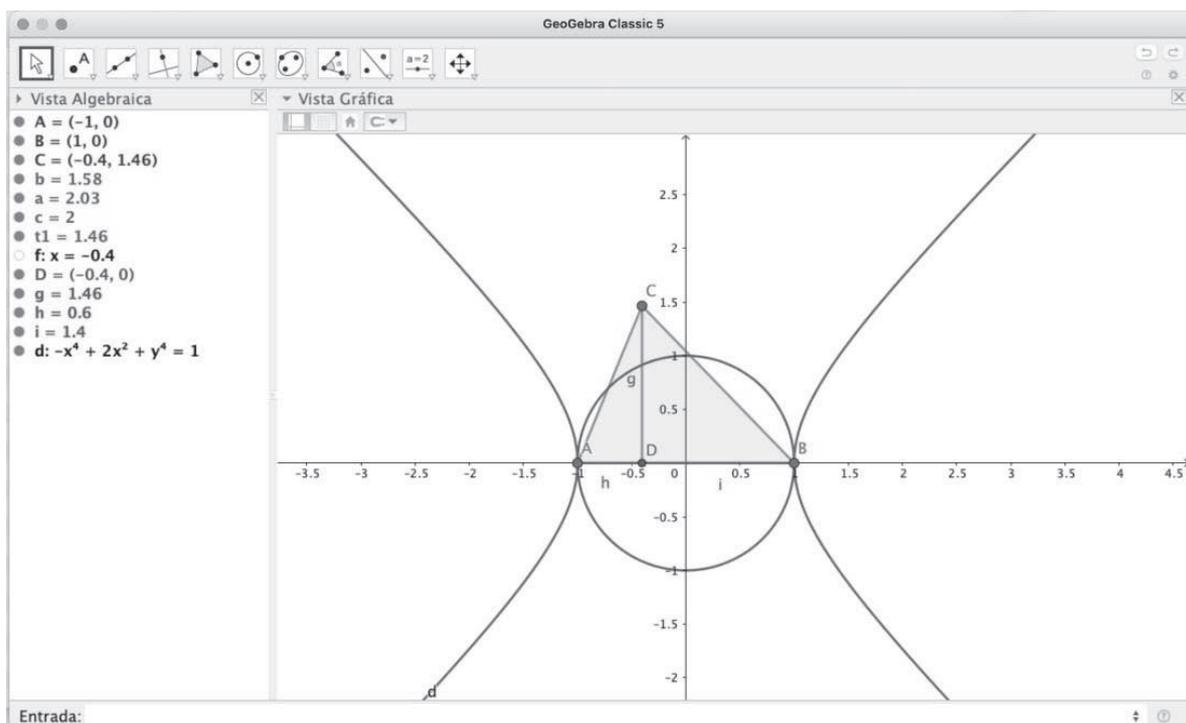


Figura 7: El mismo lugar geométrico, para el caso  $A(-1,0), B(1,0)$ . La curva  $d$  es la unión de la circunferencia  $x^2 + y^2 = 1$  y la hipérbola  $x^2 - y^2 = 1$ .

Así, en la Figura 7 se ha realizado la misma construcción, pero para estos valores específicos de los vértices  $A, B$ . El resultado es un lugar geométrico más sencillo de interpretar: la cuártica  $d := -x^4 + 2x^2 + y^4 - 1 = 0$  dada por una ecuación que es el producto

$$(x^2 + y^2 - 1)(x^2 - y^2 - 1) = -(-x^4 + 2x^2 + y^4 - 1) = 0$$

El primer factor es el caso clásico: la circunferencia de centro en el origen (el punto medio del lado  $AB$ ) y que pasa por  $A$  y por  $B$ . La ubicación de  $C$  en dicha circunferencia es, precisamente, la condición necesaria y suficiente para que  $ABC$  sea rectángulo.

La otra ecuación es, claramente, la de la hipérbola equilátera  $x^2 - y^2 = 1$ . Es bastante fácil comprobar que todos los puntos  $P(x, y)$  de esta hipérbola verifican la tesis del Teorema de la Altura. En efecto, tomando uno de estos puntos como vértice, tenemos

$$g = y, \quad h = -x - 1, \quad i = -x + 1$$

o, según la rama en la que se encuentre  $P$ ,

$$h = x + 1, \quad i = x - 1$$

luego

$$\begin{aligned} x^2 = y^2, \quad hi &= (-x - 1)(-x + 1) = x^2 - 1, \text{ o} \\ hi &= (x + 1)(x - 1) = x^2 - 1 \end{aligned}$$

En ambos casos, dado que  $x^2 - y^2 = 1$ , se tiene  $g^2 = hi$ , es decir, es condición suficiente la pertenencia a la hipérbola para la tesis.

El que sea, además, condición necesaria, es simplemente consecuencia del algoritmo de *EcuaciónLugar*, que obtiene la ecuación de esta curva por eliminación entre las ecuaciones que describen la construcción y la tesis propuesta. O bien, en este caso, se concluye considerando que si  $g^2 = hi$ , entonces, como

$$g = y, \quad h = -x - 1, \quad i = -x + 1$$

o, según la rama de la hipérbola,

$$h = x + 1, \quad i = x - 1,$$

se tiene que

$$y^2 = hi = (-x - 1)(-x + 1) = x^2 - 1, \text{ o}$$

$$y^2 = hi = (x + 1)(x - 1) = x^2 - 1,$$

es decir,

$$x^2 - y^2 = 1$$

También es fácil ver que esta hipérbola tiene el origen como centro,  $A$  y  $B$  como vértices, y sus focos están ubicados en  $(-\sqrt{2}, 0)$ ,  $(\sqrt{2}, 0)$ , puesto que, en la expresión canónica de la hipérbola  $\frac{x^2}{a^2} - \frac{y^2}{b^2} = 1$ , se tiene  $c^2 = a^2 + b^2$ , donde el valor de  $c$  corresponde a la ubicación de los focos en las coordenadas  $(c, 0)$ ,  $(-c, 0)$ , luego, en este caso  $a = 1$ ,  $b = 1$ ,  $c = \sqrt{2}$ . Por tanto, en el caso general, empleando la correspondiente homotecia, los vértices se ubicarán a distancia  $\frac{d}{2}$  del centro de la hipérbola y los focos se ubicarán a distancia  $d \frac{\sqrt{2}-1}{2}$  de los vértices, sobre la recta que estos determinen.

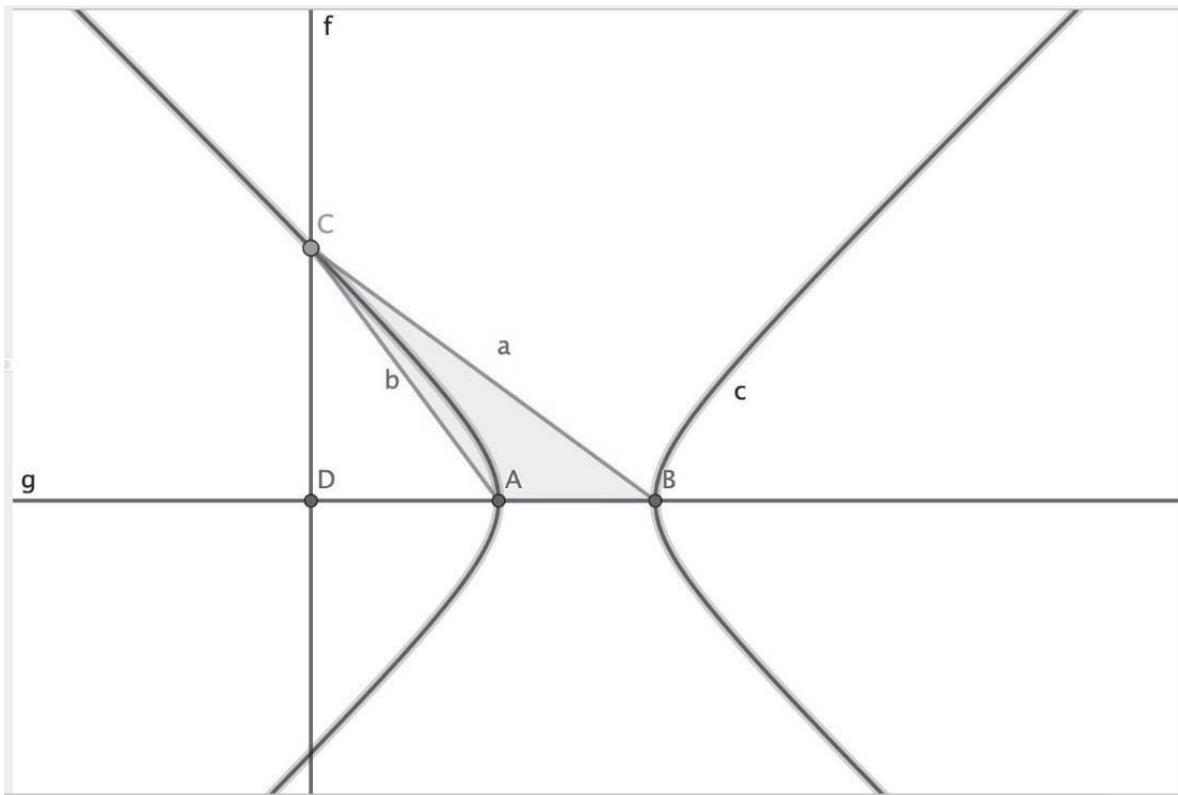


Figura 8: Un triángulo ABC verificando el Teorema de la Altura

Pero ¿cómo podemos caracterizar los triángulos  $ABC$  que verifiquen el Teorema de la Altura? Dejando a un lado el caso bien conocido de los triángulos rectángulos, buscamos propiedades definitorias de los triángulos que sean semejantes a triángulos  $ABC$ , con  $A(-1,0)$ ,  $B(1,0)$  y cuyo tercer vértice  $C$  esté en la hipérbola  $x^2 - y^2 = 1$ . La respuesta tiene pequeñas variantes de formulación según la rama de la hipérbola que se considere; en lo que sigue supongamos que consideramos la rama de la izquierda, es decir, triángulos  $ABC$  que tienen en  $A$  un ángulo obtuso, véase Figura 8. En este contexto afirmamos que:

*El vértice  $C$  de un triángulo  $ABC$ , obtusángulo en  $A$ , verifica la tesis del Teorema de la Altura si y solo si  $\alpha - \beta = 90^\circ$ , donde  $\alpha$  y  $\beta$  representan las medidas de los ángulos en los vértices  $A$ ,  $B$ , respectivamente.*

En efecto, supongamos que  $\alpha - \beta = 90^\circ$ . Entonces, como  $\widehat{DCA} + \widehat{CAD} = 90^\circ$  (puesto que  $\widehat{ADC} = 90^\circ$  por construcción), tenemos que

$$\widehat{DCA} = 90^\circ - \widehat{CAD}.$$

Por otra parte,  $\widehat{CAD} + \alpha = 180^\circ$ . Luego

$$\widehat{DCA} = 90^\circ - \widehat{CAD} = 90^\circ - 180^\circ + \alpha = \alpha - 90^\circ = \beta.$$

Así, la condición  $\alpha - \beta = 90^\circ$  implica que  $\widehat{DCA} = \widehat{CBA}$ . Por tanto, los triángulos  $DAC$  y  $DCB$  son semejantes, puesto que tienen dos ángulos iguales (dado que ambos son rectángulos en  $D$ ) y, así, tienen los tres ángulos iguales. En consecuencia, se corresponden en la semejanza los segmentos  $DA$  (del triángulo  $DAC$ ) y  $DC$  (de  $DCB$ ), como opuestos a ángulos iguales, así como los segmentos  $DC$  (de  $DAC$ ) y  $DB$  (de  $DCB$ ), por la misma razón. Se sigue que  $\frac{|DA|}{|DC|} = \frac{|DC|}{|DB|}$ , que es la tesis del Teorema de la Altura.

Recíprocamente, supongamos que el triángulo  $ABC$  verifica la tesis del Teorema de la Altura, esto es,  $\frac{|DA|}{|DC|} = \frac{|DC|}{|DB|}$ . Esto implica que los triángulos  $DAC$  y  $DCB$  son semejantes, puesto que tienen dos lados proporcionales y el ángulo  $D$  común; en particular se tiene  $\widehat{DCA} = \widehat{CBA}$  (que hemos denominado  $\beta$ ). Como, por construcción,  $\widehat{DCA} = 90^\circ - \widehat{CAD}$ , tenemos  $\beta = \widehat{CBA} = 90^\circ - \widehat{CAD}$ . Además, también por construcción,  $\widehat{CAD} + \alpha = 180^\circ$ , luego

$$\beta = 90^\circ - \widehat{CAD} = 90^\circ - 180^\circ + \alpha = \alpha - 90^\circ,$$

o lo que es lo mismo,  $\alpha - \beta = 90^\circ$ .

Concluimos así que los triángulos que verifican el Teorema de la Altura son, exactamente, una suerte de triángulos que podríamos denominar *pseudo-rectángulos*. Si un triángulo rectángulo es aquel que tiene dos ángulos que suman 90 grados, los pseudo-rectángulos serían aquellos que tienen dos ángulos cuya diferencia es 90 grados.

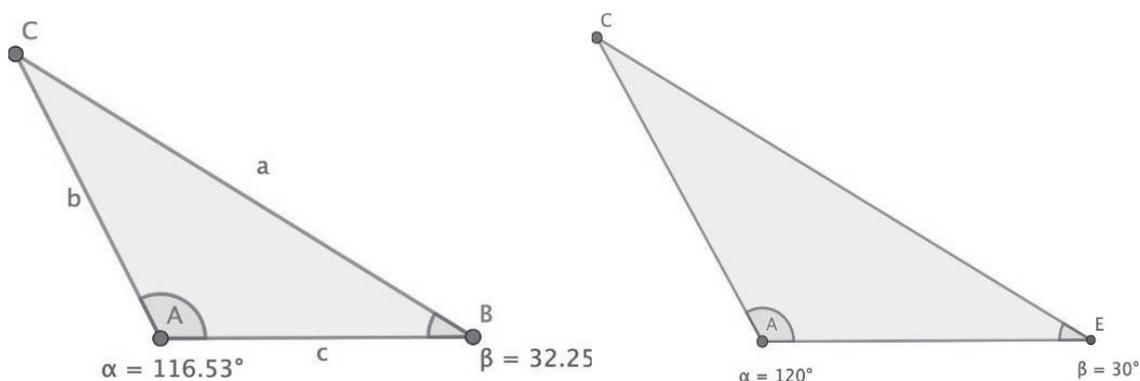


Figura 9: *A la izquierda, un triángulo no pseudo-rectángulo. A la derecha, un triángulo pseudo-rectángulo.*

Nótese que en los triángulos pseudo-rectángulos se tiene que, necesariamente,  $\alpha < 135^\circ$  y  $\beta < 45^\circ$ , porque superados esos límites ya no se cierra el triángulo  $ABC$ , dado que la inclinación de la recta  $CB$  superaría la asíntota de la hipérbola.

Por último, en esta Sección nos planteamos el hallar una forma elemental de construir tales triángulos, a partir de dos vértices dados,  $A, B$ . La Figura 10 desarrolla una posible construcción, comenzando con los dos vértices arbitrarios  $A, B$ , se traza la recta  $h$  que estos determinan. Ahora se toma otro punto arbitrario  $G$  y la recta  $i = AG$ , que va a determinar el triángulo pseudo-rectángulo que queremos construir. Esto es, veremos, a través de esta construcción, que existe un conjunto 1-dimensional de pseudo-rectángulos con  $A, B$  fijos, tantos como posibles rectas  $i$  pasando por  $A$ .

Sea  $h$  la recta determinada por  $AB$  y sea  $H$  un punto de dicha recta (irrelevante desde el punto de vista de la construcción, pero que hemos usado para definir posteriormente, y medir, el ángulo  $CAH$ ). Ahora tomamos una recta  $j$  perpendicular a  $i$  y pasando por  $B$ . Sea  $I = j \cap i$ . Finalmente, sea  $j'$  la recta simétrica de  $j$  respecto del eje  $h = AB$ , y sea  $C = j' \cap i$ . Afirmamos que  $ABC$  es un triángulo pseudo-rectángulo.

En efecto,  $\widehat{BAC} = 180^\circ - \widehat{CAH} = 180^\circ - \widehat{IAB}$ . Dado que  $j, i$  son perpendiculares,  $\widehat{ABI} = 90^\circ - \widehat{IAB}$ . Pero, por simetría,

$$\widehat{CBA} = \widehat{ABI} = 90^\circ - \widehat{IAB} = 90^\circ - \widehat{CAH} = 90^\circ - 180^\circ + \widehat{BAC} = \widehat{BAC} - 90^\circ$$

En definitiva:  $\widehat{BAC} - \widehat{CBA} = 90^\circ$ , y el triángulo  $ABC$  es pseudo-rectángulo, como queríamos demostrar.

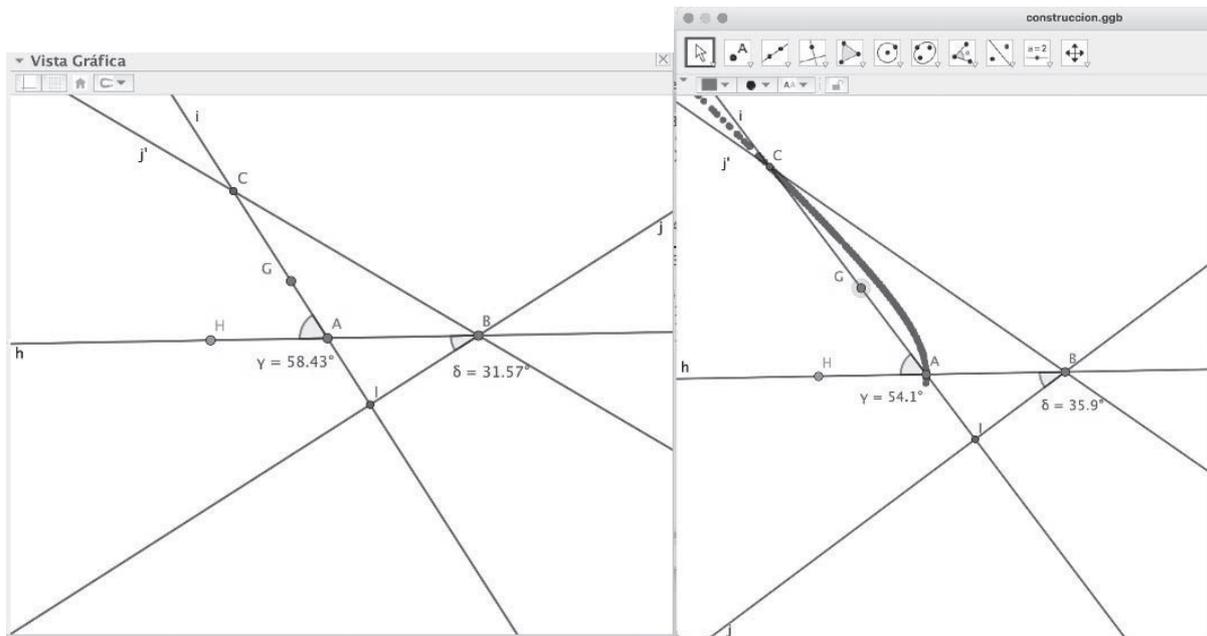


Figura 10: *Construcción de un triángulo pseudo-rectángulo.*  
*A la izquierda, elementos iniciales de la construcción.*  
*A la derecha, verificación visual de la corrección de la construcción, a través de la traza de  $C$  cuando se mueve  $G$ .*

Una última observación: nótese que dado un triángulo pseudo-rectángulo cualquiera  $ABC$ , con  $\widehat{BAC} - \widehat{CBA} = 90^\circ$ , se verifica que el simétrico de  $BC$  respecto de la recta  $AB$  es perpendicular a la recta  $CA$ , por lo que la construcción dada cubre todos los posibles triángulos pseudo-rectángulos.

### 3. Aproximación lorentziana

La hipérbola equilátera tiene un papel tan especial respecto del resto de las hipérbolas como la circunferencia respecto de las elipses. Los resultados previos son una muestra de ello. Pero, de hecho, existe un parecido mucho mayor entre las propiedades de circunferencias e hipérbolas equiláteras.

La circunferencia (centrada en el origen  $O$  y de radio  $r$ ) es el lugar geométrico de los puntos  $P$  del plano tales que la norma del vector  $OP$  sea  $r$ . La norma es la raíz cuadrada del producto escalar del vector  $OP$  por sí mismo, y el producto escalar de dos vectores es  $(a, b) \cdot (c, d) = ac + bd$ .

Consideremos ahora el producto lorentziano  $(a, b) * (c, d) = ac - bd$ . Es una aplicación bilineal y simétrica, pero no definida positiva. Dos vectores tienen producto escalar lorentziano nulo si y sólo si son simétricos respecto de alguna de las diagonales, pues  $(a, b) * (b, a) = 0$ . Se puede definir el cuadrado de la norma de un vector  $(a, b)$  como

$$\|(a, b)\|^2 = (a, b) * (a, b) = a^2 - b^2.$$

Obviamente, los vectores de las diagonales verifican  $v * v = 0$ . Los de los cuadrantes superior e inferior a las diagonales tienen  $v * v < 0$  y los que quedan a derecha e izquierda tienen  $v * v > 0$ . Así los vectores se clasifican en vectores luz, temporales y espaciales, atendiendo a las definiciones empleadas en teoría de relatividad (véase [7]). Con este producto lorentziano resulta que el conjunto de puntos  $(x, y)$  del plano tales que el cuadrado de su norma lorentziana es 1 es precisamente la hipérbola

$$\{(x, y) \in \mathbb{R}^2: x^2 - y^2 = 1\}.$$

En el caso de la circunferencia de radio 1, si  $A = (-1, 0)$ ,  $B = (1, 0)$  y  $C$  es otro punto de la circunferencia,  $\widehat{ACB} = 90^\circ$ , esto es, los vectores  $AC$  y  $BC$  son perpendiculares. La misma propiedad se tiene para los puntos de la hipérbola con el producto lorentziano. En efecto, si  $C = (x, y)$  es un punto de la hipérbola, entonces  $x^2 - y^2 = 1$  y los vectores  $\overrightarrow{AC} = (x + 1, y)$ ,  $\overrightarrow{BC} = (x - 1, y)$  tienen producto lorentziano

$$\overrightarrow{AC} * \overrightarrow{BC} = (x + 1)(x - 1) - y^2 = x^2 - 1 - y^2 = 0.$$

Los que hemos denominado triángulos pseudo-rectángulos son aquellos en que dos de los lados son perpendiculares en sentido lorentziano. En efecto, imaginemos un triángulo como el de la Figura 8, con  $A = (-1, 0)$ ,  $B = (1, 0)$  y  $C = (x, y)$  un punto del plano, y llamemos  $\alpha$ ,  $\beta$  y  $\gamma$  a los ángulos en  $A$ ,  $B$  y  $C$ , respectivamente. Si  $C$  está en la hipérbola, los vectores  $\overrightarrow{AC}$  y  $\overrightarrow{BC}$  tienen producto lorentziano nulo, con lo que son simétricos respecto de la diagonal, así que

$$\alpha = 135^\circ - \frac{\gamma}{2}$$

y el suplementario de  $\beta$  es  $135^\circ + \frac{\gamma}{2}$ , con lo que

$$\beta = 45^\circ - \frac{\gamma}{2}.$$

Por lo tanto,  $\alpha - \beta = 90^\circ$ , como antes obtuvimos. El proceso es reversible, lo que caracteriza los triángulos pseudo-rectángulos como los triángulos rectángulos lorentzianos.

#### 4. Discusión y conclusiones

El desarrollo en torno al Teorema de la Altura mostrado en estas líneas es un claro ejemplo de cómo el uso de herramientas digitales no tiene por qué sustituir al razonamiento humano a la hora de hacer matemáticas. Muy al contrario, la existencia, el avance y la disponibilidad de herramientas digitales que contribuyan al desarrollo de las actividades matemáticas puede conducir a razonamientos más profundos e, incluso, a resultados sorprendentes; por tanto, debemos considerar el uso del razonamiento automático en GeoGebra como un fenómeno cualitativamente diferente.

Es más, podríamos decir que este ejemplo del Teorema de la Altura es “extremo” porque, por un lado, estamos usando un programa, una “máquina” muy avanzada en lo que se refiere al razonamiento geométrico, pero que, a pesar de ello, ella sola no es capaz de dar una respuesta eficiente al problema planteado, sin la contribución humana. Y por otro, porque el teorema cuya generalización estamos abordando es, también “extremo” en el sentido de ser sencillo y bien conocido, estar incluido habitualmente en el currículo de la educación secundaria obligatoria, y tener una antigüedad que se remonta al menos a los Elementos de Euclides. Sin embargo, entendemos que esta generalización es novedosa.

En concreto, partiendo de una construcción en GeoGebra y usando el comando *EcuaciónLugar* descubrimos que la tesis del clásico Teorema de la Altura la verifican una familia más amplia de triángulos que, por supuesto, incluye a los triángulos rectángulos y también a los que denominamos pseudo-rectángulos. Sin embargo, la máquina aporta una respuesta, una ecuación implícita del lugar de puntos donde debe estar el vértice  $C$  del triángulo para que se verifique la tesis, que no es capaz de interpretar en términos de la construcción geométrica inicial, los otros dos vértices  $A$  y  $B$ .

La máquina nos ha descubierto la existencia estos triángulos pseudo-rectángulos y nosotros buscamos una caracterización de estos nuevos triángulos que verifican el Teorema de la Altura combinando de nuevo nuestro conocimiento y razonamiento con las herramientas (GeoGebra) que nos brinda la máquina.

Se trata por tanto de una forma de aproximarse a la geometría que combinaría la experimentación empírica y el razonamiento formal mediante la interacción hombre-máquina, en línea con la propuesta *computer-mediated thinking* [2] de Corless. Como indica Corless en [2]: “*Any tool should always be used to expand the user’s capabilities, and not as a crutch to prop up weak skills*”.

El uso a nivel educativo de estas utilidades GeoGebra se encuentra todavía en una fase incipiente y experimental. No obstante, hay que tener en cuenta, por una parte, que estas herramientas están ahora fácilmente disponibles para los más de 100 millones de usuarios de GeoGebra en todo el mundo. Y, por otra parte, la revolución educativa que supondría el proponer actividades que lleven al estudiante a hacer mejor o más rápido las matemáticas, de una manera más creativa, explorando, descubriendo y conjeturando, fomentando la curiosidad y el espíritu crítico, además de potenciar una forma de razonamiento centrada en las competencias para la era digital.

Como señalan Hohenwarter, Kovács y Recio en [3], al igual que ocurre y ocurrió con las calculadoras de bolsillo, es probable que la gente empiece a utilizar estas herramientas de razonamiento automático para comprobar hechos geométricos sin el consenso de la comunidad pedagógica sobre su función. Creemos, pues, que es urgente reflexionar sobre su potencial papel en el aula y compartir experiencias. Tal ha sido el propósito de esta nuestra modesta aportación.

## 5. Agradecimientos

El tercer y cuarto autor están parcialmente financiados por FEDER/Ministerio de Ciencia, Innovación y Universidades - Agencia Estatal de Investigación / MTM2017-88796-P (Computación simbólica: nuevos retos en Álgebra y Geometría, y sus aplicaciones).

## Referencias

- [1] M. Abánades, F. Botana, Z. Kovács, T. Recio, C. Sólyom-Gecse (2016), Development of automatic reasoning tools in GeoGebra. *ACM Communications in Computer Algebra* 50, 85-88. doi:10.1145/3015306.3015309.
- [2] R. Corless (2004), Computer-Mediated Thinking. *Proceedings of Technology in Mathematics Education Workshop 2004*, Montreal, Canada. doi:10.1.1.414.706
- [3] M. Hohenwarte, Z. Kovács, T. Recio (2019). Using GeoGebra Automated Reasoning Tools to explore geometric statements and conjectures. In Hanna, G., de Villiers, M., Reid, D. (Eds.), *Proof Technology in Mathematics Research and Teaching*, Series: Mathematics Education in the Digital Era, Vol. 14, 2019, 215-236. Springer Cham.
- [4] M. Josefsson (2016), 100.30 Generalisations of the altitude theorem. *The Mathematical Gazette*, 100 (549), 501-505. doi:10.1017/mag.2016.117.
- [5] Z. Kovács, T. Recio, M.P. Vélez (2018), Using Automated Reasoning Tools in GeoGebra in the Teaching and Learning of Proving in Geometry. *International Journal of Technology in Mathematics Education*. Vol. 25, no. 2. pp. 33-50.
- [6] Z. Kovács, T. Recio, M.P. Vélez (2019), Detecting truth, just on parts. *Revista Matemática Complutense*, Volume 32, Issue 2, May 2019. pp. 451-474 doi: 10.1007/s13163-018-0286-1.
- [7] B. O'Neill (1983), *Semi-Riemannian Geometry with applications to Relativity*. Academic Press.
- [8] T. Recio, R. Losada, J.L. Valcarce (2009), Sobre el descubrimiento automático de diversas generalizaciones del Teorema de Steiner-Lehmus. *Boletín de la Soc. Puig Adam*, no. 82, pp. 53-76.
- [9] T. Recio, S. Van Vaerenbergh, M.P. Vélez (2020), Herramientas de Razonamiento Automático en GeoGebra: qué son y para qué sirven. *Unión, Revista Iberoamericana de Educación Matemática*. Año XVI - Número 59. Agosto 2020, páginas 08-15. <https://union.fespm.es/index.php/UNION/article/view/202>.

# About a family of curves associated with a square

## Sobre una familia de curvas asociadas a un cuadrado

**Ricardo Moreno Castillo**  
Catedrático de instituto jubilado  
moreno\_castillo@hotmail.es

### **Abstract**

*The family of curves that pass through the vertices of a square and the midpoints of its sides is studied in this article.*

### **Planteamiento del problema**

Es cosa sabida que por ocho puntos (entre los cuales no haya cuatro alineados) pasan muchas curvas de tercer grado. Se trata de estudiar esta familia de curvas cuando los puntos son los vértices y los puntos medios de los lados un cuadrado. Para facilitar las cuentas, el cuadrado será concéntrico con el sistema de coordenadas, con lados paralelos a los ejes y de longitud dos.

### **1. La ecuación de la familia de cúbicas**

Las ocho puntos son  $A = (1,1)$ ,  $B = (-1,1)$ ,  $C = (-1,-1)$  y  $D = (1,-1)$  (vértices del cuadrado) y  $L = (1,0)$ ,  $M = (0,1)$ ,  $N = (-1,0)$  y  $P = (0,-1)$  (puntos medios de los lados).

Consideramos una cúbica genérica:

$$f(x, y) = ax^3 + bx^2y + cxy^2 + dy^3 + ex^2 + gxy + hy^2 + ix + jy + k = 0$$

Si la hacemos pasar por  $L, M, N$  y  $P$ , tenemos las siguientes ecuaciones:

$$\begin{aligned} a + e + i + k &= 0 & d + h + j + k &= 0 \\ -a + e - i + k &= 0 & -d + h - j + k &= 0 \end{aligned}$$

De ellas se deduce que  $i = -a$ ,  $j = -d$  y  $k = -e = -h$ . Entonces la ecuación de la curva queda, de momento, de este modo:

$$ax^3 + bx^2y + cxy^2 + dy^3 - kx^2 + gxy - ky^2 - ax - dy + k = 0$$

A continuación obligamos a la curva a pasar por  $A, B, C$  y  $D$ :

$$\begin{aligned} b + c + g - k &= 0 & b - c - g - k &= 0 \\ -b - c + g - k &= 0 & -b + c - g - k &= 0 \end{aligned}$$

De aquí tenemos que  $b = c = g = k = 0$ . Como  $a \neq 0$  y  $d \neq 0$  (de lo contrario la curva sería reducible), podemos hacer  $m = d/a$ , y la ecuación de la familia de cúbicas queda de la forma  $x^3 + my^3 - x - my = 0$ . En la Figuras 1 y 2 tenemos las curvas para los valores  $m = 3$  y  $m = 1/2$ .

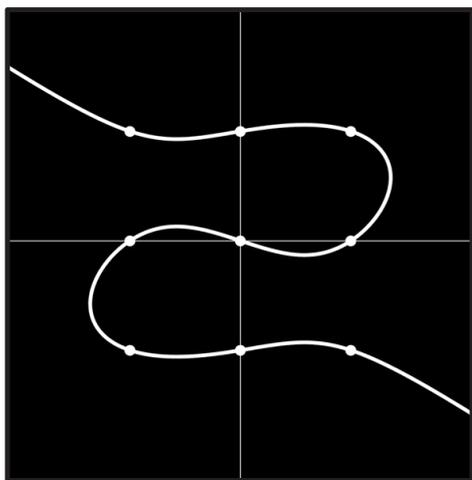


Figura 1

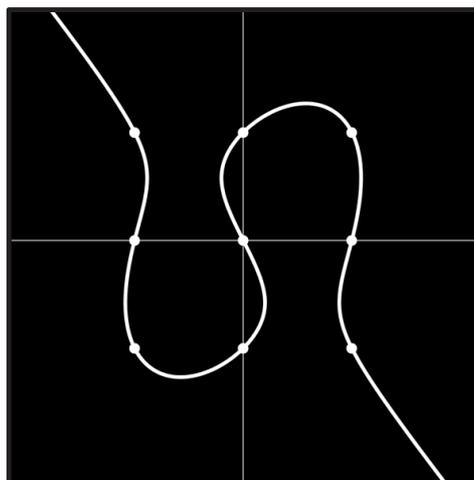


Figura 2

Que  $k = 0$  significa que todas las curvas de la familia pasan también por su centro del cuadrado. Ahora bien, en 1834 demostró Plücker que siempre que tenemos ocho puntos (entre los que no haya cuatro colineales) existe otro tal que cualquier cúbica que pase por los ocho primeros pasa también por ese punto.

Entonces, si los puntos son los vértices de un cuadrado y los puntos medios de sus lados, el noveno punto postulado por Plücker es el centro del cuadrado.

## 2. Bajo qué condiciones la curva es reducible

Si la curva es reducible, se puede escribir como el producto de una cónica (que podría ser degenerada) y una recta:

$$x^3 + my^3 - x - my = (x^2 + lxy + ny^2 + px + qy + r)(x + sy + t)$$

Hechas las cuentas pertinentes e igualados los coeficientes de los monomios de idéntico grado, tenemos las siguientes igualdades:

$$\begin{aligned} l+s=0 & \quad n+ls=0 & \quad ns=m & \quad p+t=0 & \quad lt+q+sp=0 \\ nt+qs=0 & \quad r+pt=-1 & \quad rs+qt=-m & \quad rt=0 \end{aligned}$$

De la última se deduce que  $t=0$  o  $r=0$  (la igualdad séptima demuestra que ambas cosas no pueden darse simultáneamente). Supongamos lo primero. Entonces, yendo hacia atrás en las igualdades, tenemos que  $rs = -m$ ,  $r = -1$  (y en consecuencia  $s = m$ ),  $q = 0$ ,  $p = 0$ ,  $n = 1$ ,  $ls = -1$ , y entonces  $m = 1$  o  $m = -1$ . En cada uno de estos casos tenemos las descomposiciones siguientes:

$$\begin{aligned} x^3 + y^3 - x - y &= (x^2 - xy + y^2 - 1)(x + y) \\ x^3 - y^3 - x + y &= (x^2 + xy + y^2 - 1)(x - y) \end{aligned}$$

Suponemos ahora  $r=0$ . Un razonamiento muy parecido al que se acaba de hacer nos lleva a que  $qt = -m$ ,  $pt = -1$ . Entonces, (por ser  $p+t=0$ ) sucede que  $p=1$  y  $t=-1$ , o  $p=-1$  y  $t=1$ . En el primer caso, tenemos que  $q=m$ ,  $l-s=m$ ,  $l=m/2$ ,  $s=-m/2$  y  $n=-m^2/2$ . Como  $ls=-n$ , sucede que  $m^2/4 = m^2/2$ ,  $m=0$  y la cúbica se descompone en tres rectas:  $x^3 - x = (x-1)(x+1)x$ . Si seguimos la segunda posibilidad, llegamos a la misma conclusión. Entonces, salvo para los valores  $m=1$ ,  $m=-1$  o  $m=0$ , las curvas son irreducibles.

## 3. Las asíntotas de las curvas

Sea la ecuación de la curva en coordenadas homogéneas:

$$F(x, y, z) = x^3 + my^3 - xz^2 - myz^2 = 0$$

Hacemos  $z=0$  y tenemos que  $x^3 + my^3 = 0$ , de manera que los puntos donde la curva encuentra a la recta del infinito son  $(-\sqrt[3]{m}, 1, 0)$ ,  $(-\alpha\sqrt[3]{m}, 1, 0)$  y  $(-\beta\sqrt[3]{m}, 1, 0)$  (donde  $\alpha$  y  $\beta$  son las raíces cúbicas complejas de  $-1$ ). Entonces la única asíntota real es la recta de ecuación  $x + y\sqrt[3]{m} = 0$ .

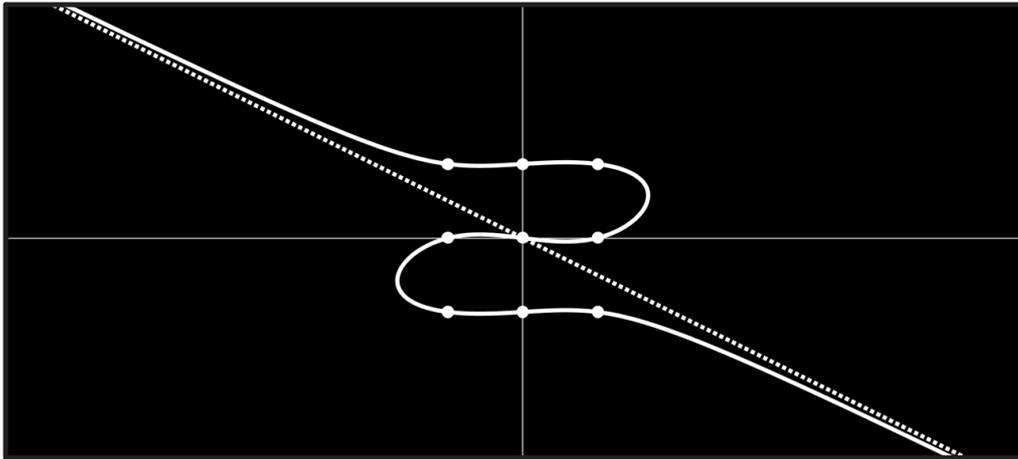


Figura 3

En la Figura 3 se puede ver la curva de ecuación  $x^3 + 8y^3 - x - 8y = 0$  y su asíntota, la recta  $x + 2y = 0$ .

#### 4. Los diámetros de la curva

En su *Enumeratio linearum tertii ordinis* (publicado en 1704) demostró Newton que si una curva de grado tres es cortada por un haz de rectas paralelas, los centros de gravedad de los puntos de corte de cada una de ellas con la curva están sobre una misma recta (si bien es cierto que el resultado es válido para curvas algebraicas de cualquier grado). Tales rectas se llaman *diámetros* de la curva, y si los diámetros concurren en un punto, diremos que la curva tiene *centro*.

Para encontrar los de nuestra curva resolvemos el sistema formado por las ecuaciones  $x^3 + my^3 - x - my = 0$  e  $y = px + q$  (que es una recta cualquiera). Esto nos lleva a lo siguiente:

$$x^3(1+mp^3) + 3mp^2qx^2 + (3mpq^2 - mp - 1)x + mq^3 - mq$$

Si  $x_1$ ,  $x_2$  y  $x_3$  son sus soluciones, la abscisa y la ordenada del centro de gravedad de los puntos de corte (según la primera fórmula de Viète) son:

$$x = \frac{x_1 + x_2 + x_3}{3} = -\frac{mp^2q}{1+mp^3}$$

Y la ordenada, en consecuencia es:

$$y = -\frac{mp^3q}{1+mp^3} + q = \frac{q}{1+mp^3}$$

Entonces  $x + mp^2y = 0$ . Como la  $q$  ha sido eliminada, esta es la ecuación del diámetro correspondiente al haz de rectas  $y = px + q$  (con  $p$  fija y  $q$  variable).

En la Figura 4 aparece la cúbica de ecuación  $x^3 + 4y^3 - x - 4y = 0$  y el haz formado por las rectas  $y = (1/3)x + q$ . El diámetro correspondiente es la recta de ecuación  $9x + 4y = 0$ .

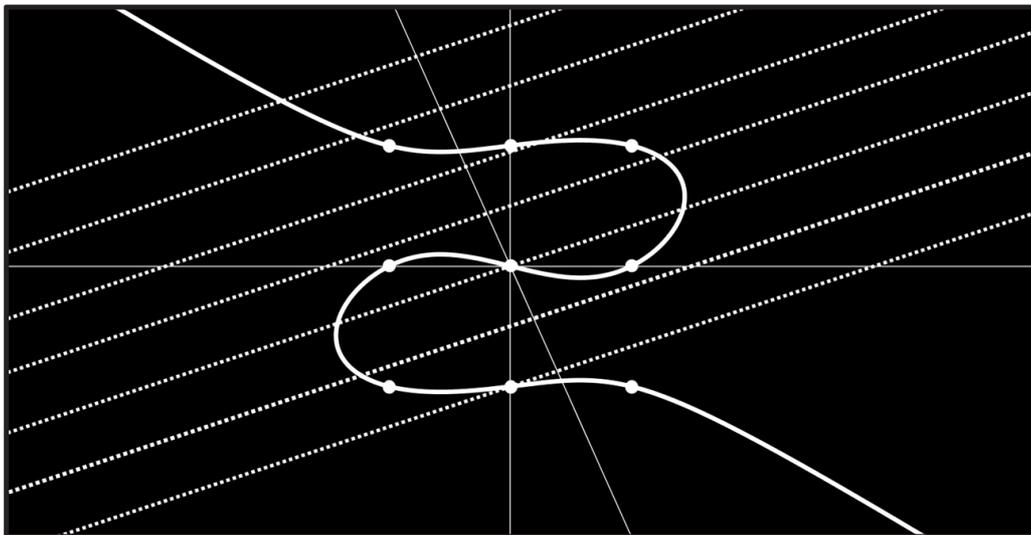


Figura 4

## 5. Puntos singulares

Para encontrar los puntos singulares de la curva fabricamos el siguiente sistema:

$$F(x, y, z) = x^3 + my^3 - xz^2 - myz^2 = 0$$

$$F_x = 3x^2 - z^2 = 0$$

$$F_y = 3my^2 - mz^2 = 0$$

$$F_z = -2xz - 2myz = 0$$

Si  $z=0$ , entonces  $x=y=0$ , luego no hay singularidades en el infinito. Si  $z=1$ , tendríamos que  $x = \pm\sqrt{3}/3$  e  $y = \pm\sqrt{3}/3$ , valores que dan lugar a cuatro puntos, ninguno de los cuales está en la curva (salvo que  $m=1$  o  $m=-1$ , pero estamos suponiendo la curva irreducible). Entonces es una cúbica no singular (lo que se llama una curva *elíptica*), lo cual significa que es de género uno, clase seis y posee nueve inflexiones, todas ellas ordinarias.

## 6. Puntos de inflexión

Los puntos de inflexión son aquellos donde la cúbica corta a su curva hessiana:

$$H(x, y, z) = \begin{vmatrix} 3x & 0 & -z \\ 0 & 3y & -z \\ z & mz & x+my \end{vmatrix} = 0$$

Si  $z=0$  llegamos a la expresión  $xy(x+my)=0$ , lo cual proporciona tres puntos del espacio proyectivo:  $(0, 1, 0)$ ,  $(1, 0, 0)$  y  $(-m, 1, 0)$ . Ninguno está sobre la curva, entonces ninguno de los puntos del infinito es una inflexión.

Hacemos entonces  $z=1$  y la curva hessiana resulta ser la siguiente:

$$3x^2y + 3mxy^2 + mx + y = 0$$

Entonces el punto  $(0, 0)$  ya es una inflexión. Si ahora tanto en la curva como en la hessiana hacemos  $y = \lambda x$  (y suponemos  $x \neq 0$ ), llegamos a las expresiones:

$$x^2 = \frac{m\lambda + 1}{m\lambda^3 + 1} \quad x^2 = -\frac{\lambda + m}{3m\lambda^2 + 3\lambda}$$

Igualando ambas, obtenemos una ecuación en  $\lambda$  de grado cuatro:

$$m\lambda^4 + 4m^2\lambda^3 + 6m\lambda^2 + 4\lambda + m = 0$$

Cada solución de la ecuación proporciona dos puntos de inflexión, pero habremos de conformarnos, casi siempre, con soluciones aproximadas. Pensemos por ejemplo la curva correspondiente a  $m=3$ . La ecuación en este caso es  $3\lambda^4 + 36\lambda^3 + 18\lambda^2 + 4\lambda + 3 = 0$ . Posee dos soluciones reales cuyos valores aproximados son  $\lambda \cong -11.49$  y  $\lambda \cong -0.58$ . La primera proporciona los puntos  $(0.08, -0.98)$  y  $(-0.08, +0.98)$ , la segunda  $(i1.35, -i0.78)$  y  $(-i1.35, i0.78)$ . Las otras cuatro inflexiones son también complejas, pero más difíciles de encontrar.

En la Figura 5 aparece la curva (en trazo continuo), su hessiana (en trazo discontinuo) y los dos únicos puntos de inflexión reales

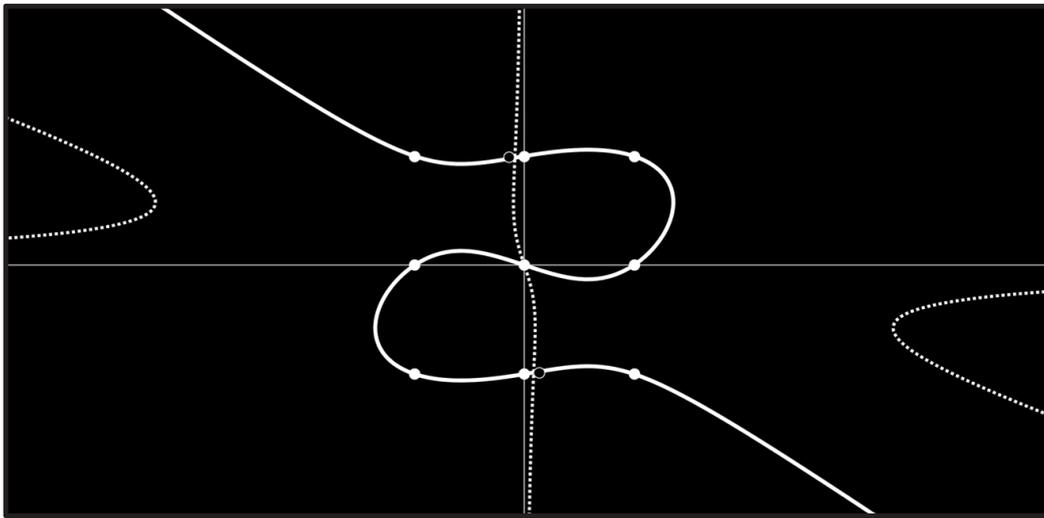


Figura 5

## 7. Círculo tangente a la curva

Si una circunferencia centrada en el origen es tangente a la curva, su pendiente en el punto de tangencia ha de ser  $-x/y$ . Entonces:

$$y' = -\frac{3x^2 - 1}{3my^2 - m} = -\frac{x}{y}$$

Si igual que antes hacemos  $y = \lambda x$  en la ecuación de la curva y en esta última expresión, llegamos a lo que viene a continuación:

$$x^2 = \frac{m\lambda + 1}{m\lambda^3 + 1} \quad x^2 = \frac{m - \lambda}{3m\lambda^2 - 3\lambda}$$

Esto da lugar a la ecuación siguiente (la cual, lo mismo que la anterior, ha de abordarse por aproximación):

$$m\lambda^4 + 2m^2\lambda^3 - 2\lambda - m = 0$$

Si  $m = 3$ , la ecuación es  $3\lambda^4 - 18\lambda^3 - 2\lambda + 3 = 0$ , que tiene dos soluciones reales que aproximadamente son  $\lambda \cong 0.6$  y  $\lambda \cong -5.99$ . Para la primera tenemos que  $x^2 \cong 1.7$ , y en consecuencia  $y^2 \cong 1.7 \times (0.6)^2 \cong 2.31$ . Entonces una circunferencia tangente es la de ecuación  $x^2 + y^2 = 2.31$ , y los puntos de tangencia son  $(1.3, 0.78)$   $(-1.3, -0.78)$ .

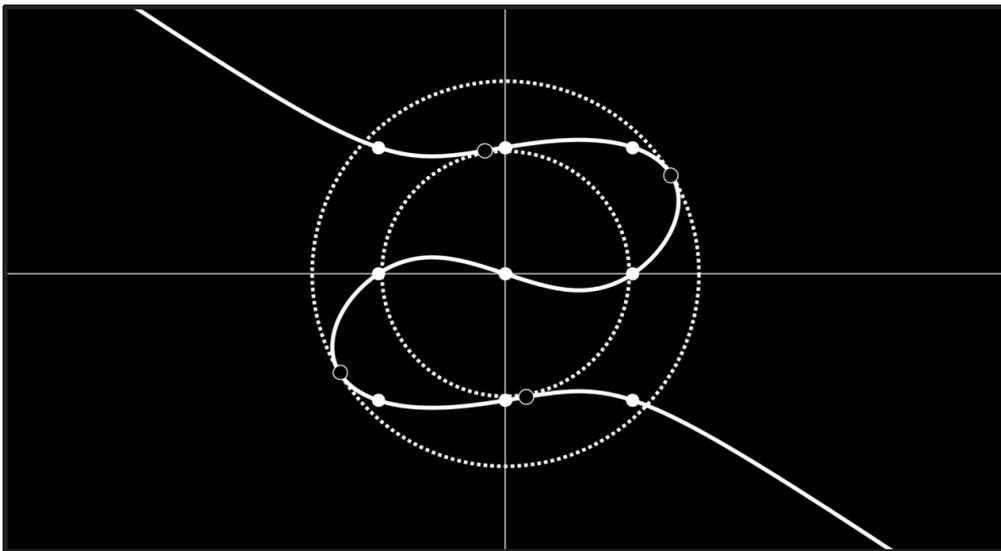


Figura 6

Para la segunda sucede que  $x^2 \cong 0.026$ , y en consecuencia  $y^2 \cong 0.026 \times (5.99)^2 \cong 0.93$ . Entonces otra circunferencia tangente es la de ecuación  $x^2 + y^2 = 0.95$  (muy próxima a la circunferencia unidad), y los puntos de tangencia

son  $(-0.16, 0.97)$ .  $(0.16, -0.97)$ . Las otras dos circunferencias tangentes son imaginarias. Todo esto se puede ver muy bien en la Figura 6.

## 8. La clase de la curva

Ya sabemos que la clase de nuestra cúbica es seis: la de cualquier curva de grado  $n$  sin singularidades es  $n(n-1)$ . Con todo, vamos a comprobar que desde cualquier punto se pueden trazar seis tangentes a la curva. Escogeremos el punto  $(1, 0, 0)$ , el del infinito del eje de abscisas (podría valer cualquier otro, pero así se facilitan las cuentas). Entonces las rectas trazadas desde ese punto son de la forma  $y = \alpha$ , a las que vamos a cortar con la curva  $x^3 + my^3 - x - my = 0$ . Esto lleva a la ecuación  $x^3 - x + m\alpha^3 - m\alpha = 0$  (recordemos que el discriminante de la ecuación  $x^3 + px + q = 0$  es  $(p/3)^3 + (q/2)^3$ , y que su anulación implica la existencia de raíces dobles). En nuestro caso  $p = -1$  y  $q = m\alpha^3 - m\alpha$ , y el discriminante es:

$$\left(-\frac{1}{3}\right)^3 + \left(\frac{m\alpha^3 - m\alpha}{2}\right)^2$$

Si igualamos a cero tenemos las ecuaciones  $\alpha^3 - \alpha - 2\sqrt{3}/(9m) = 0$   $\alpha^3 - \alpha + 2\sqrt{3}/(9m) = 0$ , cada una de las cuales proporciona tres rectas tangentes. Para la curva de la familia correspondiente a  $m = 3/2$  las ecuaciones son  $\alpha^3 - \alpha - 4\sqrt{3}/27 = 0$  y  $\alpha^3 - \alpha + 4\sqrt{3}/27 = 0$ , cuyas soluciones aproximadas son 1.11,  $-0.28$  y  $-0.83$ , y 0.83, 0.28 y  $-1.11$  respectivamente.

Ahora bien, los puntos de contacto de una curva  $C$  de grado  $n$  con las tangentes a ella trazadas desde un punto  $P$  están sobre una curva de grado  $n-1$  llamada *curva polar* de  $C$  respecto del punto  $P$ . Si  $P = (a, b)$  y la ecuación de  $C$  es  $f(x, y) = 0$ , la de la polar es  $(x-a)f_x(x, y) + (y-b)f_y(x, y) - nf(x, y) = 0$ .

La polar de una curva de nuestra familia es una cónica de ecuación  $3ax^2 + 3bmy^2 - 2x - 2my - (a + mb) = 0$ . En coordenadas proyectivas, si  $P = (a, b, c)$ , la ecuación de la polar es  $aF_x(x, y, z) + bF_y(x, y, z) + cF_z(x, y, z) = 0$ . En el ejemplo que se acaba de ver, la curva polar respecto de  $(1, 0, 0)$  es  $3x^2 - 1 = 0$ , que se desdobra en dos rectas.

En la Figura 7 se pueden ver las rectas tangentes, la curva polar (formada por las rectas  $x = \sqrt{3}/3$  y  $x = -\sqrt{3}/3$ ) los puntos de tangencia.

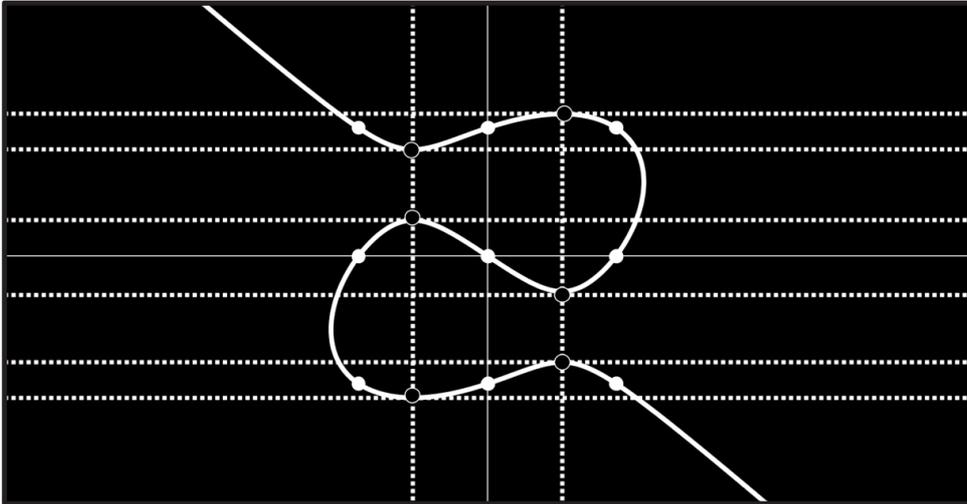


Figura 7

En la Figura 8 aparece el punto  $(5, 0)$ , las rectas tangentes a la cúbica que pasan por él y la curva polar, cuya ecuación es  $15x^2 - 2x - 3y - 5 = 0$ .

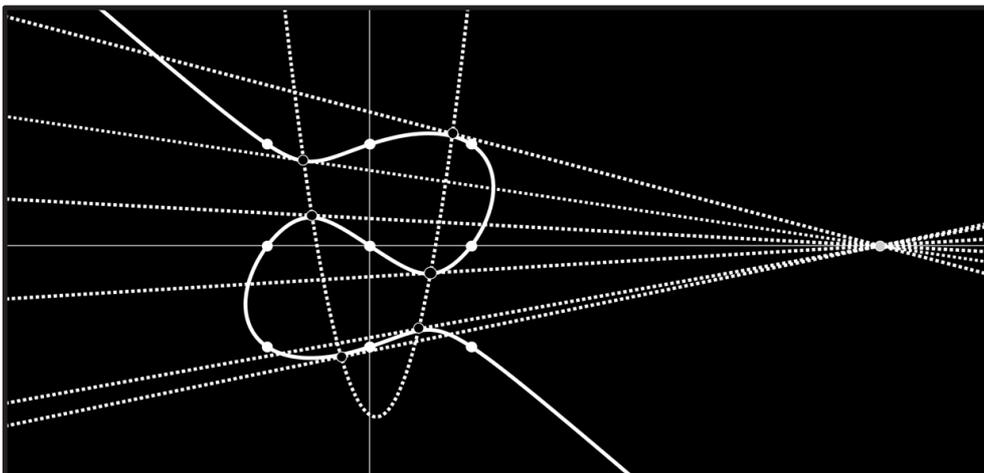


Figura 8

## 9. De cómo se transforman nuestras cúbicas en parábolas divergentes

Al final de su ya citada obra *Enumeratio Linearum Tertii Ordinis*, afirma Newton que cualquier cúbica es la proyección de una parábola divergente (curvas que tienen la forma  $y^2 = ax^3 + bx^2 + cx + d$ ), pero esto no fue justificado hasta 1733 por Alexis Clairaut (1713-1765) y François Nicole (1683-1758) quienes, con diferencia de muy pocos días, presentaron sendas demostraciones a la *Académie Royale des Sciences* de París. Aquí demostraremos cómo es esto posible con las curvas de la familia que estamos estudiando. En la ecuación  $x^3 + my^3 - x - my = 0$  ponemos  $(y-x)/m$  en lugar de la  $y$ , resulta lo siguiente:

$$\left(\frac{m^2-1}{m^2}\right)x^3 + \frac{1}{m^2}y^3 - \frac{3}{m^2}xy^2 + \frac{3}{m^2}x^2y - y = 0$$

A continuación pasamos la ecuación en coordenadas homogéneas:

$$\left(\frac{m^2-1}{m^2}\right)x^3 + \frac{1}{m^2}y^3 - \frac{3}{m^2}xy^2 + \frac{3}{m^2}x^2y - yz^2 = 0$$

Intercambiamos la  $y$  con la  $z$ :

$$\left(\frac{m^2-1}{m^2}\right)x^3 + \frac{1}{m^2}z^3 - \frac{3}{m^2}xz^2 + \frac{3}{m^2}x^2z - y^2z = 0$$

Y ahora aislamos la  $y$ , volvemos a las coordenadas cartesianas ordinarias y eliminamos denominadores:

$$m^2y^2 = (m^2-1)x^3 + 3x^2 - 3x + 1$$

Ahora cambiamos  $y$  por  $y/m$ , y ya estamos donde queríamos llegar:

$$y^2 = (m^2-1)x^3 + 3x^2 - 3x + 1$$

También puede ser puesta de la forma  $y^2 = m^2x^3 - (x-1)^3$ . De los nueve puntos comunes a las cúbicas, solo pasa por  $(0,1)$  y  $(0,-1)$ .

En la Figura 9 se puede ver la cúbica correspondiente a  $m=2$  y la parábola divergente proyectivamente equivalente a ella, de ecuación  $y^2 = 3x^3 + 3x^2 - 3x + 1$ .

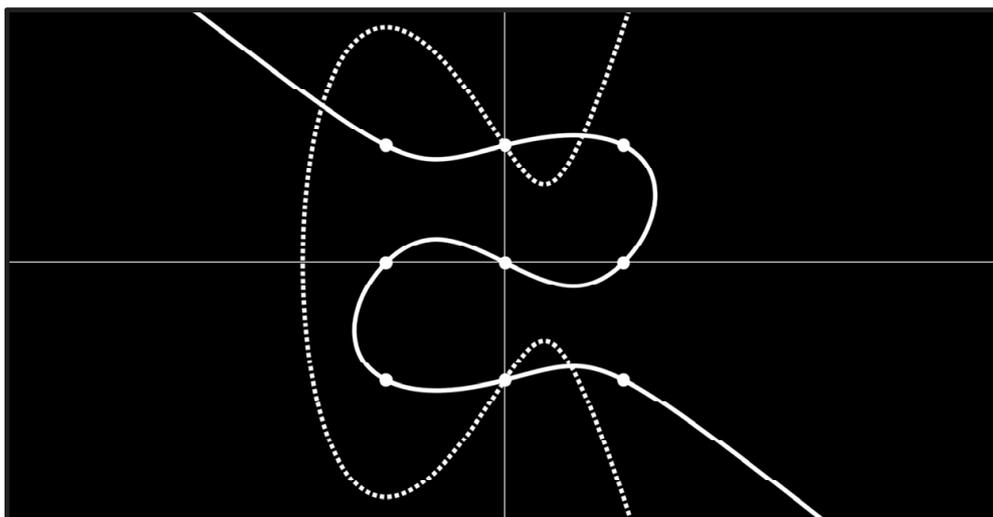


Figura 9

## Bibliografía

W. Fulton (1971), *Curvas algebraicas*, Editorial Reverté, Barcelona.

R. Moreno Castillo (2005), *Plücker y Poncelet. Dos modos de entender la geometría*, Editorial Nivola, Madrid.

R. Moreno Castillo. (2021), *Breve introducción a la historia de las curvas algebraicas*, Editorial Nivola, Madrid.

M<sup>a</sup>. J. De la Puente Muñoz (2007), *Curvas algebraicas planas*, Servicio de Publicaciones de la Universidad de Cádiz.

# A family of polynomials of degree 8 whose Galois group is the quaternion group $\mathcal{Q}_8$

## Una familia de polinomios de grado 8 cuyo grupo de Galois es el grupo cuaternión $\mathcal{Q}_8$

Arturo Rodríguez Rodríguez\*,  
María Belén Rodríguez Rodríguez\*\*

\* Departamento de Matemáticas, I.E.S. Celestino Mutis

\*\* Departamento de Matemáticas, I.E.S. Carlos III

arturomath@hotmail.com,  
maria.rodriguez13@educa.madrid.org

### Resumen

*Let  $p, q$  be prime integers with  $q < p$  and let  $\alpha_{pq} := (q + \sqrt{q})(p + \sqrt{p})$ . Let  $\beta_{pq}$  be a real square root of  $\alpha_{pq}$ . We prove that  $\mathbb{Q}(\beta_{pq})|\mathbb{Q}$  is a Galois extension if and only if  $q - 1$  is a square in  $\mathbb{Z}$  and, either  $p - 1$  is a square in  $\mathbb{Z}$  or  $(p - 1)/q$  is a square in  $\mathbb{Z}$ . In the first case the Galois group  $\text{Gal}(\mathbb{Q}(\beta_{pq})|\mathbb{Q})$  is isomorphic to  $\mathbb{Z}_4 \times \mathbb{Z}_2$  and in the second one it is isomorphic to the quaternion group  $\mathcal{Q}_8$ . Thus, under these hypothesis, the minimal polynomial of  $\beta_{pq}$  over  $\mathbb{Q}$  has degree 8 and its Galois group over  $\mathbb{Q}$  is either  $\mathbb{Z}_4 \times \mathbb{Z}_2$  or  $\mathcal{Q}_8$ .*

### Introducción

El denominado *problema inverso de la teoría de Galois* consiste en, fijados un cuerpo  $E$  y un grupo finito  $G$ , encontrar una extensión de Galois  $F|E$  cuyo grupo de Galois sea  $G$ . Dedekind encontró en 1886 una extensión de Galois de los racionales cuyo grupo de Galois es el grupo cuaternión  $\mathcal{Q}_8$ . Este resultado fue publicado en su artículo póstumo [1] y es el origen de este trabajo. Cabe

señalar que la estrategia de Dedekind consiste en rescatar la estructura que ha de tener el retículo de subextensiones de una extensión cuyo grupo de Galois sea  $\mathcal{Q}_8$  a partir de la estructura del retículo de subgrupos de  $\mathcal{Q}_8$ .

Posteriormente Witt encontró qué condiciones debe cumplir un cuerpo  $E$  para que una extensión suya  $F|E$  tenga a  $\mathcal{Q}_8$  por grupo de Galois. La monografía [7] contiene el citado resultado de Witt y mucho más acerca del problema inverso de la teoría de Galois. La construcción de Witt exige la existencia de elementos en el cuerpo  $E$  que son suma de tres cuadrados en  $E$  pero no de dos y fue refinada posteriormente por Fujisaki en [5]. Merece la pena señalar que su construcción y la nuestra son completamente distintas.

En este artículo asociamos a cada par de números primos  $(q, p)$  con  $q < p$  el número real  $\alpha_{pq} := (q + \sqrt{q})(p + \sqrt{p})$ , su raíz cuadrada positiva  $\beta_{pq} \in \mathbb{R}$  y el menor cuerpo  $\mathbb{Q}(\beta_{pq})$  que contiene a  $\mathbb{Q}$  y a  $\beta_{pq}$ . Probamos que  $\mathbb{Q}(\beta_{pq})|\mathbb{Q}$  es una extensión de  $\mathbb{Q}$  de grado 8 y demostramos que es de Galois si y sólo si  $q - 1$  es el cuadrado de un número entero y, bien  $p - 1$  es el cuadrado de un número entero o bien  $(p - 1)/q$  es el cuadrado de un número entero.

En el primer caso el grupo de Galois de la extensión es  $\mathbb{Z}_4 \times \mathbb{Z}_2$ , mientras que en el segundo dicho grupo es  $\mathcal{Q}_8$ .

Durante el Congreso Internacional de Matemáticos celebrado en Cambridge in 1912, Edmund Landau conjeturó que existen infinitos números primos  $q$  tales que  $q - 1$  es el cuadrado de un entero. Once años después Hardy y Littlewood conjeturaron en [6] que, excepto en casos triviales, dados enteros  $a, b$  y  $c$  la sucesión  $(an^2 + bn + c)_{n \in \mathbb{N}}$  contiene infinitos números primos. Un caso particular corresponde a la elección:  $a := q, b := 0$  y  $c := 1$ , esto es, los primos de la forma  $1 + qn^2$  que aparecen en el Teorema 3.1, pero también este caso es a día de hoy sólo una conjetura. Por tanto no se sabe si la familia de polinomios de grado 8 construidos en este artículo, irreducibles en  $\mathbb{Z}[t]$  y cuyo grupo de Galois es o bien  $\mathbb{Z}_4 \times \mathbb{Z}_2$  o bien  $\mathcal{Q}_8$ , es finita o infinita.

El lector encontrará en [2], [8] o [9] los prerrequisitos sobre Teoría de Galois empleados en este artículo, y en [3] los referentes a la Teoría de grupos. Las notaciones utilizadas son estándar. En particular, dada una extensión de cuerpos  $E|K$  denotamos  $[E : K]$  a su *grado*, es decir, la dimensión de  $E$  como  $K$ -espacio vectorial, y emplearemos constantemente la denominada *transitividad del grado*, que dice que dadas extensiones de cuerpos  $E|K$  y

$F|E$  se tiene  $[F : K] = [F : E] \cdot [E : K]$ .

Dados  $u_1, \dots, u_r \in E$ , denotamos  $K(u_1, \dots, u_r)$  al menor subcuerpo de  $E$  que contiene a  $K$  y a  $u_1, \dots, u_r$ . El *grupo de Galois* de  $E|K$ , esto es, el grupo de los automorfismos de  $E$  que dejan fijo cada elemento de  $K$ , se denotará  $\text{Gal}(E|K)$ . Si  $x \in E$  es algebraico sobre  $K$  denotamos  $\text{Irr}(x; K)$  el *polinomio mínimo* de  $x$  sobre  $K$ , es decir, el único polinomio mónico de  $K[t]$  cuyo grado es mínimo entre los grados de los polinomios no nulos de  $K[t]$  que tienen a  $x$  por raíz.

Por último señalemos que a lo largo del trabajo  $A \subset B$  significa que el conjunto  $A$  está contenido o es igual al conjunto  $B$ , y pondremos  $A \subsetneq B$  para indicar que  $A$  está estrictamente contenido en  $B$ . Además empleamos la denominada *notación sajona* para multiplicar biyecciones de un conjunto dado; en particular automorfismos de extensiones de cuerpos. Dadas biyecciones  $f$  y  $g$  de un conjunto  $X$  se denota  $f \cdot g$ , o simplemente  $fg$ , la biyección definida por  $fg(x) = g(f(x))$  para cada  $x \in X$ . Nótese que  $fg = g \circ f$ .

Con el fin de hacer este artículo casi autocontenido dedicamos su primera sección a presentar algunos resultados muy elementales acerca de extensiones cuadráticas de cuerpos.

## 1. Extensiones cuadráticas

**Lema 1.1** (1) Sean  $E|K$  una extensión de cuerpos y  $a, b \in K$  tales que  $\sqrt{a}, \sqrt{b} \in E \setminus K$ . Entonces,  $K(\sqrt{a}) = K(\sqrt{b})$  si y sólo si el cociente  $\frac{b}{a}$  es un cuadrado en  $K$ .

(2) Sean  $p_1$  y  $p_2$  números enteros primos entre sí tales que  $p_2 - 1$  no es un cuadrado en  $\mathbb{Z}$ . Entonces

$$\mathbb{Q}(\sqrt{p_2 - 1}) \neq \mathbb{Q}(\sqrt{p_2}) \quad \text{y} \quad \mathbb{Q}(\sqrt{p_2 - 1}) \neq \mathbb{Q}(\sqrt{p_1 p_2}).$$

*Demostración.* (1) Supongamos que  $\frac{b}{a} = c^2$  donde  $c \in K$ . Así,  $\sqrt{b} = \pm c\sqrt{a}$ , luego  $K(\sqrt{b}) = K(\sqrt{a})$ . Recíprocamente, supongamos que se cumple la igualdad  $K(\sqrt{a}) = K(\sqrt{b})$ . Como  $\sqrt{a} \notin K$ , una base de  $K(\sqrt{a})$  como  $K$ -espacio vectorial es  $\{1, \sqrt{a}\}$ . Por tanto  $\sqrt{b} = x + y\sqrt{a}$  para ciertos  $x, y \in K$ . En consecuencia  $b = x^2 + ay^2 + 2xy\sqrt{a}$ , luego  $b = x^2 + ay^2$  y  $xy = 0$ . Si  $y = 0$

entonces  $b = x^2$ , es decir,  $\sqrt{b} = \pm x \in K$ , contra la hipótesis. Por ello  $y \neq 0$  y  $b = ay^2$ , es decir,  $\frac{b}{a} = y^2$  es un cuadrado en  $K$ .

(2) Supongamos que  $\mathbb{Q}(\sqrt{p_2 - 1}) = \mathbb{Q}(\sqrt{p_2})$ . Por el apartado (1) existen enteros coprimos  $x$  e  $y$  tales que  $\frac{p_2 - 1}{p_2} = \left(\frac{x}{y}\right)^2$ , es decir,  $(p_2 - 1)y^2 = p_2x^2$ . Así, como  $\text{mcd}(p_2 - 1, p_2) = 1$ , se tiene que  $p_2$  divide a  $y$ . Sea  $z \in \mathbb{Z}$  tal que  $y = p_2z$ . Entonces  $(p_2 - 1)z^2p_2^2 = p_2x^2$ , o sea,  $(p_2 - 1)z^2p_2 = x^2$ . En consecuencia  $p_2$  también divide a  $x$ , lo que contradice el hecho de que  $\text{mcd}(x, y) = 1$ .

De igual forma, si  $\mathbb{Q}(\sqrt{p_2 - 1}) = \mathbb{Q}(\sqrt{p_1p_2})$ . Por el apartado (1) existen  $x$  e  $y$  enteros coprimos tales que  $(p_2 - 1)y^2 = p_1p_2x^2$ . Por tanto  $p_2$  divide a  $y$ , y sea  $z \in \mathbb{Z}$  tal que  $y = p_2z$ . Entonces  $(p_2 - 1)z^2p_2 = p_1x^2$ , así que  $p_2$  también divide a  $x$  y esto es falso.  $\square$

**Observación 1.2** Los primos  $p_1 := 3$  y  $p_2 := 13$  están en las condiciones del lema anterior pero  $\frac{p_2 - 1}{p_1} = 2^2$ , por lo que  $\mathbb{Q}(\sqrt{p_2 - 1}) = \mathbb{Q}(\sqrt{p_1})$ .

**Lema 1.3** (1) Sean  $q_1, \dots, q_r$  enteros positivos coprimos dos a dos y tales que ninguno de ellos es el cuadrado de un número entero. Entonces,

$$[\mathbb{Q}(\sqrt{q_1}, \dots, \sqrt{q_r}) : \mathbb{Q}] = 2^r.$$

(2) Sean  $p, q$  primos distintos. Entonces  $\mathbb{Q}(\sqrt{p}, \sqrt{q})|\mathbb{Q}$  es una extensión de Galois de grado 4. Una base de  $\mathbb{Q}(\sqrt{p}, \sqrt{q})$  como  $\mathbb{Q}$ -espacio vectorial es la dada por  $\mathcal{B} := \{1, \sqrt{p}, \sqrt{q}, \sqrt{pq}\}$  y el grupo de Galois de  $\mathbb{Q}(\sqrt{p}, \sqrt{q})|\mathbb{Q}$  es

$$\text{Gal}(\mathbb{Q}(\sqrt{p}, \sqrt{q})|\mathbb{Q}) = \{\varphi_{ij} : i, j = 0, 1\}, \quad (1)$$

donde cada automorfismo  $\varphi_{ij}$  queda determinado por las condiciones

$$\varphi_{ij}(\sqrt{q}) := (-1)^i \sqrt{q} \quad \text{y} \quad \varphi_{ij}(\sqrt{p}) := (-1)^j \sqrt{p}.$$

En particular,  $\text{Gal}(\mathbb{Q}(\sqrt{p}, \sqrt{q})|\mathbb{Q}) \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$ .

*Demostración.* (1) Realizaremos la demostración por inducción sobre  $r$ . Sea  $r = 1$ . Como  $q_1$  no es un cuadrado en  $\mathbb{Z}$  existe un divisor primo  $p$  de  $q_1$  tal que  $p^2 \nmid q_1$  luego, por el Criterio de Eisenstein, [4, VI.2.6], el polinomio  $t^2 - q_1$  es irreducible en  $\mathbb{Z}[t]$ , así que  $[\mathbb{Q}(\sqrt{q_1}) : \mathbb{Q}] = 2$ . Sea  $r \geq 2$  y, para

cada  $1 \leq s \leq r$ , denotamos  $K_s := \mathbb{Q}(\sqrt{q_1}, \dots, \sqrt{q_s})$ . Como  $\mathbb{Q} \subset K_{r-1} \subset K_r$  se deduce de la transitividad del grado que

$$[K_r : \mathbb{Q}] = [K_r : K_{r-1}] \cdot [K_{r-1} : \mathbb{Q}] \leq [\mathbb{Q}(\sqrt{q_r}) : \mathbb{Q}] \cdot 2^{r-1} = 2^r, \quad (2)$$

porque  $\mathfrak{t}^2 - q_r$  es el polinomio mínimo de  $\sqrt{q_r}$  sobre  $\mathbb{Q}$ . Para comprobar que la desigualdad en (2) es de hecho una igualdad basta ver que  $[K_r : K_{r-1}] = 2$  o, equivalentemente, que  $\sqrt{q_r} \notin K_{r-1} = K_{r-2}(\sqrt{q_{r-1}})$ . En caso contrario, y puesto que por hipótesis de inducción  $[K_{r-1} : K_r] = 2$ , existirían  $a, b \in K_{r-2}$  tales que

$$\sqrt{q_r} = a + b\sqrt{q_{r-1}}. \quad (3)$$

Si  $b = 0$  se tendría  $\sqrt{q_r} \in K_{r-2}$ , o sea,  $K_{r-2}(\sqrt{q_r}) = K_{r-2}$  y, por la hipótesis de inducción,

$$2^{r-2} = [K_{r-2} : \mathbb{Q}] = [K_{r-2}(\sqrt{q_r}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{q_1}, \dots, \sqrt{q_{r-2}}, \sqrt{q_r}) : \mathbb{Q}] = 2^{r-1},$$

que es falso. En consecuencia  $b \neq 0$  y, por (3),

$$0 = (\sqrt{q_r} - b\sqrt{q_{r-1}})^2 - a^2 = q_r + b^2q_{r-1} - a^2 - 2b\sqrt{q_rq_{r-1}},$$

lo que implica que  $\sqrt{q_rq_{r-1}} \in K_{r-2}$ .

Como ni  $q_r$  ni  $q_{r-1}$  son cuadrados en  $\mathbb{Q}$  y  $\text{mcd}(q_{r-1}, q_r) = 1$ , entonces tampoco  $q_rq_{r-1}$  es un cuadrado en  $\mathbb{Q}$ , y  $\text{mcd}(q_i, q_rq_{r-1}) = 1$  para todo índice  $i = 1, \dots, r-2$ . Así, empleando de nuevo la hipótesis de inducción,

$$\begin{aligned} 2^{r-2} &= [K_{r-2} : \mathbb{Q}] = [K_{r-2}(\sqrt{q_rq_{r-1}}) : \mathbb{Q}] \\ &= [\mathbb{Q}(\sqrt{q_1}, \dots, \sqrt{q_{r-2}}, \sqrt{q_rq_{r-1}}) : \mathbb{Q}] = 2^{r-1}, \end{aligned}$$

que es una contradicción.

(2) Por el apartado (1) se tiene  $[\mathbb{Q}(\sqrt{p}, \sqrt{q}) : \mathbb{Q}] = 4$  y  $[\mathbb{Q}(\sqrt{p}) : \mathbb{Q}] = 2$ , lo que implica  $[\mathbb{Q}(\sqrt{p}, \sqrt{q}) : \mathbb{Q}(\sqrt{p})] = 2$ . Por ello  $\{1, \sqrt{q}\}$  es una base de  $\mathbb{Q}(\sqrt{p}, \sqrt{q})$  como  $\mathbb{Q}(\sqrt{p})$ -espacio vectorial y  $\{1, \sqrt{p}\}$  es una base de  $\mathbb{Q}(\sqrt{p})$  como  $\mathbb{Q}$ -espacio vectorial. Entonces, por transitividad,  $\mathcal{B}$  es una base de  $\mathbb{Q}(\sqrt{p}, \sqrt{q})$  como  $\mathbb{Q}$ -espacio vectorial.

Además  $\mathbb{Q}(\sqrt{p}, \sqrt{q})$  es el cuerpo de descomposición sobre  $\mathbb{Q}$  del polinomio  $(\mathfrak{t}^2 - p)(\mathfrak{t}^2 - q)$ , por lo que  $\mathbb{Q}(\sqrt{p}, \sqrt{q})|\mathbb{Q}$  es una extensión de Galois de grado

4. Cada elemento  $\sigma$  de su grupo de Galois fija  $p$  y  $q$ , luego  $\sigma(\sqrt{p}) = \pm\sqrt{p}$  y  $\sigma(\sqrt{q}) = \pm\sqrt{q}$ , de donde se deduce que  $\sigma^2$  es la identidad, así que

$$\text{Gal}(\mathbb{Q}(\sqrt{p}, \sqrt{q})|\mathbb{Q}) \simeq \mathbb{Z}_2 \times \mathbb{Z}_2.$$

□

**Lema 1.4** Sean  $p$  y  $q$  números primos distintos,  $K := \mathbb{Q}(\sqrt{q}, \sqrt{p})$ ,

$$\alpha_{pq} := (q + \sqrt{q})(p + \sqrt{p}) \quad \text{y} \quad \beta_{pq} := \sqrt{\alpha_{pq}} \in \mathbb{R}^+.$$

(1) Se tiene  $[\mathbb{Q}(\alpha_{pq}) : \mathbb{Q}] = 4$  y por tanto  $K = \mathbb{Q}(\alpha_{pq})$ .

(2) El polinomio mínimo de  $\alpha_{pq}$  sobre  $\mathbb{Q}$  es

$$\begin{aligned} \text{Irr}(\alpha_{pq}; \mathbb{Q})(\mathfrak{t}) &= \mathfrak{t}^4 - 4qpt^3 + 2qp(3qp - p - q - 1)t^2 \\ &\quad - 4q^2p^2(q - 1)(p - 1)t + q^2(q - 1)^2p^2(p - 1)^2. \end{aligned}$$

(3) Se tiene  $[\mathbb{Q}(\beta_{pq}) : \mathbb{Q}] = 8$  y el polinomio mínimo de  $\beta_{pq}$  sobre  $\mathbb{Q}$  es

$$f_{pq}(\mathfrak{t}) := \text{Irr}(\beta_{pq}; \mathbb{Q})(\mathfrak{t}) = \text{Irr}(\alpha_{pq}; \mathbb{Q})(\mathfrak{t}^2).$$

*Demostración.* (1) Escribimos

$$\alpha_{pq} = qp + p\sqrt{q} + q\sqrt{p} + \sqrt{qp}. \quad (4)$$

Por el Lema 1.3,  $\mathcal{B} := \{1, \sqrt{q}, \sqrt{p}, \sqrt{qp}\}$  es una base de  $K$  como  $\mathbb{Q}$ -espacio vectorial, luego  $[K : \mathbb{Q}] = 4$ . Además,  $\mathbb{Q} \subset \mathbb{Q}(\alpha_{pq}) \subset K$ , y de la escritura (4) se deduce que  $\alpha_{pq} \in K \setminus \mathbb{Q}$  ya que  $p, q \neq 0$ . En consecuencia  $\mathbb{Q} \subsetneq \mathbb{Q}(\alpha_{pq}) \subset K$ , por lo que  $[\mathbb{Q}(\alpha_{pq}) : \mathbb{Q}] \in \{2, 4\}$ .

Además  $\text{Gal}(K|\mathbb{Q})$  es isomorfo a  $\mathbb{Z}_2 \times \mathbb{Z}_2$ , por lo que tiene, exactamente, tres subgrupos no triviales, todos de orden 2. Por el Teorema fundamental de la Teoría de Galois, [2, Ch. IV.2], la extensión  $K|\mathbb{Q}$  tiene, exactamente, tres subextensiones no triviales, las tres de grado 2. Como  $\mathbb{Q}(\sqrt{q})$ ,  $\mathbb{Q}(\sqrt{p})$  y  $\mathbb{Q}(\sqrt{qp})$  son subcuerpos de  $K$  y cada uno de ellos es una extensión de  $\mathbb{Q}$  de grado 2 deducimos que estas son, justamente, las únicas subextensiones de  $K|\mathbb{Q}$  de dicho grado.

Para probar la igualdad  $K = \mathbb{Q}(\alpha_{pq})$  es suficiente ver que el grado de la extensión  $\mathbb{Q}(\alpha_{pq})|\mathbb{Q}$  es 4, es decir, que  $\mathbb{Q}(\alpha_{pq})$  no coincide ni con  $\mathbb{Q}(\sqrt{p})$  ni

con  $\mathbb{Q}(\sqrt{q})$  ni con  $\mathbb{Q}(\sqrt{pq})$ . Probaremos que  $\mathbb{Q}(\alpha_{pq}) \neq \mathbb{Q}(\sqrt{q})$  y dejamos las comprobaciones restantes al lector. En caso contrario,  $\alpha_{pq} \in \mathbb{Q}(\sqrt{q})$ , luego existen  $a, b \in \mathbb{Q}$  tales que

$$qp + p\sqrt{q} + q\sqrt{p} + \sqrt{qp} = \alpha_{pq} = a + b\sqrt{q},$$

es decir,

$$(qp - a) + (p - b)\sqrt{q} + q\sqrt{p} + \sqrt{qp} = 0,$$

y esto es falso porque los elementos de  $\mathcal{B}$  son  $\mathbb{Q}$ -linealmente independientes.

(2) Con las notaciones del Lema 1.3,

$$\varphi_{ij}(\alpha_{pq}) = (q + (-1)^i \sqrt{q}) \cdot (p + (-1)^j \sqrt{p}) \quad \text{para } i, j = 0, 1.$$

Por ser  $\mathbb{Q}(\alpha_{pq})|\mathbb{Q}$  una extensión de Galois de grado 4 el polinomio mínimo  $\text{Irr}(\alpha_{pq}; \mathbb{Q})$  de  $\alpha_{pq}$  sobre  $\mathbb{Q}$  tiene grado 4 y sus cuatro raíces son los números  $\varphi_{ij}(\alpha_{pq})$  donde  $i, j = 0, 1$ . En consecuencia,

$$\begin{aligned} \text{Irr}(\alpha_{pq}; \mathbb{Q})(\mathfrak{t}) &= \prod_{i,j=0,1} (\mathfrak{t} - \varphi_{ij}(\alpha_{pq})) = \mathfrak{t}^4 - 4qpt^3 + 2qp(3qp - p - q - 1)\mathfrak{t}^2 \\ &\quad - 4q^2p^2(q-1)(p-1)\mathfrak{t} + q^2(q-1)^2p^2(p-1)^2. \end{aligned}$$

(3) Aplicando la transitividad del grado a  $\mathbb{Q} \subset \mathbb{Q}(\alpha_{pq}) \subset \mathbb{Q}(\beta_{pq})$  se tiene

$$[\mathbb{Q}(\beta_{pq}) : \mathbb{Q}] = [\mathbb{Q}(\beta_{pq}) : \mathbb{Q}(\alpha_{pq})] \cdot [\mathbb{Q}(\alpha_{pq}) : \mathbb{Q}] = 4 \cdot [\mathbb{Q}(\beta_{pq}) : \mathbb{Q}(\alpha_{pq})]$$

y  $\beta_{pq}$  es raíz de  $\mathfrak{t}^2 - \alpha_{pq} \in \mathbb{Q}(\alpha_{pq})[\mathfrak{t}]$ . Por tanto, o bien  $[\mathbb{Q}(\beta_{pq}) : \mathbb{Q}] = 8$ , si  $\beta_{pq} \notin \mathbb{Q}(\alpha_{pq})$ , o bien  $[\mathbb{Q}(\beta_{pq}) : \mathbb{Q}] = 4$  si  $\beta_{pq} \in \mathbb{Q}(\alpha_{pq})$ . Probemos, por reducción al absurdo, que  $\beta_{pq} \notin \mathbb{Q}(\alpha_{pq})$ . En caso contrario,

$$\begin{aligned} \mathbb{Q}(\sqrt{p})(\beta_{pq}) \subset K(\beta_{pq}) &= \mathbb{Q}(\alpha_{pq})(\beta_{pq}) = \mathbb{Q}(\alpha_{pq}) \\ &= K = \mathbb{Q}(\sqrt{p})(\sqrt{q}) \subset \mathbb{Q}(\sqrt{p})(\beta_{pq}). \end{aligned}$$

Entonces  $\mathbb{Q}(\sqrt{p})(\beta_{pq}) = \mathbb{Q}(\sqrt{p})(\sqrt{q})$  y  $\beta_{pq}, \sqrt{q} \notin \mathbb{Q}(\sqrt{p})$ . Se deduce del Lema 1.1 que el cociente  $\frac{\alpha_{pq}}{q}$  es un cuadrado en  $\mathbb{Q}(\sqrt{p})$ , esto es, existen  $x, y \in \mathbb{Q}$  tales que  $\frac{\alpha_{pq}}{q} = (x + y\sqrt{p})^2$ . Por tanto,

$$\frac{(p + \sqrt{p})(q + \sqrt{q})}{q} = x^2 + py^2 + 2xy\sqrt{p},$$

o lo que es igual,

$$q(p - x^2 - py^2) + q(1 - 2xy)\sqrt{p} + p\sqrt{q} + \sqrt{pq} = 0.$$

Esto es absurdo porque  $\{1, \sqrt{q}, \sqrt{p}, \sqrt{pq}\}$  son  $\mathbb{Q}$ -linealmente independientes. Por último, de que  $\mathbb{Q}(\beta_{pq})|\mathbb{Q}$  tiene grado 8 resulta la igualdad

$$f_{pq}(\mathbf{t}) = \text{Irr}(\beta_{pq}; \mathbb{Q})(\mathbf{t}) = \text{Irr}(\alpha_{pq}; \mathbb{Q})(\mathbf{t}^2).$$

□

**Observación 1.5** Con las notaciones anteriores sean  $p$  y  $q$  números primos distintos y

$$\begin{aligned} f_{pq}(\mathbf{t}) : &= \mathbf{t}^8 - 4qpt^6 + 2qp(3qp - p - q - 1)\mathbf{t}^4 \\ &\quad - 4q^2p^2(q - 1)(p - 1)\mathbf{t}^2 + q^2(q - 1)^2p^2(p - 1)^2. \end{aligned}$$

En las Secciones 2 y 3 se estudiará bajo qué condiciones el grupo de Galois del polinomio  $f_{pq}$  tiene orden 8.

**Notación 1.6** Se desprende de los apartados (1) y (3) del Lema 1.4 que  $\mathbb{Q}(\beta_{pq})|K$  es una extensión de grado 2. Esto implica, por el Teorema 10.1 en [9], que existen  $\tau, \sigma \in \text{Gal}(\mathbb{Q}(\beta)|\mathbb{Q})$  tales que  $\tau|_K = \varphi_{1,0}$  y  $\sigma|_K = \varphi_{0,1}$ . En particular,

$$\tau(\sqrt{p}) = \sqrt{p}, \quad \tau(\sqrt{q}) = -\sqrt{q}, \quad \sigma(\sqrt{q}) = \sqrt{q} \quad \text{y} \quad \sigma(\sqrt{p}) = -\sqrt{p}. \quad (5)$$

Fijamos estas notaciones en todo lo que sigue y, dados un grupo  $G$  y un elemento  $g \in G$  denotamos  $o(g)$  el *orden* de  $g$ , esto es, el menor exponente positivo  $k$  tal que  $g^k = 1_G$ .

## 2. El caso en que $\mathbb{Q}(\beta_{pq})|\mathbb{Q}$ es extensión de Galois

A lo largo de esta sección mantenemos las notaciones introducidas en el Lema 1.4 y en 1.6 y suponemos que la extensión  $\mathbb{Q}(\beta_{pq})|\mathbb{Q}$  es de Galois. En el Lema 2.1 demostramos que esto implica que el grupo de Galois de la extensión es bien  $\mathbb{Z}_4 \times \mathbb{Z}_2$  o bien  $\mathbb{Q}_8$ , y que  $p$  y  $q$  satisfacen ciertas condiciones de naturaleza aritmética. En el Lema 2.2 probamos que los automorfismos  $\sigma$  y  $\tau$

introducidas en (5) tienen orden 4, mientras que en el Teorema 2.3 estudiamos cuándo estos automorfismos conmutan. Como consecuencia, en el Corolario 2.4 determinamos bajo qué condiciones el grupo de Galois de la extensión es  $\mathbb{Z}_4 \times \mathbb{Z}_2$  y bajo cuáles es  $\mathcal{Q}_8$ .

**Lema 2.1** *Supongamos que  $q < p$  y que  $\mathbb{Q}(\beta_{pq})|\mathbb{Q}$  es una extensión de Galois.*

(1) *El grupo de Galois  $\text{Gal}(\mathbb{Q}(\beta_{pq})|\mathbb{Q})$  es isomorfo o bien a  $\mathbb{Z}_4 \times \mathbb{Z}_2$ , o bien al grupo diedral  $\mathcal{D}_4$  o bien al grupo cuaternión  $\mathcal{Q}_8$ , y*

$$\mathbb{Q}(\sqrt{p})|\mathbb{Q}, \quad \mathbb{Q}(\sqrt{q})|\mathbb{Q} \quad \text{y} \quad \mathbb{Q}(\sqrt{qp})|\mathbb{Q}$$

*son las únicas subextensiones de grado 2 de  $\mathbb{Q}(\beta_{pq})|\mathbb{Q}$ .*

(2)  *$q - 1$  es el cuadrado de un número entero y, bien  $p - 1$  es el cuadrado de un número entero o bien existe  $r \in \mathbb{Z}^+$  tal que  $p - 1 = qr^2$ .*

*Demostración.* (1) Como  $\mathbb{Q}(\alpha_{pq}) \subset \mathbb{Q}(\beta_{pq})$  es claro que  $\mathbb{Q}(\sqrt{q})|\mathbb{Q}$  y  $\mathbb{Q}(\sqrt{p})|\mathbb{Q}$ , son subextensiones de grado 2 (distintas) de  $\mathbb{Q}(\beta_{pq})|\mathbb{Q}$ . Por tanto, por el Teorema Fundamental de la Teoría de Galois, el grupo  $\text{Gal}(\mathbb{Q}(\beta_{pq})|\mathbb{Q})$  tiene, al menos, dos subgrupos de orden 4 distintos, por lo que no es cíclico.

Comprobemos a continuación que no es isomorfo a  $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ . Esto demostrará la primera parte de este apartado ya que los dos anteriores son, junto con  $\mathcal{Q}_8$ ,  $\mathbb{Z}_4 \times \mathbb{Z}_2$  y el grupo diedral  $\mathcal{D}_4$ , los únicos grupos de orden 8.

Como las raíces del polinomio mínimo  $\text{Irr}(\alpha_{pq}; \mathbb{Q})$  de  $\alpha_{pq}$  sobre  $\mathbb{Q}$  son

$$\begin{aligned} \alpha_1 &:= \alpha_{pq} = (q + \sqrt{q})(p + \sqrt{p}), & \alpha_2 &:= (q - \sqrt{q})(p + \sqrt{p}), \\ \alpha_3 &:= (q + \sqrt{q})(p - \sqrt{p}) & \text{y} & \quad \alpha_4 := (q - \sqrt{q})(p - \sqrt{p}), \end{aligned}$$

las raíces del polinomio mínimo  $\text{Irr}(\beta_{pq}; \mathbb{Q})$  de  $\beta_{pq}$  sobre  $\mathbb{Q}$  son

$$\begin{aligned} \beta_1 &:= \sqrt{\alpha_1}, & \beta_2 &:= \sqrt{\alpha_2}, & \beta_3 &:= \sqrt{\alpha_3}, & \beta_4 &:= \sqrt{\alpha_4}, \\ \beta_5 &:= -\beta_1, & \beta_6 &:= -\beta_2, & \beta_7 &:= -\beta_3 & \text{y} & \beta_8 := -\beta_4, \end{aligned} \tag{6}$$

donde  $\beta_1 := \beta_{pq}$ . Cada  $\beta_i$  pertenece a  $\mathbb{Q}(\beta_{pq})$  porque estamos suponiendo que la extensión  $\mathbb{Q}(\beta_{pq})|\mathbb{Q}$  es de Galois. Entonces, con las notaciones en 1.6,

$$\tau(\beta_1^2) = \varphi_{1,0}(\alpha_1) = (q - \sqrt{q})(p + \sqrt{p}) = \alpha_2 = \beta_2^2,$$

por lo que  $\tau(\beta_1) = \pm\beta_2$  y podemos suponer sin pérdida de generalidad que  $\tau(\beta_1) = \beta_2$ . Nótese que

$$\begin{aligned}\beta_1\beta_2 &= \sqrt{(q + \sqrt{q})(p + \sqrt{p})(q - \sqrt{q})(p + \sqrt{p})} \\ &= (p + \sqrt{p})\sqrt{q^2 - q} = (p + \sqrt{p})\sqrt{q}\sqrt{q - 1}.\end{aligned}\tag{7}$$

En particular,

$$\sqrt{q - 1} = \frac{\beta_1\beta_2}{(p + \sqrt{p})\sqrt{q}} \in \mathbb{Q}(\beta_{pq}).\tag{8}$$

Supongamos, por reducción al absurdo, que  $\text{Gal}(\mathbb{Q}(\beta_{pq})|\mathbb{Q}) \simeq \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ . Entonces  $\tau^2 = \text{id}$ , luego  $\tau(\beta_2) = \beta_1$ . Además

$$\begin{aligned}\beta_1\beta_2 &= \tau(\beta_1)\tau(\beta_2) = \tau(\beta_1\beta_2) \\ &= (p + \sqrt{p})(-\sqrt{q})\tau(\sqrt{q - 1}) = -\frac{\beta_1\beta_2\tau(\sqrt{q - 1})}{\sqrt{q - 1}},\end{aligned}\tag{9}$$

por lo que  $\tau(\sqrt{q - 1}) = -\sqrt{q - 1}$ . En consecuencia,

$$\tau(\sqrt{p}) = \sqrt{p}, \quad \tau(\sqrt{q}) = -\sqrt{q} \quad \text{y} \quad \tau(\sqrt{q - 1}) = -\sqrt{q - 1}.\tag{10}$$

Comprobemos que  $\sqrt{q - 1} \notin K$ . En caso contrario existirían  $a_0, a_1, a_2, a_3 \in \mathbb{Q}$  tales que

$$\sqrt{q - 1} = a_0 + a_1\sqrt{p} + a_2\sqrt{q} + a_3\sqrt{pq}.$$

Empleando (10) se deduce que

$$\tau(\sqrt{q - 1}) = -\sqrt{q - 1} = -a_0 - a_1\sqrt{p} - a_2\sqrt{q} - a_3\sqrt{pq},$$

pero también

$$\tau(\sqrt{q - 1}) = a_0 + a_1\tau(\sqrt{p}) + a_2\tau(\sqrt{q}) + a_3\tau(\sqrt{pq}) = a_0 + a_1\sqrt{p} - a_2\sqrt{q} - a_3\sqrt{pq},$$

luego  $a_0 = a_1 = 0$  ya que  $\{1, \sqrt{p}, \sqrt{q}, \sqrt{pq}\}$  son  $\mathbb{Q}$ -linealmente independientes. Por tanto,

$$\sqrt{q - 1} = a_2\sqrt{q} + a_3\sqrt{pq} = \sqrt{q}(a_2 + a_3\sqrt{p}).$$

Elevando al cuadrado,  $q - 1 = q(a_2^2 + a_3^2p + 2a_2a_3\sqrt{p})$ . Esto implica  $a_2a_3 = 0$  ya que  $\{1, \sqrt{p}\}$  son  $\mathbb{Q}$ -linealmente independientes, luego bien  $a_2 = 0$  o bien

$a_3 = 0$ . En ambos casos se llega a contradicción empleando los argumentos empleados en la demostración del Lema 1.1 (2). En consecuencia,

$$K \subsetneq K(\sqrt{q-1}) \subset \mathbb{Q}(\beta_{pq}) \quad \text{y} \quad [\mathbb{Q}(\beta_{pq}) : K] = 2,$$

luego  $\mathbb{Q}(\beta_{pq}) = K(\sqrt{q-1})$ . En particular  $\beta_{pq} \in K(\sqrt{q-1})$  y existen  $a, b \in K$  tales que  $\beta_{pq} = a + b\sqrt{q-1}$ . Elevando al cuadrado,

$$\beta_{pq}^2 = a^2 + (q-1)b^2 + 2ab\sqrt{q-1},$$

y esto implica  $ab = 0$  porque  $\beta_{pq}^2 \in K$  y  $\sqrt{q-1} \notin K$ . Si  $b = 0$  entonces  $\beta_{pq} = a \in K$ , lo que es falso pues  $[K : \mathbb{Q}] = 4$  y  $[\mathbb{Q}(\beta_{pq}) : \mathbb{Q}] = 8$ . Por tanto  $a = 0$ , es decir,  $\beta_{pq} = b\sqrt{q-1}$ . Como  $b \in K$  existen  $b_0, b_1, b_2, b_3 \in \mathbb{Q}$  tales que

$$b = b_0 + b_1\sqrt{p} + b_2\sqrt{q} + b_3\sqrt{pq}.$$

Calculamos las imágenes de los dos miembros de la igualdad  $\beta_{pq} = b\sqrt{q-1}$  vía  $\tau$ . Resulta

$$\beta_2 = \tau(\beta_{pq}) = \tau(b)\tau(\sqrt{q-1}) = -(b_0 + b_1\sqrt{p} - b_2\sqrt{q} - b_3\sqrt{pq})\sqrt{q-1}.$$

Empleando la igualdad (7) se tiene

$$\begin{aligned} (p + \sqrt{p})\sqrt{q}\sqrt{q-1} &= \beta_1\beta_2 = b\sqrt{q-1}\beta_2 \\ &= (1-q)(b_0 + b_1\sqrt{p} + b_2\sqrt{q} + b_3\sqrt{pq}) \cdot (b_0 + b_1\sqrt{p} - b_2\sqrt{q} - b_3\sqrt{pq}) \in K, \end{aligned}$$

luego  $(p + \sqrt{p})\sqrt{q}\sqrt{q-1} \in K$ , y esto es falso porque  $(p + \sqrt{p})\sqrt{q} \in K$  y hemos probado que  $\sqrt{q-1} \notin K$ . Hemos demostrado así que  $\text{Gal}(\mathbb{Q}(\beta_{pq})|\mathbb{Q})$  no es isomorfo a  $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$  como pretendíamos.

La segunda parte es consecuencia de lo que acabamos de probar y el Teorema fundamental de la Teoría de Galois, porque cada uno de los grupos  $\mathbb{Z}_4 \times \mathbb{Z}_2$ ,  $\mathcal{D}_4$  y  $\mathcal{Q}_8$  tiene, exactamente, tres subgrupos de orden 4.

(2) Supongamos, por reducción al absurdo, que  $q-1$  no es un cuadrado en  $\mathbb{Z}$ . Entonces  $\mathbb{Q}(\sqrt{q-1})|\mathbb{Q}$  es una subextensión de grado 2 de  $\mathbb{Q}(\beta_{pq})|\mathbb{Q}$  y, por el apartado (2) y el Lema 1.1 (2),  $\mathbb{Q}(\sqrt{q-1}) = \mathbb{Q}(\sqrt{p})$ . Esto implica, por el Lema 1.1 (1), que existen enteros coprimos  $x, y$  tales que  $\frac{p}{q-1} = \left(\frac{x}{y}\right)^2$ , esto

es,  $py^2 = (q-1)x^2$ . Entonces  $p$  divide a  $x$  ya que  $p > q > q-1$ . Sea  $z \in \mathbb{Z}$  tal que  $x = pz$ . Así,  $y^2 = p(q-1)z^2$  y  $p$  también divide a  $y$ , lo que es absurdo.

Veamos la segunda parte. Por ser la extensión  $\mathbb{Q}(\beta_{pq})|\mathbb{Q}$  de Galois el producto  $\beta_1\beta_3 \in \mathbb{Q}(\beta_{pq})$ . Pero

$$\beta_1\beta_3 = \sqrt{(q+\sqrt{q})(p+\sqrt{p})} \cdot \sqrt{(q+\sqrt{q})(p-\sqrt{p})} = (q+\sqrt{q})\sqrt{p}\sqrt{p-1} \quad (11)$$

y, como  $\sqrt{q}, \sqrt{p} \in K \subset \mathbb{Q}(\beta_{pq})$ , se deduce que  $\sqrt{p-1} \in \mathbb{Q}(\beta_{pq})$ . Por tanto, bien  $p-1$  es un cuadrado en  $\mathbb{Z}$  y hemos terminado, o bien  $\mathbb{Q}(\sqrt{p-1})|\mathbb{Q}$  es una subextensión de grado 2 de  $\mathbb{Q}(\beta_{pq})|\mathbb{Q}$ .

En tal caso  $\mathbb{Q}(\sqrt{p-1}) = \mathbb{Q}(\sqrt{q})$  en virtud del apartado (2) y el Lema 1.1 (2). Esto implica, por el Lema 1.1 (1), que existe  $r \in \mathbb{Q}$  tal que  $\frac{p-1}{q} = r^2$ , i.e.,  $p-1 = qr^2$ . Sin pérdida de generalidad,  $r > 0$ . Supongamos que  $q$  no divide a  $p-1$ . Entonces, existen enteros coprimos  $a$  y  $b$  tales que  $r := \frac{a}{b}$ , esto es,  $(p-1)b^2 = qa^2$ . Así,  $q$  divide a  $b$  y existe  $c \in \mathbb{Z}$  tal que  $b = cq$ , o sea,  $(p-1)c^2q = a^2$  y  $q$  también divide a  $a$ , que es una contradicción. Por ello,  $q$  divide a  $p-1$  y  $\frac{p-1}{q} \in \mathbb{Z}$  es el cuadrado de un número racional, luego es el cuadrado de un entero.  $\square$

**Lema 2.2** Sean  $q < p$  números primos tales que  $\mathbb{Q}(\beta_{pq})|\mathbb{Q}$  es extensión de Galois. Los automorfismos  $\sigma$  y  $\tau$  definidos en (5) tienen orden 4.

*Demostración.* Probemos que el orden  $o(\tau)$  de  $\tau$  es 4. Por el Lema 2.1 existe  $n \in \mathbb{Z}^+$  tal que  $q-1 = n^2$ . Como  $\tau(\sqrt{q}) = -\sqrt{q}$  y  $\tau(\sqrt{p}) = \sqrt{p}$  obtenemos

$$\tau^2(\beta_{pq}) = \tau\left(\frac{n(p+\sqrt{p})\sqrt{q}}{\beta_{pq}}\right) = \frac{-n(p+\sqrt{p})\sqrt{q}}{n(p+\sqrt{p})\sqrt{q}} \cdot \beta_{pq} = -\beta_{pq},$$

lo que prueba que  $o(\tau) = 4$ . La prueba de que  $\sigma$  tiene orden 4 es análoga empleando ahora la igualdad (11), por lo que la omitimos.  $\square$

**Teorema 2.3** Sean  $q < p$  números primos tales que  $\mathbb{Q}(\beta_{pq})|\mathbb{Q}$  es extensión de Galois. Sean  $\sigma, \tau$  los automorfismos de  $\mathbb{Q}(\beta_{pq})|\mathbb{Q}$  definidos en (5).

- (1) Si  $p-1$  es un cuadrado en  $\mathbb{Z}$ , entonces  $\sigma\tau = \tau\sigma$  y  $\langle\tau\rangle \neq \langle\sigma\rangle$ .
- (2) Si existe  $r \in \mathbb{Z}^+$  tal que  $p-1 = qr^2$ , entonces  $\sigma\tau \neq \tau\sigma$ .

*Demostración.* Sin pérdida de generalidad podemos suponer que  $\sigma(\beta_{pq}) = \beta_3$ .

(1) Sea  $m \in \mathbb{Z}^+$  tal que  $\sqrt{p-1} = m$ . Para la primera afirmación basta comprobar que  $\sigma\tau(\beta_{pq}) = \tau\sigma(\beta_{pq})$ . Se tiene,

$$\begin{aligned}\sigma\tau(\beta_{pq}) &= \tau(\sigma(\beta_{pq})) = \tau\left(\frac{m(q + \sqrt{q})\sqrt{p}}{\beta_{pq}}\right) \\ &= \frac{m(q - \sqrt{q})\sqrt{p}}{\tau(\beta_{pq})} = \frac{m(q - \sqrt{q})\sqrt{p}}{n(p + \sqrt{p})\sqrt{q}} \cdot \beta_{pq},\end{aligned}$$

mientras que

$$\begin{aligned}\tau\sigma(\beta_{pq}) &= \sigma(\tau(\beta_{pq})) = \sigma\left(\frac{n(p + \sqrt{p})\sqrt{q}}{\beta_{pq}}\right) \\ &= \frac{n(p - \sqrt{p})\sqrt{q}}{\sigma(\beta_{pq})} = \frac{n(p - \sqrt{p})\sqrt{q}}{m(q + \sqrt{q})\sqrt{p}} \cdot \beta_{pq}.\end{aligned}$$

Dividiendo,

$$\begin{aligned}\frac{\sigma\tau(\beta_{pq})}{\tau\sigma(\beta_{pq})} &= \frac{m(q - \sqrt{q})\sqrt{p}}{n(p + \sqrt{p})\sqrt{q}} \cdot \frac{n(p - \sqrt{p})\sqrt{q}}{m(q + \sqrt{q})\sqrt{p}} \\ &= \frac{m^2(q^2 - q)p}{n^2(p^2 - p)q} = \frac{(p-1)(q^2 - q)p}{(q-1)(p^2 - p)q} = 1,\end{aligned}$$

luego  $\sigma\tau(\beta_{pq}) = \tau\sigma(\beta_{pq})$ .

Para demostrar que  $\langle \tau \rangle \neq \langle \sigma \rangle$  basta comprobar que  $\tau^3 \neq \sigma$ . Ahora bien,

$$\tau^3(\beta_{pq}) = -\tau(\beta_{pq}) = -\beta_2 < 0 < \beta_3 = \sigma(\beta_{pq}).$$

(2) Ahora probaremos que  $\sigma\tau(\beta_{pq}) \neq \tau\sigma(\beta_{pq})$ . Por un lado,

$$\begin{aligned}\sigma\tau(\beta_{pq}) &= \tau(\sigma(\beta_{pq})) = \tau\left(\frac{r(q + \sqrt{q})\sqrt{p}\sqrt{q}}{\beta_{pq}}\right) = \frac{-r(q - \sqrt{q})\sqrt{p}\sqrt{q}}{\tau(\beta_{pq})} \\ &= \frac{-r(q - \sqrt{q})\sqrt{p}\sqrt{q}}{n(p + \sqrt{p})\sqrt{q}} \cdot \beta_{pq} = \frac{-r(q - \sqrt{q})\sqrt{p}}{n(p + \sqrt{p})} \cdot \beta_{pq},\end{aligned}$$

mientras que

$$\begin{aligned}\tau\sigma(\beta_{pq}) &= \sigma(\tau(\beta_{pq})) = \sigma\left(\frac{n(p + \sqrt{p})\sqrt{q}}{\beta_{pq}}\right) = \frac{n(p - \sqrt{p})\sqrt{q}}{\sigma(\beta_{pq})} \\ &= \frac{n(p - \sqrt{p})\sqrt{q}}{r(q + \sqrt{q})\sqrt{p}\sqrt{q}} \cdot \beta_{pq} = \frac{n(p - \sqrt{p})}{r(q + \sqrt{q})\sqrt{p}} \cdot \beta_{pq},\end{aligned}$$

luego

$$\frac{\sigma\tau(\beta_{pq})}{\tau\sigma(\beta_{pq})} = -\frac{r^2p(q^2 - q)}{n^2p(p - 1)} = -\frac{r^2q(q - 1)}{n^2(p - 1)} = -\frac{r^2q}{p - 1} = -1,$$

lo que prueba que  $\tau\sigma(\beta_{pq}) \neq \sigma\tau(\beta_{pq})$ .  $\square$

**Corolario 2.4** Sean  $q < p$  números primos tales que  $\mathbb{Q}(\beta_{pq})|\mathbb{Q}$  es una extensión de Galois.

- (1) Si  $p - 1$  es un cuadrado en  $\mathbb{Z}$ , entonces  $\text{Gal}(\mathbb{Q}(\beta_{pq})|\mathbb{Q}) \simeq \mathbb{Z}_4 \times \mathbb{Z}_2$ .
- (2) Si existe  $r \in \mathbb{Z}^+$  tal que  $p - 1 = qr^2$ , entonces  $\text{Gal}(\mathbb{Q}(\beta_{pq})|\mathbb{Q}) \simeq \mathcal{Q}_8$ .

*Demostración.* (1) Por el Lema 2.2 el grupo de Galois  $\text{Gal}(\mathbb{Q}(\beta_{pq})|\mathbb{Q})$  contiene elementos  $\sigma$  y  $\tau$ , ambos de orden 4, tales que  $\langle \tau \rangle \neq \langle \sigma \rangle$  y  $\sigma\tau = \tau\sigma$ . Ni el grupo diedral  $\mathcal{D}_4$  ni el cuaternión  $\mathcal{Q}_8$  tienen elementos que satisfacen estas condiciones luego  $\text{Gal}(\mathbb{Q}(\beta_{pq})|\mathbb{Q}) \simeq \mathbb{Z}_4 \times \mathbb{Z}_2$  en virtud del Lema 2.1 (2).

(2) Hemos visto en el Lema 2.2 que  $\text{Gal}(\mathbb{Q}(\beta_{pq})|\mathbb{Q})$ , que es un grupo de orden 8, contiene dos elementos de orden 4 que no conmutan, de lo que se deduce que  $\text{Gal}(\mathbb{Q}(\beta_{pq})|\mathbb{Q}) \simeq \mathcal{Q}_8$ .  $\square$

### 3. ¿Cuándo es $\mathbb{Q}(\beta_{pq})|\mathbb{Q}$ una extensión de Galois?

En esta sección encontramos condiciones suficientes para que la extensión  $\mathbb{Q}(\beta_{pq})|\mathbb{Q}$  sea de Galois.

**Teorema 3.1** Sean  $q < p$  números primos y supongamos que existe un entero positivo  $n$  tal que  $q - 1 = n^2$ .

- (1) Si  $p - 1$  es un cuadrado en  $\mathbb{Z}$ , entonces la extensión  $\mathbb{Q}(\beta_{pq})|\mathbb{Q}$  es de Galois.

(2) Si existe  $r \in \mathbb{Z}^+$  tal que  $p - 1 = qr^2$ , entonces la extensión  $\mathbb{Q}(\beta_{pq})|\mathbb{Q}$  es de Galois.

*Demostración.* (1) Por hipótesis existe  $m \in \mathbb{Z}^+$  tal que  $p - 1 = m^2$ . Entonces, empleando las igualdades (5),

$$\frac{(\tau(\beta_{pq}))^2}{\beta_{pq}^2} = \frac{\tau(\beta_{pq}^2)}{\beta_{pq}^2} = \frac{\tau(\alpha_{pq})}{\alpha_{pq}} = \left( \frac{\sqrt{q} - 1}{n} \right)^2.$$

Sea  $u := \frac{1}{n} \in \mathbb{Q}$ . Así,  $(\tau(\beta_{pq}))^2 = (u\beta_{pq}(\sqrt{q} - 1))^2$  luego existe  $\varepsilon_1 \in \{-1, +1\}$  tal que

$$\tau(\beta_{pq}) = \varepsilon_1 u \beta_{pq} (\sqrt{q} - 1). \quad (12)$$

Por tanto,

$$\begin{aligned} \tau^2(\beta_{pq}) &= \tau(\varepsilon_1 u \beta_{pq} (\sqrt{q} - 1)) = -\varepsilon_1 u \tau(\beta_{pq}) (\sqrt{q} + 1) \\ &= -\varepsilon_1^2 u^2 \beta_{pq} (\sqrt{q} + 1) (\sqrt{q} - 1) = -\beta_{pq}, \end{aligned}$$

así que  $o(\tau) = 4$ . Análogamente,

$$\frac{(\sigma(\beta_{pq}))^2}{\beta_{pq}^2} = \frac{\sigma(\beta_{pq}^2)}{\beta_{pq}^2} = \frac{\sigma(\alpha_{pq})}{\alpha_{pq}} = \left( \frac{1}{m} (1 - \sqrt{p}) \right)^2.$$

Entonces,

$$v := \frac{1}{m} (1 - \sqrt{p}) \in \mathbb{Q}(\sqrt{p}) \subset K$$

satisface  $(\sigma(\beta_{pq}))^2 = v^2 \beta_{pq}^2 = (v\beta_{pq})^2$ , así que  $\sigma(\beta_{pq}) = \varepsilon_2 v \beta_{pq}$  para cierto  $\varepsilon_2 \in \{-1, +1\}$ . Además,  $\sigma(v) = \frac{1}{m} (1 + \sqrt{p})$ , por lo que

$$\begin{aligned} \sigma^2(\beta_{pq}) &= \varepsilon_2 \sigma(v) \sigma(\beta_{pq}) = \varepsilon_2^2 \sigma(v) v \beta_{pq} \\ &= \sigma(v) v \beta_{pq} = \frac{1}{m} (1 + \sqrt{p}) \cdot \frac{1}{m} (1 - \sqrt{p}) \cdot \beta_{pq} = -\beta_{pq}, \end{aligned}$$

de lo que se sigue que  $o(\sigma) = 4$ . Supongamos por un momento que  $\tau \notin \langle \sigma \rangle$ . Entonces el grupo  $\text{Gal}(\mathbb{Q}(\beta_{pq})|\mathbb{Q})$  contiene estrictamente a su subgrupo  $\langle \sigma \rangle$ , que tiene orden 4, luego

$$8 \leq \text{ord}(\text{Gal}(\mathbb{Q}(\beta_{pq})|\mathbb{Q})) \leq [\mathbb{Q}(\beta_{pq}) : \mathbb{Q}] = 8.$$

Por tanto  $\text{ord}(\text{Gal}(\mathbb{Q}(\beta_{pq})|\mathbb{Q})) = [\mathbb{Q}(\beta_{pq}) : \mathbb{Q}] = 8$  y  $\mathbb{Q}(\beta_{pq})|\mathbb{Q}$  es una extensión de Galois de orden 8. Ahora bien,

$$\sigma(\beta_{pq}) = \varepsilon_2 v \beta_{pq}, \quad \sigma^2(\beta_{pq}) = -\beta_{pq} \quad \text{y} \quad \sigma^3(\beta_{pq}) = -\varepsilon_2 v \beta_{pq},$$

y ninguno de estos valores coincide con  $\tau(\beta_{pq}) = \varepsilon_1 u \beta_{pq}(\sqrt{q} - 1)$  puesto que  $\sqrt{q} \notin \mathbb{Q}(\sqrt{p})$ . Esto demuestra, como queríamos, que  $\tau \notin \langle \sigma \rangle$ .

(2) Ahora tenemos

$$\frac{(\sigma(\beta_{pq}))^2}{\beta_{pq}^2} = \frac{\sigma(\beta_{pq}^2)}{\beta_{pq}^2} = \frac{\sigma(\alpha_{pq})}{\alpha_{pq}} = \left( \frac{\sqrt{p}-1}{r\sqrt{q}} \right)^2.$$

Por ello existe  $\varepsilon_2 \in \{-1, +1\}$  tal que  $\sigma(\beta_{pq}) = \varepsilon_2 \left( \frac{\sqrt{p}-1}{r\sqrt{q}} \right) \beta_{pq}$ , luego

$$\begin{aligned} \sigma\tau(\beta_{pq}) &= \tau(\sigma(\beta_{pq})) = -\varepsilon_2 \left( \frac{\sqrt{p}-1}{r\sqrt{q}} \right) \tau(\beta_{pq}) \\ &= -\varepsilon_1 \varepsilon_2 u (\sqrt{q}-1) \left( \frac{\sqrt{p}-1}{r\sqrt{q}} \right) \beta_{pq}. \end{aligned}$$

Por otro lado,

$$\begin{aligned} \tau\sigma(\beta_{pq}) &= \sigma(\tau(\beta_{pq})) = \sigma(\varepsilon_1 u \beta_{pq}(\sqrt{q}-1)) \\ &= \varepsilon_1 \varepsilon_2 u (\sqrt{q}-1) \left( \frac{\sqrt{p}-1}{r\sqrt{q}} \right) \beta_{pq} = -\sigma\tau(\beta_{pq}). \end{aligned}$$

En consecuencia,  $\sigma\tau(\beta_{pq}) \neq \tau\sigma(\beta_{pq})$  luego  $\sigma \in \text{Gal}(\mathbb{Q}(\beta_{pq})|\mathbb{Q}) \setminus \langle \tau \rangle$ . Como  $\text{ord}(\text{Gal}(\mathbb{Q}(\beta_{pq})|\mathbb{Q})) \leq [\mathbb{Q}(\beta_{pq}) : \mathbb{Q}] = 8$  se concluye que

$$\text{ord}(\text{Gal}(\mathbb{Q}(\beta_{pq})|\mathbb{Q})) = 8 = [\mathbb{Q}(\beta_{pq}) : \mathbb{Q}],$$

por lo que  $\mathbb{Q}(\beta_{pq})|\mathbb{Q}$  es una extensión de Galois.  $\square$

**Ejemplos 3.2** (1) Sea  $\beta := \sqrt{(2 + \sqrt{2})(5 + \sqrt{5})}$ . En virtud del Teorema 3.1  $\mathbb{Q}(\beta)|\mathbb{Q}$  es una extensión de Galois y por el Corolario 2.4 su grupo de Galois es isomorfo a  $\mathbb{Z}_4 \times \mathbb{Z}_2$ .

(2) Sea  $\beta := \sqrt{(5 + \sqrt{5})(181 + \sqrt{181})}$ . En virtud del Teorema 3.1  $\mathbb{Q}(\beta)|\mathbb{Q}$  es una extensión de Galois y por el Corolario 2.4 su grupo de Galois es isomorfo a  $\mathcal{Q}_8$ .

**Observación 3.3** Sean  $q < p$  números primos tales que  $q - 1$  es el cuadrado de un número entero y ni  $p - 1$  ni  $\frac{p-1}{q}$  son cuadrados de números enteros. Hemos demostrado en el Lema 2.1 que en este caso la extensión  $\mathbb{Q}(\beta_{pq})|\mathbb{Q}$  no es de Galois. Buscamos un conjunto finito de generadores de la clausura de Galois  $\widehat{\mathbb{Q}(\beta_{pq})}$  de  $\mathbb{Q}(\beta_{pq})$  sobre  $\mathbb{Q}$ , es decir, la menor extensión de Galois sobre  $\mathbb{Q}$  que contiene a  $\mathbb{Q}(\beta_{pq})$ . En (6) hemos calculado las raíces del polinomio mínimo de  $\beta_{pq}$  sobre  $\mathbb{Q}$ . Es claro que

$$\widehat{\mathbb{Q}(\beta_{pq})} = \mathbb{Q}(\beta_{pq}, \beta_2, \beta_3, \beta_4) = \mathbb{Q}(\beta_{pq}, \beta_{pq}\beta_2, \beta_{pq}\beta_3, \beta_{pq}\beta_4).$$

Se desprende de (7) y (11) y de la igualdad

$$\beta_{pq}\beta_4 = \sqrt{(q + \sqrt{q})(p + \sqrt{p})} \sqrt{(q - \sqrt{q})(p - \sqrt{p})} = \sqrt{q}\sqrt{q-1}\sqrt{p}\sqrt{p-1}$$

que  $\widehat{\mathbb{Q}(\beta_{pq})} = \mathbb{Q}(\beta_{pq}, \sqrt{p-1})$  porque  $q - 1$  es un cuadrado en  $\mathbb{Z}$ . Además  $\sqrt{p-1} \notin \mathbb{Q}(\beta_{pq})$ . En particular,

$$[\widehat{\mathbb{Q}(\beta_{pq})} : \mathbb{Q}(\beta_{pq})] = 2 \quad \text{por lo que} \quad [\widehat{\mathbb{Q}(\beta_{pq})} : \mathbb{Q}] = 16.$$

Como la subextensión  $\mathbb{Q}(\beta_{pq})|\mathbb{Q}$  de  $\widehat{\mathbb{Q}(\beta)}|\mathbb{Q}$  no es de Galois se deduce del Teorema fundamental de la Teoría de Galois que el grupo  $\text{Gal}(\widehat{\mathbb{Q}(\beta)}|\mathbb{Q})$  no es abeliano. Describimos a continuación su estructura, para lo que emplearemos el cuerpo intermedio  $K := \mathbb{Q}(\sqrt{q}, \sqrt{p})$ . Como la extensión  $K|\mathbb{Q}$  es de Galois, se tiene una sucesión exacta corta escindida (para la noción de sucesión exacta corta escindida véase el Ejercicio II. 30 de [3])

$$0 \rightarrow \text{Gal}(\widehat{\mathbb{Q}(\beta_{pq})}|K) \xrightarrow{j} \text{Gal}(\widehat{\mathbb{Q}(\beta_{pq})}|\mathbb{Q}) \xrightarrow{\rho} \text{Gal}(K|\mathbb{Q}) \rightarrow 0,$$

donde  $j$  es la inclusión y  $\rho(\psi) = \psi|_K$  para todo  $\psi \in G(\widehat{\mathbb{Q}(\beta_{pq})}|\mathbb{Q})$ . Para comprobar que es escindida recordemos la igualdad (1) y observemos que

$$\varphi_{ij} \cdot \varphi_{kl} = \varphi_{i+k, j+l} \quad \text{para todo} \quad i, j, k, l \in \{0, 1\}.$$

Entonces, una sección  $s : \text{Gal}(K|\mathbb{Q}) \rightarrow \text{Gal}(\widehat{\mathbb{Q}(\beta_{pq})}|\mathbb{Q})$  de  $\rho$  es la definida por

$$s(\varphi_{ij})(\beta_{pq}) := \sqrt{\varphi_{ij}(\alpha_{pq})} \quad \text{y} \quad s(\varphi_{ij})(\sqrt{p-1}) := \sqrt{p-1}.$$

En consecuencia,  $\text{Gal}(\widehat{\mathbb{Q}(\beta_{pq})}|\mathbb{Q})$  es un producto semidirecto

$$\text{Gal}(\widehat{\mathbb{Q}(\beta_{pq})}|\mathbb{Q}) \simeq \text{Gal}(\widehat{\mathbb{Q}(\beta_{pq})}|K) \rtimes \text{Gal}(K|\mathbb{Q}).$$

Por el Lema 1.3,  $\text{Gal}(K|\mathbb{Q}) \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$ . Además  $\phi(\alpha_{pq}) = \alpha_{pq}$ , para todo  $\phi \in G(\widehat{\mathbb{Q}(\beta_{pq})}|K)$ . Entonces,  $\phi(\beta_{pq}) = \pm\beta_{pq}$  y como  $\phi(\sqrt{p-1}) = \pm\sqrt{p-1}$  se tiene  $\text{Gal}(\widehat{\mathbb{Q}(\beta_{pq})}|K) \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$ . Por tanto,

$$\text{Gal}(\widehat{\mathbb{Q}(\beta_{pq})}|\mathbb{Q}) \simeq (\mathbb{Z}_2 \times \mathbb{Z}_2) \rtimes (\mathbb{Z}_2 \times \mathbb{Z}_2).$$

Para terminar comprobemos que, salvo isomorfismo, existe un único producto semidirecto de  $V := \mathbb{Z}_2 \times \mathbb{Z}_2$  por sí mismo. Los elementos  $\mathbf{e}_1 := (1+2\mathbb{Z}, 0+2\mathbb{Z})$  y  $\mathbf{e}_2 := (0+2\mathbb{Z}, 1+2\mathbb{Z})$  generan  $V$ , luego todo automorfismo  $\psi$  de  $V$  está determinado por las imágenes  $\psi(\mathbf{e}_1)$  y  $\psi(\mathbf{e}_2)$ , que han de ser vectores linealmente independientes del  $\mathbb{Z}_2$ -espacio vectorial  $V$ . En consecuencia,  $|\text{Aut}(V)| = 3 \cdot 2 = 6$ . El grupo de automorfismos de  $V$  no es abeliano. De hecho, los automorfismos  $\psi_1$  y  $\psi_2$  de  $V$  definidos por

$$\psi_1(\mathbf{e}_1) = \mathbf{e}_2, \quad \psi_1(\mathbf{e}_2) = \mathbf{e}_1, \quad \psi_2(\mathbf{e}_1) = \mathbf{e}_1 + \mathbf{e}_2 \quad \text{y} \quad \psi_2(\mathbf{e}_2) = \mathbf{e}_2$$

no conmutan porque

$$\begin{aligned} (\psi_1\psi_2)(\mathbf{e}_1) &= \psi_2(\psi_1(\mathbf{e}_1)) = \psi_2(\mathbf{e}_2) = \mathbf{e}_2 \quad \text{y} \\ (\psi_2\psi_1)(\mathbf{e}_1) &= \psi_1(\psi_2(\mathbf{e}_1)) = \psi_1(\mathbf{e}_1 + \mathbf{e}_2) = \mathbf{e}_1 + \mathbf{e}_2. \end{aligned}$$

Como  $\mathbb{Z}_6$  y el grupo simétrico  $\mathcal{S}_3$  son los únicos grupos de orden 6, véase [3, Cor. IV.2.2], se deduce que  $\text{Aut}(V) \simeq \mathcal{S}_3$ , y la estructura del producto semidirecto  $V \rtimes V$  está dada por un homomorfismo no trivial  $\Psi : V \rightarrow \mathcal{S}_3$ , que no es inyectivo porque  $\text{ord}(V) = 4$  no divide a  $6 = \text{ord}(\mathcal{S}_3)$ . Por tanto podemos suponer que  $\Psi(\mathbf{e}_1) = \text{id}$ , mientras que  $\Psi(\mathbf{e}_2)$  debe ser una de las tres transposiciones de  $\mathcal{S}_3$ , lo que determina  $\Psi$ , y con ello  $V \rtimes V$ , salvo isomorfismo.

**Question 3.4** A lo largo de todo el trabajo hemos fijado dos números primos  $q < p$  de modo que  $q - 1$  es el cuadrado de un número entero. Si se suprime esta hipótesis el grado de la clausura de Galois  $\widehat{\mathbb{Q}(\beta_{pq})}$  de  $\mathbb{Q}(\beta_{pq})$  sobre  $\mathbb{Q}$  es 16 o 32, respectivamente, según que bien  $p - 1$  o  $(p - 1)/q$  sea el cuadrado de un entero, o no lo sea ninguno de los dos. Es un reto, que actualmente no sabemos abordar, determinar en este caso la estructura del grupo de Galois  $\text{Gal}(\widehat{\mathbb{Q}(\beta_{pq})}|\mathbb{Q})$ .

**Agradecimientos 3.5** Expresamos nuestro agradecimiento a los referees, quienes detectaron un error en el enunciado original del Lema 1.1 (2) y cuyas propuestas han contribuido muy sustancialmente a reestructurar la presentación de los resultados, evitando además repeticiones innecesarias en algunos de los argumentos empleados. Uno de los referees ha propuesto la Cuestión 3.4, a la que intentaremos dar respuesta en próximos trabajos.

## Referencias

- [1] R. Dedekind (1931): Konstruktion von Quaternionkörpern. *Gesammelte mathematische, Werke* Band **2**, 376-384.
- [2] J.F. Fernando, J.M. Gamboa (2017), *Ecuaciones Algebraicas; extensiones de cuerpos y teoría de Galois*. Editorial Sanz y Torres. Segunda edición.
- [3] J.F. Fernando, J.M. Gamboa (2017), *Estructuras Algebraicas: Teoría Elemental de Grupos*. Editorial Sanz y Torres. Segunda edición.
- [4] J.F. Fernando, J.M. Gamboa (2017), *Estructuras Algebraicas: Divisibilidad en anillos conmutativos*. Editorial Sanz y Torres. Segunda edición.
- [5] G. Fujisaki (1990), An elementary construction of Galois Quaternion extension. *Proc. Japan Acad. Math* **66**, Ser. A, 80-83.
- [6] G.H. Hardy, J.E. Littlewood (1923), Some problems of “Partitio numerorum” III: On the expression of a number as a sum of primes. *Acta Math* **44**, 1, 1-70.
- [7] C.U. Jensen, A. Ledet, N. Yui (2002), Generic polynomials: Constructive aspects of the inverse Galois Problem. Math. Sci. Res. Inst. Publ. **45**. Cambridge Univ. Press **167**, x+258 pp.
- [8] P.J. Morandi (1996), *Field and Galois Theory* . Graduate Texts in Mathematics **167**, Springer, New York.
- [9] I. Stewart (1990), *Galois Theory*. Second edition. Chapman & Hall/CRC Mathematics. Chapman & Hall/CRC, Boca Raton, FL.

# Kepler and the Rhombic Dodecahedron

## Kepler y el dodecaedro rómbico

Roberto Cardil Ricol  
IES Alonso Quijano de Alcalá de Henares (Madrid)  
roberto.cardil@gmail.com  
www.matematicasvisuales.com

### Resumen

*The principal goal of this article is to study the polyhedron called the Rhombic Dodecahedron. The Rhombic Dodecahedron is a simple, beautiful and interesting polyhedron that can delight young and adults alike. Johannes Kepler discovered it and we are going to follow Kepler's wonderful mind in our travel exploring its properties in an historical context. Our main source will be Kepler's book 'The Six-Cornered Snowflake'. How the Rhombic Dodecahedron was conceived is fascinating because Kepler discovered it inspired in Nature, taking a deep look into how bees build their cells. To follow all these ideas is not easy without real mathematical models. A second objective of this article is to encourage readers to build their own polyhedra and to play with them. Building polyhedra is a relaxing activity and the results are appealing because of their beauty. But there is more: we learn mathematical properties of this bodies when we build, look and touch them.*

### Introducción

El dodecaedro rómbico es un poliedro sencillo y bonito. Tiene propiedades matemáticas muy interesantes. La historia de su descubrimiento es fascinante y nos permite hablar de su descubridor, Johannes Kepler, y situar el poliedro

en su contexto histórico. Por otro lado, veremos que Kepler encontró su inspiración en la observación de la Naturaleza. La Historia de las Matemáticas y el estudio de la Naturaleza se dan la mano en este poliedro. El desarrollo de estas ideas, en los apartados 1 y 2, constituye la primera parte de este artículo.

En la segunda parte se propone la construcción del dodecaedro rómbico y de la celda de las abejas. A pesar de su brevedad podemos verla como el núcleo del artículo. Una vez más se insiste en la conveniencia de realizar modelos matemáticos. Como es bien sabido, la construcción de poliedros nos ayuda a desarrollar la visión espacial y mejorar nuestra comprensión de problemas geométricos. Por otra parte, es una actividad relajante en la que interviene nuestra habilidad manual y el deseo de obtener un resultado limpio y perfecto (que requiere un poco de técnica). La belleza del resultado atrae a todo el mundo. Estos son motivos más que suficientes para construir figuras geométricas. Pero no nos olvidamos de lo que puede ser fundamental para un profesor o aficionado a las Matemáticas: a partir de la construcción obtendremos resultados matemáticos.

Si en muchas ocasiones es muy conveniente realizar construcciones geométricas, en otras resulta casi imprescindible. Dos ejemplos claros se nos presentan cuando queremos estudiar teselaciones del espacio o empaquetamiento de esferas: dibujos y fotografías se vuelven confusos e incluso las aplicaciones interactivas son clarificadoras solo para personas entrenadas y con buena visión espacial.

Esta propuesta ha sido puesta en práctica en repetidas ocasiones con alumnos y, en particular, en varias sesiones del Taller de Talento Matemático de Zaragoza. Siempre con buenos resultados. Vamos sobre seguro. Sobre el tema se ha realizado una exposición en el IES Alonso Quijano de Alcalá de Henares en la que se han explorado varias técnicas de construcción, en particular, el uso de la impresión 3d para la realización de grandes estructuras.

El artículo se cierra con un repaso rápido a otros tres puntos de vista sobre el dodecaedro rómbico que son distintos y complementarios. Nos mostrarán la creatividad de Kepler y su relación, por un lado, con unos problemas sencillos pero, por otro, también ideas profundas que han resultado ser muy fértiles para las Matemáticas.

# 1. Kepler y su tiempo

Johannes Kepler (1571-1630) fue un científico, matemático, astrónomo y astrólogo alemán.

Podemos decir que la época en la que vivió Kepler es heredera de la explosión intelectual del Renacimiento y precursora de los revolucionarios descubrimientos de Newton y Leibniz.

A partir del siglo XVI y favorecido por la invención de la imprenta, se difunden y estudian seriamente las grandes obras maestras de los matemáticos griegos, como los Elementos de Euclides, las Cónicas de Apolonio y los trabajos de Arquímedes. La Geometría interesó tanto a científicos como a artistas y artesanos.

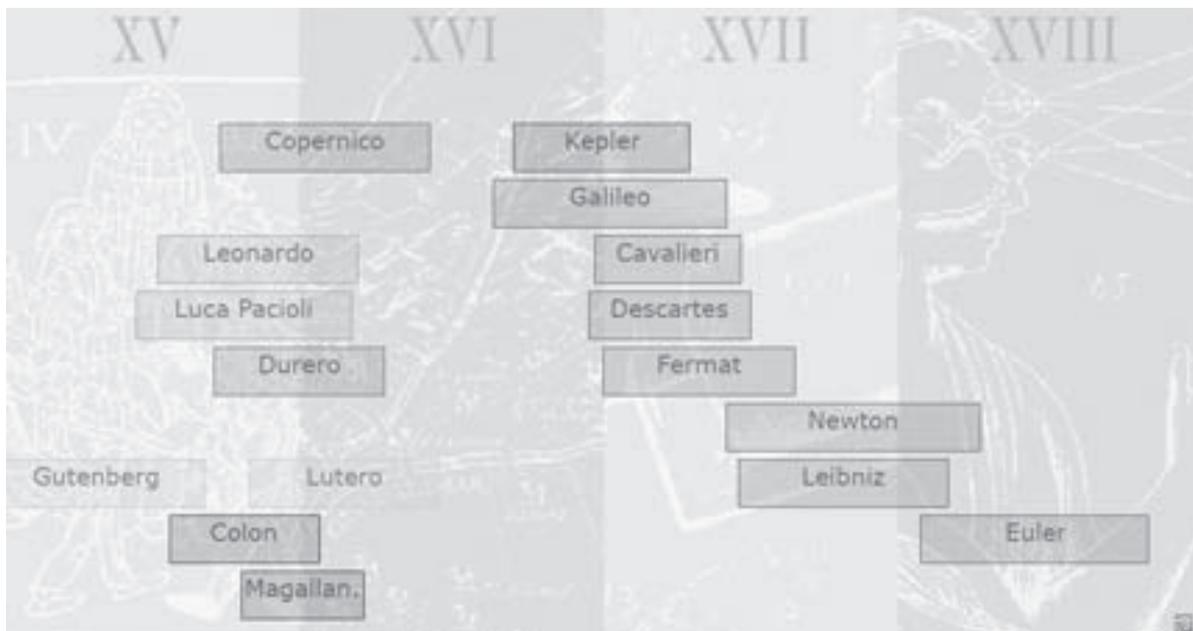


Figura 1: *Kepler y su tiempo.*

Una de las más importantes nuevas ideas que influyeron en Kepler fue la cosmología heliocéntrica de Copérnico. La publicación del libro de Copérnico ‘The Revolutionibus’ en 1543 inicia lo que llamamos la Revolución Copernicana. Sus observaciones le llevan a apoyar la idea de que la Tierra y todos los planetas giran en torno al Sol. En particular, la Tierra ya no era el centro estático del Universo. Desde su juventud, Kepler fue un defensor del modelo heliocéntrico de Copérnico.

Johannes Kepler nació en la ciudad alemana de Weil der Stadt in 1571. Su familia era pobre. Él fue un chico inteligente y de salud delicada.

Su vida no fue fácil, no gozó de buena salud, casi siempre con problemas financieros y dificultades familiares. Tuvo que cambiar de residencia varias veces: estudió en la Universidad de Tübingen, fue profesor de Matemáticas en Graz, después trabajó para el famoso astrónomo Tycho Brahe en Praga, donde llegó a ser Matemático Imperial, luego vivió en Linz y en Sagan. Murió en Regensburg en 1630. Se vio afectado por conflictos religiosos (Kepler fue un hombre muy religioso) e incluso guerras (la Guerra de los Treinta años, que devastó Alemania, comenzó en 1618).

A pesar de todas estas circunstancias, Kepler fue capaz de hacer importantes contribuciones a la ciencia, en particular a la Astronomía, Matemáticas y Óptica.

Como astrónomo, Kepler es famoso por su descubrimiento de las tres leyes del movimiento de los planetas alrededor del Sol. Las conocemos como las Leyes de Kepler y, posteriormente, fueron deducidas por Newton.

Como matemático, Kepler descubrió dos nuevos poliedros regulares no convexos (pequeño dodecaedro estrellado y gran dodecaedro estrellado), dos nuevos poliedros rómbicos (el dodecaedro rómbico y el triacontaedro), trabajó en el problema del empaquetamiento óptimo de esferas (Conjetura de Kepler), se interesó por los logaritmos y estudió volúmenes de cuerpos de revolución.

Debido a sus contribuciones en el desarrollo del Cálculo y su interés en los poliedros podemos decir que Kepler fue un digno heredero de Arquímedes y precursor de los descubrimientos de Newton y Leibniz.

Kepler tenía mucha imaginación y exploraba los problemas desde puntos de vista diferentes. Era muy observador y una simple anécdota le llevaba a plantearse cuestiones profundas. Muchas veces nos describe el devenir de su pensamiento y nosotros tenemos la oportunidad de seguir los caminos que transita una mente genial guiada por sus conocimientos e intuición. Era buen escritor y hoy en día podemos leer partes de su obra con placer e instrucción.

Un primer ejemplo de una de estas anécdota le ocurrió en su segunda boda. Kepler se sorprendió al ver como el mercader del vino que se consumió en la ceremonia medía el volumen de un tonel, simplemente introduciendo una vara de madera por el agujero del tonel. Como no se quedó muy convencido se puso a estudiar cómo calcular volúmenes de cuerpos de revolución y escribió

un libro entero sobre este asunto (quizás la contribución más importante en este campo posterior a Arquímedes).

Otra anécdota está en el origen del pequeño y precioso libro que va a ser nuestra principal fuente para tratar el asunto del descubrimiento del dodecaedro rómbico.

El título de esta joya es ‘Strena seu de nive sexangula’ que se puede traducir por ‘Regalo de Año Nuevo. Sobre el copo de nieve hexagonal’. Fue escrito como regalo para su amigo y benefactor Matthew Wacker von Wackenfels. Kepler nos cuenta que iba pensando y paseando por el Puente de Carlos un día invernal en Praga...

*Por suerte se dio la feliz casualidad de que un poco de vapor de agua se condensó por el frío en forma de nieve, y sus copos cayeron aquí y allá sobre mi abrigo, todos con seis esquinas y emplumados radios. ¡Por Hércules, doy mi palabra, eso es una cosa más pequeña que cualquier gota y que sin embargo posee estructura! Había encontrado el regalo ideal de año nuevo para el devoto de nada, la cosa digna que puede ofrecer un matemático, que no tiene nada y no recibe nada, ya que los copos de nieve bajan del cielo y se asemejan a las estrellas. [Kepler. *De Nive Sexangula*, traducción castellana y notas de Ana García Azcárate y Ángel Requena Fraile, p. 8][1].*

A lo largo del libro intentará explicar la forma hexagonal de los cristales de nieve pero su imaginación volará desde los panales de las abejas a los guisantes, de las semillas de la granada a las balas de cañón y, en el medio de sus pensamientos, nos va a explicar cómo descubre un nuevo poliedro, el dodecaedro rómbico.

Vamos a seguir los pensamientos de Kepler sobre este poliedro y cómo su intuición le lleva a descubrirlo en la base de las celdas de las abejas.

## **2. Los panales de las abejas y el descubrimiento del dodecaedro rómbico**

El primer matemático del que tenemos noticia que se interesó por este tema fue Pappus de Alejandría (alrededor del año 320 de nuestra era). En sus ‘Colecciones Matemáticas’, Pappus consideró cómo las abejas construyen sus panales, con la forma hexagonal de las celdas, y escribió:

... antes de recolectar el nectar de las flores más bonitas que crecen en la tierra, hacen para él, para la recepción de la miel, los recipientes que llamamos panales (con sus celdas) todas iguales, semejantes y contiguas unas a otras, y de forma hexagonal. Y podemos inferir que esto lo han logrado en virtud de una cierta previsión geométrica. Deben pensar por fuerza que las figuras deben de ser contiguas unas a otras, es decir, que tengan sus lados en común, de modo que ninguna materia extraña pueda entrar en los intersticios entre ellas y manchar la pureza de su producto. Sólo tres figuras geométricas satisfacen la condición, y me refiero solo a figuras regulares que sean equiláteras y equiángulas, porque las abejas no considerarían figuras que no fueran uniformes... Habiendo entonces tres figuras capaces por ellas mismas de llenar el espacio en torno al mismo punto [desde luego, se refiere al triángulo, cuadrado y hexágono], las abejas, debido a su sabiduría instintiva, eligen para la construcción de su colmena la figura que tiene más ángulos porque ellas conciben que contendrá más miel que cualquiera de las otras dos.[2].

En este famoso y precioso párrafo trata varios asuntos que no son nada sencillos. Y no me refiero a si las abejas son inteligentes o no, sino a los problemas de optimización que plantea.

Nosotros nos vamos a quedar con lo más básico, que es el tema de las teselaciones planas o mosaicos. Es un tema con muchas posibilidades. Las más sencillas son las formadas por polígonos regulares iguales, de las que hay tres, formadas por triángulos, cuadrados y hexágonos.

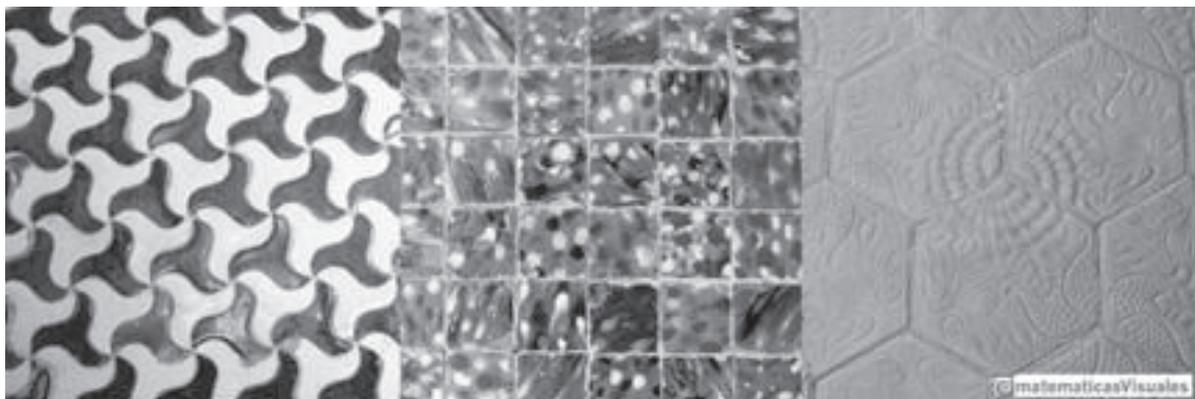


Figura 2: Tres ejemplos de teselaciones planas.

La imagen anterior es una aproximación artística a estas tres teselaciones regulares. Una basada en el triángulo equilátero (en la Alhambra de Grana-

da), la segunda se basa en la cuadrícula (los Reales Alcázares de Sevilla) y la tercera, basada en hexágonos, fue diseñada por el arquitecto Antoni Gaudí (Barcelona).

La misma idea pero aplicada en dimensión 3, es decir, las teselaciones del espacio, jugarán un papel importante en nuestro estudio del dodecaedro rómbico. Nos preguntamos ¿cómo podemos rellenar el espacio usando poliedros iguales? La cuestión no es nada sencilla pero tenemos, al menos, una respuesta clara y que nos resulta familiar: el cubo rellena el espacio. Un poco más en general podemos decir que con paralelepípedos iguales rellenamos el espacio. Pero aquí nos conviene destacar que el cubo es el único de los poliedros regulares que tiene esta propiedad.

El texto de Pappus es un buen ejemplo de la fascinación que la regularidad de los panales de las abejas ha ejercido en la Humanidad desde tiempo inmemorial. Hemos visto que la estructura hexagonal era bien conocida. Pero tienen que pasar más de mil doscientos años después de Pappus para que alguien se fije en cómo es el fondo de las celdas de las abejas, escriba sobre ello y saque interesantes conclusiones matemáticas. Ese genio fue Kepler.

Además, tenemos la suerte de que él mismo nos va contando cómo funciona su mente creativa en su librito 'De nive sexangula'. Leerlo es un placer y un auténtico regalo [1].

Sobre la estructura de los panales de las abejas, Kepler escribió:

*Si usted pregunta a los geómetras sobre la forma de los panales de las abejas, su respuesta será en forma de hexágono. La respuesta es obvia tras un mero vistazo a las aperturas o puertas, y a las paredes con los cuales están contruidos los alveolos. Cada celda esta rodeada por otras seis, y cada una comparte una pared medianera entre ella y la siguiente. Pero cuando usted examine el fondo de las celdas, verá que cada terminación está formada por tres planos en ángulo obtuso. Seis vértices forman este fondo (usted más bien podría llamarlo la quilla) cada una de las seis paredes de la celda terminan uniéndose, insertadas en un ángulo triedro, exactamente como el ángulo inferior de la quilla; los tres de más abajo en un ángulo con cuatro aristas [...] Las superficies planas de la quilla son siempre tres. Todas se parecen y con la forma que los geómetras llamamos rombo. Págs. 11-12 de [1].*

A partir de la observación de este maravilloso ejemplo tomado de la Naturaleza, Kepler descubre un poliedro formado por 12 caras rómbicas que

llamamos dodecaedro rómbico o rombododecaedro.

La siguiente ilustración se encuentra en otro libro de Kepler, ‘*Harmonice Mundi*’ (‘La armonía de los mundos’, publicado en 1619) y nos muestra claramente cómo Kepler concibe este poliedro:

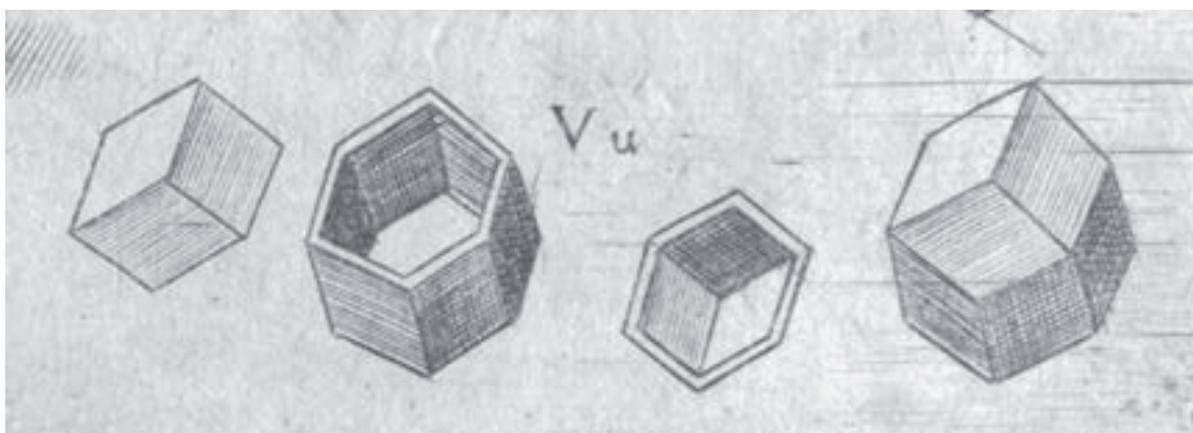


Figura 3: *Dibujo del dodecaedro rómbico en ‘Harmonice Mundi’.*

Seis rombos forman un ‘cinturón’. Nos podemos imaginar esos seis rombos sobre las paredes del prisma hexagonal de la celda. Añade tres rombos más de la misma manera que las abejas cierran sus celdas (lo que Kepler llama ‘la quilla’) y añade tres rombos más para cerrar el poliedro (las abejas no cierran la celda de este modo pues necesitan una entrada).

A partir de esta descripción del dodecaedro rómbico, ¿qué propiedades básicas podemos deducir y cuáles podemos intuir?

El dodecaedro rómbico tiene 12 caras que son rombos y 24 aristas. Los doce rombos son iguales.

Tiene 14 vértices de dos tipos distintos. En seis de ellos concurren cuatro aristas (donde los ángulos de los rombos son agudos) y en ocho vértices concurren tres aristas (los ángulos de los rombos son obtusos).

Seis rombos forman un cinturón. De hecho, el dodecaedro rómbico puede verse como formado por cuatro cinturones de seis rombos (cada rombo está en dos cinturones).

El ángulo diedro entre dos caras adyacentes de esos rombos que forman un cinturón hexagonal es de  $120^\circ$ . Puede probarse que el ángulo diedro entre dos caras adyacentes del poliedro es  $120^\circ$ .

Si imaginamos una capa de celda de las abejas y en cada celda colocamos

un dodecaedro rómbico lo que nos podemos imaginar es una capa infinita de dodecaedros rómbicos.

Pero sabemos que las abejas construyen sus panales en dos capas.

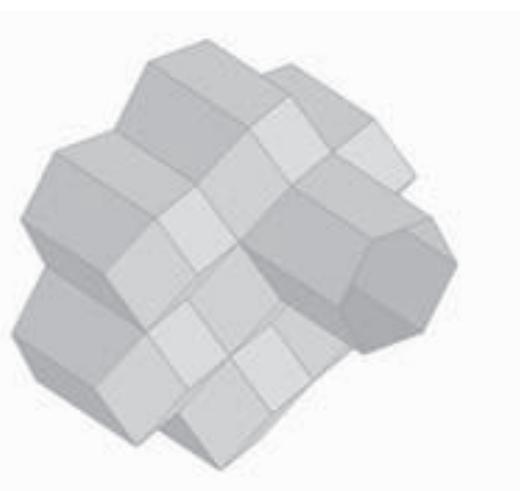


Figura 4: *Las abejas construyen dos capas de celdas.*

Kepler va más allá y saca una importante conclusión:

*Además debe anotarse que el orden de las celdas es doble. Uno abierto y el otro con las esquinas de cada quilla en una capa insertada entre las tres esquinas de las tres quillas de la segunda capa. La arquitectura es tal que cualquier celda comparte no sólo seis paredes con las seis celdas que lo rodean en la misma capa, sino también con las superficies planas de la base de las otras tres celdas de la capa contrapuesta. El resultado es que cada abeja tiene nueve vecinas, separadas de cada una y cualquier otra por una pared medianera en común.* Pág. 12 de [1].

Entonces podemos imaginar que en esta segunda capa ponemos también un dodecaedro rómbico en cada celda y no tendremos especial dificultad en imaginar que hacemos lo mismo en sucesivas capas.

Lo que Kepler está deduciendo es que el dodecaedro rómbico comparte con el cubo la sorprendente propiedad de teselar el espacio.

Y nosotros no podemos dejar de maravillarnos ante este ejemplo de imaginación y creación matemática a partir de la observación de la Naturaleza. Especialmente si intentamos hacer la prueba nosotros mismos y hemos tenido en las manos un panal de abejas natural. Lo que hace Kepler es, simplemente, genial.

Llegados a este punto, lo que procede es construir un modelo de este poliedro y de la celda de las abejas. Es lo que se propone en la siguiente sección.

### 3. Construcción de un dodecaedro rómbico y una celda de las abejas

Para disfrutar de este poliedro y comprender mejor sus interesantes propiedades es muy recomendable construir modelos.

Hay muchas maneras de construir este bonito poliedro (origami modular, con doce cartas de la baraja, etc.) pero aquí proponemos una muy sencilla que es una cajita con cartulina. Se trata de un modelo diseñado por John Jeremiah Edminster del poliedro y una variante que tiene la forma de una celda de las abejas. (Se reproducen con autorización del autor).

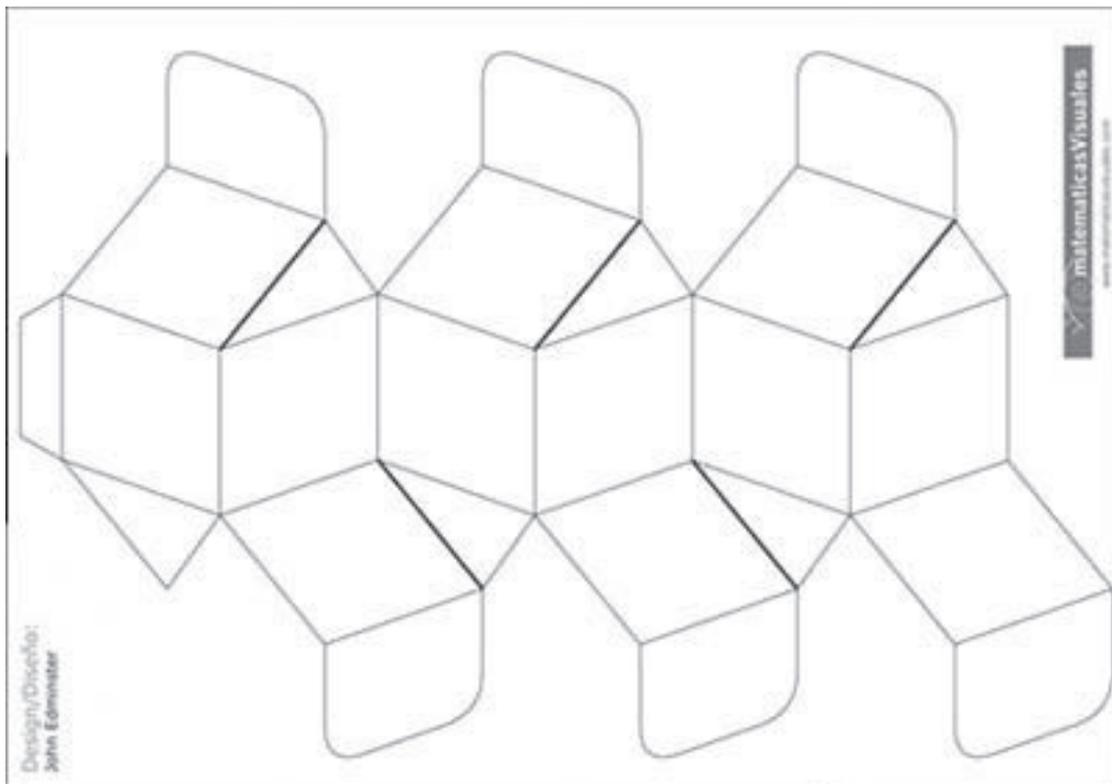


Figura 5: *Desarrollo del dodecaedro rómbico.*

Se pueden descargar los desarrollos de las figuras, imprimir, recortar y pe-

gar. Los modelos están en la página web complementaria a este artículo (<http://www.matematicasvisuales.com/html/geometria/construccionpoliedros/RDindice.html>).

Si construimos varios de estos modelos podemos explorar cómo las abejas contruyen sus panales, cómo encajan unos con otros en dos capas y las propiedades del dodecaedro rómbico, en particular, la de teselar el espacio.

Por mi experiencia puedo decir que un taller con el material expuesto hasta este punto es siempre un éxito: la actividad de las abejas es fascinante y el modelo para construir es sencillo, bonito e interesante.

## 4. ¿Qué más nos enseña Kepler sobre el dodecaedro rómbico?

La manera en la que Kepler nos muestra cómo ha descubierto el dodecaedro rómbico a partir de la observación de la Naturaleza es maravillosa, desde luego. Pero Kepler va a seguir investigando con su mente creativa este poliedro desde diferentes ángulos sorprendentes y cada uno de ellos nos aportará un punto de vista complementario y una mejor comprensión de esta figura.

Aquí solo podemos hacer un breve resumen de estos logros. El lector interesado disfrutará con ‘De Nive Sexangula’ [1]. Si se desea profundizar un poco en alguno de los aspectos que vamos a comentar se puede recurrir a la página complementaria de este artículo (<http://www.matematicasvisuales.com/html/geometria/construccionpoliedros/RDindice.html>).

### 4.1. Una figura conocida desde tiempo inmemorial

Un asunto que nos puede llamar la atención es por qué Kepler está interesado en el dodecaedro rómbico y en qué sentido podemos decir que es el descubridor de este poliedro. Resulta que esta forma era bien conocida desde tiempo inmemorial pues se encuentra en el mineral que llamamos granate.

El hecho de que este poliedro sea irregular (sus caras no son polígonos regulares y sus vértices son de dos tipos distintos) nos puede explicar el porqué este poliedro no ha sido descrito antes. Es mérito de Kepler el comprender su valor matemático. Kepler no solo está muy interesado en los sólidos platónicos (en particular, para su modelo cosmológico) y en los sólidos arquimedia-

nos, sino que también descubre dos nuevos poliedros regulares estrellados y comprende que junto al dodecaedro hay otros dos poliedros rómbicos relacionados. En su estudio de los poliedros podemos decir que es un digno sucesor de Arquímedes.



Figura 6: *Granate.*

#### 4.2. Un problema aplicado: el empaquetamiento de esferas

Si seguimos leyendo ‘De Nive Sexangula’ veremos que, sin aparente conexión, Kepler se interesa por los granos de la granada pues se fija en que al crecer en un espacio limitado los granos se comprimen y adoptan formas poliédricas. Esto le lleva a lo que podemos considerar el segundo punto de vista de Kepler sobre el dodecaedro rómbico. Se trata de su conexión con un problema relacionado con la Tecnología. Kepler trata el empaquetamiento óptimo de balas de cañón y plantea una hipótesis que llamamos Conjetura de Kepler. ¿Qué relación tiene este tema con el dodecaedro rómbico? Kepler se imagina que las balas de cañón se pueden comprimir y el resultado es nuestro poliedro.

Conviene destacar aquí que estamos ante un ejemplo excelente de cómo la manipulación de un modelo nos ayuda a comprender un problema matemático. Si preparamos trece bolas de arcilla podemos colocar doce de ellas rodeando una central y enseguida vemos que hay dos maneras distintas de

hacer esto. Al comprimir una de estas configuraciones obtendremos el dodecaedro rómbico. ¿Qué ocurrirá con la otra?

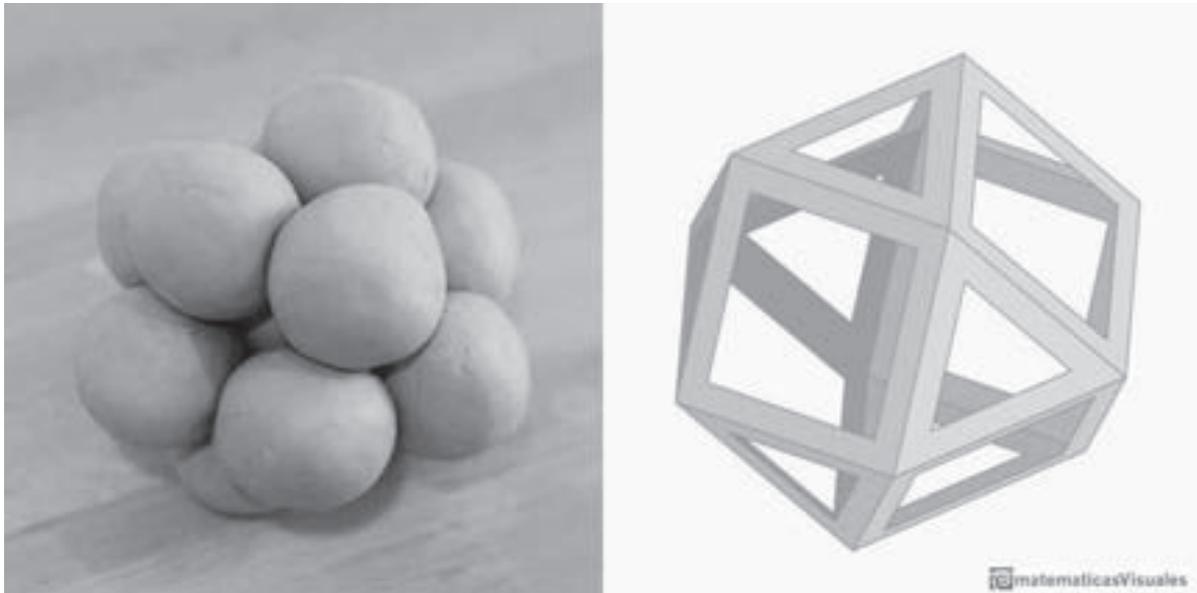


Figura 7: *Empaquetamiento de esferas y cuboctaedro.*

Esta configuración nos muestra también que hay una relación entre nuestro poliedro y el cuboctaedro. El cuboctaedro es un sólido arquimediano. Resulta que ambos poliedros son duales y, por lo tanto, el dodecaedro rómbico es un sólido de Catalan.

Este asunto tiene mucho interés para las Matemáticas. También está relacionado con el estudio de la estructura de la materia (Cristalografía, Química).

#### **4.3. Los artistas del Renacimiento: Un cubo con pirámides**

Esta conexión entre la observación de la Naturaleza y un problema de tipo técnico nos muestra la imaginación y genialidad de Kepler. Pero seguimos sin conocer muchas propiedades de este poliedro. De hecho todavía no conocemos sus dimensiones, la forma de sus caras, su volumen. Todavía nos sabemos dibujar su desarrollo. ¿Hay alguna manera más sencilla de ver el dodecaedro rómbico?

El planteamiento de esta cuestión nos permite relacionar este poliedro con el Arte.

Durante el Renacimiento los artistas y artesanos mostraron mucho interés en los poliedros. Un buen ejemplo es Leonardo Da Vinci y sus ilustraciones para el libro de su amigo Luca Pacioli ‘La divina proporción’. En este libro se nos muestra una manera de generar nuevos poliedros añadiendo pirámides a las caras de un poliedro base. Si aplicamos este procedimiento a un cubo obtenemos un poliedro de veinticuatro caras que casi es nuestro dodecaedro.

Pero el mérito vuelve a ser de Kepler que es el que nos da la idea clave.

En su libro ‘Epitome Astronomiae Copernicanae’, Kepler nos muestra que el dodecaedro rómbico es un cubo al que hemos añadido ciertas pirámides de una altura determinada. Un paso sencillo pero fundamental. Cada pareja de triángulos que se apoya en una arista del cubo son coplanarias, formando en total doce caras rómbicas. Esto es lo que consideraremos el tercer punto de vista de Kepler sobre el poliedro.

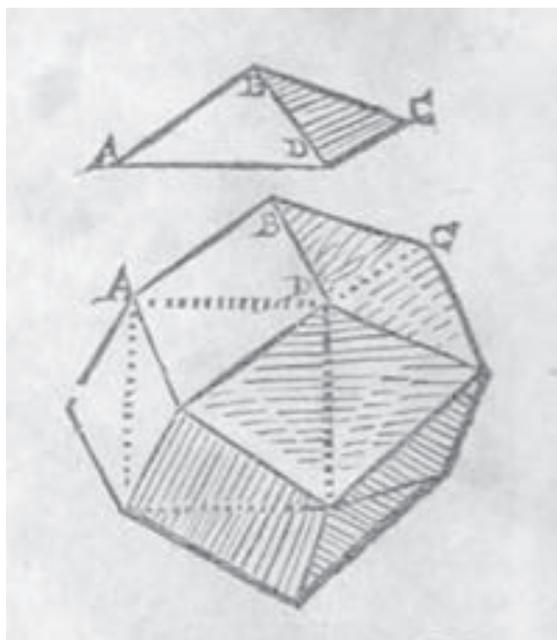


Figura 8: *Un cubo con pirámides.*

Esta es la manera más sencilla de comprender este poliedro. La que nos permite conocer las dimensiones de sus caras rómbicas en relación con su arista, que dentro del dodecaedro rómbico podemos inscribir un cubo (de paso diremos que también un octaedro), que su volumen es el doble que el del cubo inscrito, que tesela el espacio, que el ángulo entre dos caras adyacentes es de  $120^\circ$ , podremos hablar del ángulo de Maraldi, etc...Ver [3].

#### 4.4. Los poliedros rómbicos de Kepler

La manera en la que Kepler nos muestra el dodecaedro rómbico y los tres puntos de vista que hemos estudiado son muy interesantes. Pero, ¿sabemos realmente cómo Kepler descubre este poliedro? Pienso que no. Podemos plantearnos una suposición bastante plausible y que nos va a permitir hablar del cuarto modo de ver este poliedro: El dodecaedro rómbico es una consecuencia lógica de la noción de dualidad aplicada a los poliedros platónicos.

El siguiente párrafo es clave:

*Traigo estos rombos a colación para abordar un problema de geometría: ¿existirá un cuerpo, similar a los cinco poliedros sólidos regulares y a los catorce poliedros sólidos arquimedianos que pueda ser construido nada más que con rombos? Encontré dos, uno con afinidad al cubo y al octaedro, otro al dodecaedro y al icosaedro - el cubo mismo puede servir para representar un tercero, poseyendo la afinidad con dos tetraedros acoplados juntos. El primero está formado por doce rombos, el segundo por treinta. Pág 13 de [1].*

De los infinitos poliedros que se pueden imaginar formados por rombos iguales, Kepler destaca tres. Dos de ellos son descubrimiento suyo: el formado por doce rombos que es el dodecaedro rómbico y el que tiene treinta caras rómbicas que llamamos triacontaedro.

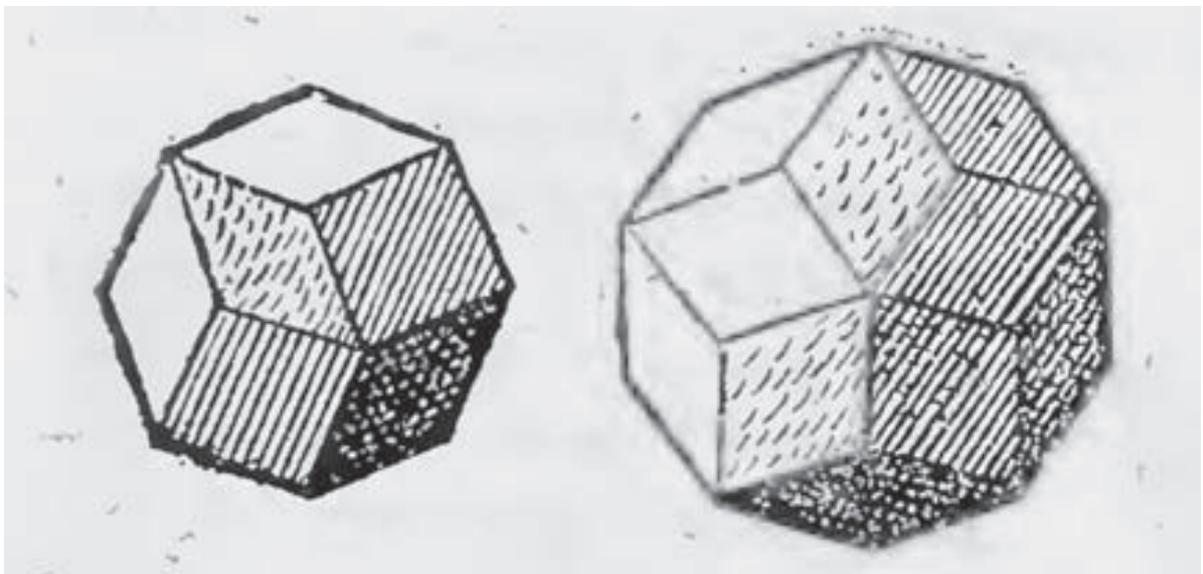


Figura 9: Dodecaedro rómbico y triacontaedro en 'Harmonice Mundi'.

El tercero es el archiconocido cubo. El motivo para incluir el cubo no es

el hecho trivial de que sus caras son cuadrados, es decir, un caso particular de rombo. El motivo es mucho más profundo e interesante.

Las parejas de sólidos platónicos duales tienen el mismo número de aristas. Cada pareja puede colocarse de modo que pares de aristas se bisequen ortogonalmente. Entonces decimos que están en ‘posición recíproca’. Una vez más, es muy conveniente construir modelos para tener una visión clara de estas relaciones.

La intersección del cubo y el octaedro en posición recíproca es el cuboctaedro y su envoltura resulta ser nuestro dodecaedro rómbico. Estos dos poliedros son también duales.

La intersección del icosaedro y del dodecaedro en posición recíproca es el icosidodecaedro. Otro precioso poliedro arquimediano. Su envoltura es el triacontaedro. Ambos poliedros son también duales y, por lo tanto, el triacontaedro es otro sólido de Catalan. Los rombos del triacontaedro son distintos de los del dodecaedro.

El tetraedro es autodual o dual de otro tetraedro. Si colocamos dos tetraedros en posición recíproca obtenemos un poliedro que ya era conocido antes de Kepler. Por ejemplo, fue dibujado por Leonardo. Kepler lo rebautiza ‘Stella Octangula’ y así lo seguimos conociendo hoy. La intersección es el octaedro y su envoltura es el cubo. Ya sabemos que ambos poliedros también son duales. Por este motivo, el cubo es el tercer poliedro rómbico de Kepler.

Se trata de un ejemplo excelente de cómo la generalización de una idea y el uso de la analogía son herramientas para obtener resultados matemáticos.

Esto es un esbozo de lo que podríamos desarrollar si quisiéramos obtener estas conclusiones de la noción de dualidad.

## Resumen

El dodecaedro rómbico es un poliedro que nos ofrece una oportunidad excelente para disfrutar de la Geometría. Nos permite conocer su descubrimiento en un contexto histórico y presentar a su descubridor, el genial astrónomo y matemático Johannes Kepler. Relacionar las Matemáticas con la observación de la Naturaleza, problemas aplicados y el Arte. A lo largo de su estudio nos encontraremos con problemas que han sido de fácil enunciado pero difícil demostración y que han sido muy fructíferos para las Matemáticas. Pero tam-

bién con cuestiones sencillas muy adecuadas para ser planteadas a jóvenes estudiantes. Avanzando un poco más podremos relacionarlo con la dualidad y, por lo tanto, entrar en el terreno de la Topología. ¿Se puede pedir más?

En el artículo se quiere destacar la importancia de la construcción de modelos matemáticos que entronca con la mejor tradición de enseñanza de las Matemáticas. Y esto lo hacemos no solo por su belleza sino también por que nos ayudan a comprender mejor sus propiedades matemáticas. Además, podemos decir que cuando nos planteamos asuntos como la teselación del espacio o el empaquetamiento de esferas, la construcción de modelos resulta casi imprescindible. Dibujos, fotografías e incluso aplicaciones interactivas se pueden volver confusas para ojos inexpertos y la percepción espacial se va desarrollando con la manipulación de este tipo de modelos.

## Referencias

- [1] Johannes Kepler (1611), *Strena Seu De Nive Sexangula (Regalo de año nuevo. Sobre el copo de nieve hexagonal)*, Editorial Aviraneta, Traducción y notas de Ana García Azcárate y Ángel Requena Fraile (2011). Este libro se puede descargar gratuitamente gracias a la generosidad de los autores a través del excelente sitio web de Ángel Requena ‘Turismo Matemático’ en su sección ‘Libros descargables’. <https://mateturismo.wordpress.com/libros-descargables/>
- [2] Thomas Heath (1921), *A History of Greek Mathematics. Volume II: From Aristarchus to Diophantus*. Oxford University Press.
- [3] Roberto Cardil Ricol (2019), <http://www.matematicasvisuales.com/html/geometria/construccionpoliedros/RDindice.html>. Página web complementaria a este artículo con más información sobre la exposición *Kepler, las abejas y el dodecaedro rómbico*, enlaces, modelos para descargar, aplicaciones interactivas y extensa bibliografía.

# Prime spirals as a tool for analysing sets within $\mathbb{N}$

## Espirales primas como una herramienta para el análisis de conjuntos en $\mathbb{N}$

Darwin Méndez Contreras

Universidad Nacional Autónoma de Honduras

dw.mendez1@gmail.com

### Resumen

*Within the area of mathematical games, spirals can be considered as sequences of natural numbers that are represented graphically, according to a drawing pattern. Initially, the most widespread is the Spiral of Ulam, which shows a very simple arrangement of the prime numbers in the spiral. In fact, the study of this type of spiral is usually limited to observing the arrangement of the subset of prime numbers in them. This article considers a type of spiral related to so-called "centered polygonal numbers". The results found show the potential utility of such spirals as a graphic support in the analysis of a figure and its background (that is, for the visualization of a numerical subset and the gap it leaves). It is also shown how certain subsets of an initial set inherit graphic properties from the main set, in terms of the drawing pattern considered.*

### Introducción

Una espiral prima se forma mediante la sucesión de números naturales partiendo de una cifra central (por ejemplo el 1), que posteriormente es rodeado por el resto de números naturales en una espiral infinita. Señalar números

primos con una espiral de este tipo da como resultado un patrón visual, por ello se les denomina frecuentemente como espirales primas, lo cual termina siendo la palabra clave para hacer búsquedas del tema.

Marcar grupos polinómicos con alta densidad de primos ha devuelto resultados que respaldan la noción de un patrón visual. La duda recae en si dichas espirales pueden conducir a una ecuación que describa de forma exacta la secuencia que siguen los números primos o si se están pasando por alto principios importantes que no han sido descritos en investigaciones previas.

Los trabajos académicos que abordan el tema aparecieron en los 60's [2] aunque su autor inicial se desligó de él y se dedicó a otros trabajos. Hoy día existen múltiples espirales por parte de distintos autores, muchos de los cuales han trabajado de manera informal en el tema centrándose únicamente en mostrar la forma en que se distribuyen los números primos y dejando pocas observaciones o conclusiones realizadas por su parte. Ahora se cuenta con herramientas digitales que permiten experimentar con algunas espirales existentes, pues el autor del presente material no tenía conocimiento de ellas y empleó herramientas menos prácticas como editores de imagen que obligaron a una revisión minuciosa en los resultados y de manera paradójica mejoró las observaciones.

El presente artículo deja un registro que expone patrones interesantes sacados de conjuntos elementales que no fueron considerados por otros autores. También se dan pautas concretas para la elaboración y revisión de espirales estrechamente relacionadas con números triangulares centrados, con observaciones entre las cuales destaca un análisis de figura y fondo, pues al descartar elementos de un conjunto dado, estos pasan a ser miembros de un conjunto complementario cuya unión da nuevamente la totalidad de los enteros.

Se aclara que las espirales son un soporte visual, pero las interpretaciones visuales no suplantán a las demostraciones matemáticas. Si no se entiende adecuadamente lo que se observa, las atribuciones de elementos aparentemente observables pueden ser erróneas y pertenecer a otros principios. Bajo este enfoque se describirá el porqué se encuentran patrones al marcar un conjunto tan complejo como el de números primos.

# 1. Antecedentes

## 1.1. Espiral de Ulam

La espiral de Ulam es considerada una representación gráfica del conjunto de números primos, creada por el matemático polaco Stanislaw Marcin Ulam, y popularizada en la columna de Juegos Matemáticos de la revista Scientific American. Ulam en 1963, aburrido durante una conferencia científica, estaba haciendo garabatos en una hoja de papel. Dispuso una malla de números en espiral, empezando por el 1 en el centro, el 2 a su derecha, el 3 arriba, el 4 encima del 1, el 5 a la izquierda, y así sucesivamente (Figura 1). Posteriormente, marcó los números primos y descubrió que los números marcados tendían a alinearse a lo largo de líneas diagonales.

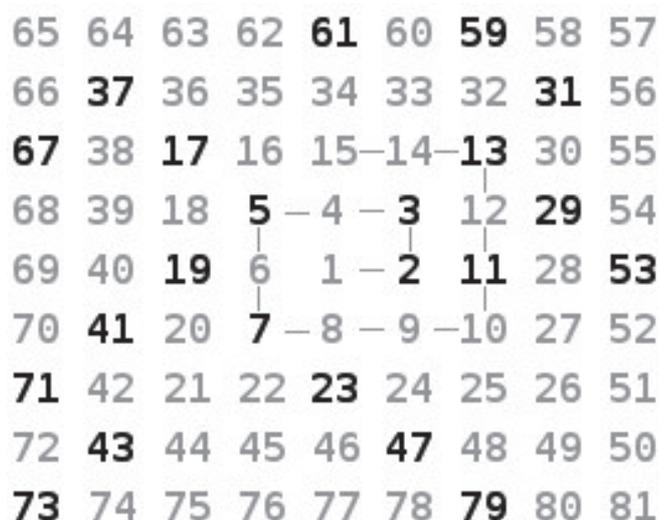


Figura 1: *Espiral de Ulam, números primos resaltados.*

Todos los números primos, excepto el 2, son impares. Como en la espiral de Ulam algunas diagonales contienen números impares y otras contienen números pares, no sorprende ver cómo los números primos caen todos (salvo el 2) en diagonales alternas. Sin embargo, entre las diagonales que contienen números impares, visualmente algunas contienen números primos en mayor proporción que otras a primeras impresiones.

El patrón se muestra igualmente aunque el número central no sea 1. Esto significa que hay muchas constantes enteras  $b$  y  $c$  tales que la función

$$f(n) = 4n^2 + bn + c$$

genera, a medida que crece  $n$  a lo largo de los naturales  $1, 2, 3, \dots$ , una gran cantidad de números primos en comparación con la proporción de primos existente en números de magnitud similar [1].

## 1.2. Espiral de Sacks

Desarrollada por Robert Sacks en 1994 mediante una espiral de Arquímedes que comienza en cero y donde la posición de cada número natural se representa mediante coordenadas polares por la ecuación

$$a = \sqrt{n}$$

donde  $a$  representa un número de rotaciones, y no un ángulo en radianes ni en grados [4].

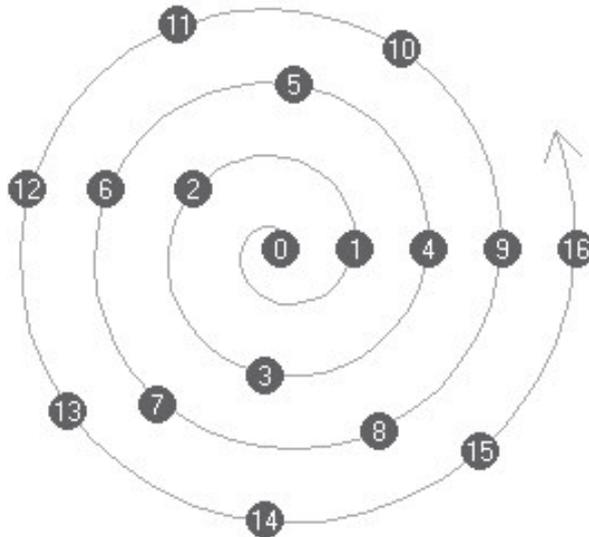


Figura 2: *Espiral de Sacks.*

Algunas curvas que comienzan en el origen parecen tener una gran densidad de números primos; una de estas curvas por ejemplo contiene números del tipo  $n^2 + n + 41$ , que es un famoso polinomio abundante en números primos que descubrió Leonhard Euler en 1774. Se desconoce hasta qué punto las curvas de la espiral permiten predecir grandes números primos o compuestos [5].

## 2. Espirales basadas en números poligonales centrados

Los números poligonales centrados generan figuras de números en las que cada figura está formada por un punto central circundado por capas poligonales con un número constante de lados. Cada lado de una capa poligonal contiene un punto más que la capa anterior, por lo que a partir de la segunda capa poligonal, cada capa de un número  $k$ -gonal centrado contiene  $k$  más puntos que la capa anterior (Figura 3).



Figura 3: *Estructura para los números hexagonales centrados.*

El centro de cada número poligonal centrado lo rodean  $k$  grupos de otros números figurados, los números triangulares [3], los cuales trabajan por niveles en lugar de capas y que son generados mediante la fórmula

$$T_n = \frac{n(n+1)}{2}$$

En concreto, para un polígono de  $k$  lados, la fórmula para calcular los números poligonales centrados es

$$\begin{aligned} CP(k, n) &= 1 + k + 2k + \dots + (n-1)k \\ &= 1 + \frac{(n-1) \cdot n \cdot k}{2} \end{aligned}$$

De manera implícita esta ecuación contiene a la de los números triangulares, teniendo en cuenta que se usa  $T_{n-1}$  en lugar de  $T_n$  por lo que internamente  $n(n+1)$  pasa a ser  $(n-1)((n-1)+1) = (n-1)(n)$  como vemos en la ecuación anterior. Por tanto, entre los números triangulares y los poligonales existe la relación siguiente:

$$CP(k, n) = 1 + k * T_{n-1}$$

La relevancia de estos elementos comienza con la existencia de un elemento central y  $k$  grupos de números triangulares, en este trabajo consideramos a  $k$  una *base* que corresponde a los lados del polígono formado por una espiral. En el caso de la espiral de Sacks esta no corresponde a un número poligonal, pero sí tiene un punto central y define el final de cada vuelta. Por otro lado, el final de las vueltas en la espiral de Ulam corresponde a un número poligonal con  $k = 8$ . De ahora en adelante se trabaja con espirales que siguen este último comportamiento.

## 2.1. Pautas al elaborar una espiral poligonal centrada

Como se dijo en un principio, el principal objetivo de este trabajo es dejar pautas, algunas de ellas simplemente para facilitar la revisión y otras serán justificadas en relación a los resultados que terminan generando.

Las pautas al elaborar una espiral centrada serán las siguientes:

- 1) Usar el número cero como punto de partida para toda espiral.
- 2) Basar la primera vuelta alrededor del origen en una base  $k$  que incrementará en función de un número triangular  $T_n$ .
- 3) Orientar la ruta que siguen los números en sentido de las manecillas del reloj dejando los números finales de cada vuelta en la posición que corresponde a las 12 horas.

## 2.2. Espiral hexagonal

Siguiendo las tres pautas anteriores procedemos a crear una espiral cuya *base* poligonal es 6, es decir  $k = 6$ . En la Figura 4 se observan dos vueltas, la primera en rodear el origen termina con el número 6 y la segunda con el 18.

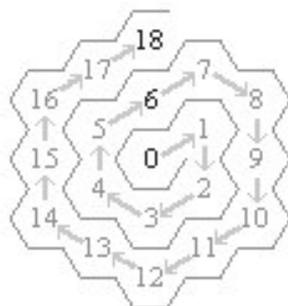


Figura 4: *Espiral hexagonal.*

Al escoger el número cero como origen se simplifica la fórmula  $CP(k, n)$  dado que ahora el número que termina cada vuelta es una unidad menor

$$CP_0(k, n) = \frac{(n-1) \cdot n \cdot k}{2}$$

$$CP_0(6, n) = 3n(n-1), \quad n \geq 1$$

que genera la sucesión  $\{0, 6, 18, 36, 60, 90, \dots\}$

Por su geometría, la espiral hexagonal permite ver con mucha claridad la distribución de sus elementos. La Figura 5 cuenta con seis filas que parten del centro a las esquinas de la espiral en donde los números están marcados con tonos oscuros; las tres filas oscuras están formadas por números pares y las otras tres intercalan números pares e impares. Esos números opacos, y no los claros, pueden ser calculados añadiendo operaciones adicionales a la fórmula  $CP_0(k, n)$  teniendo en cuenta que cada vuelta esta separada por  $\frac{1}{k}$  porciones de vuelta y ese fragmento de vuelta contiene  $n-1$  elementos.

$$CP_0(k, n, s) = \frac{(n-1) \cdot n \cdot k}{2} - s(n-1)$$

donde  $s$  representa a los sectores que restan para completar vuelta.

Para  $s = 1$ , la sucesión obtenida es  $\{0, 5, 16, 33, 56, 85, \dots\}$  obtenida como  $\{0 -0, 6 -1, 18 -2, 36 -3, 60 -4, 90 -5, \dots\}$

Si  $s = 2$  se obtiene la sucesión  $\{0, 4, 14, 30, 52, 80, \dots\}$  obtenida de  $\{0 -0, 6 -2, 18 -4, 36 -6, 60 -8, 90 -10, \dots\}$

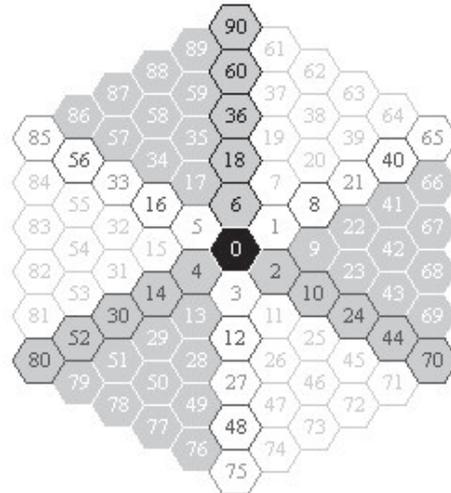


Figura 5: *Espiral hexagonal dividida en 6 sectores con  $T_{n-1}$  elementos.*

En cuanto a patrones, muchos pueden ser los puntos de partida a observar. Pero priorizando una progresión que nos da a entender la importancia de las pautas proporcionadas, comenzaremos con el patrón que siguen los múltiplos de  $k = 6$  (Figura 6). La ecuación  $CP_0(k, n)$  pasa a formar la parte superior de un eje que divide simétricamente un patrón observable.

Al revisar a detalle los elementos en los  $k$  sectores se observa que cada uno de ellos agrupa en filas la parte que le corresponde del conjunto marcado. La distribución genera filas continuas en los sectores superiores mientras que en los medios e inferiores las filas son discontinuas, lo que es provocado por el cambio de ángulo en la trayectoria que siguen los números favoreciendo la alineación al iniciar y terminar una vuelta.

Teniendo presente que los múltiplos de 6 son un subconjunto de los múltiplos de 3 y a su vez representan la mitad de este último conjunto, al observar simultáneamente ambos se aprecia cómo aparecen nuevas filas en los sectores superiores y se llenan espacios en los sectores inferiores, por lo que los sectores medios son los únicos que quedan discontinuos.

Si se hubiese utilizado el número uno como origen el patrón presentaría un desfase en la simetría debido a que 1 no es múltiplo de  $k$ , pero si se comenzara con cualquier múltiplo de  $k$  la simetría en el patrón observado volvería a ser la misma.

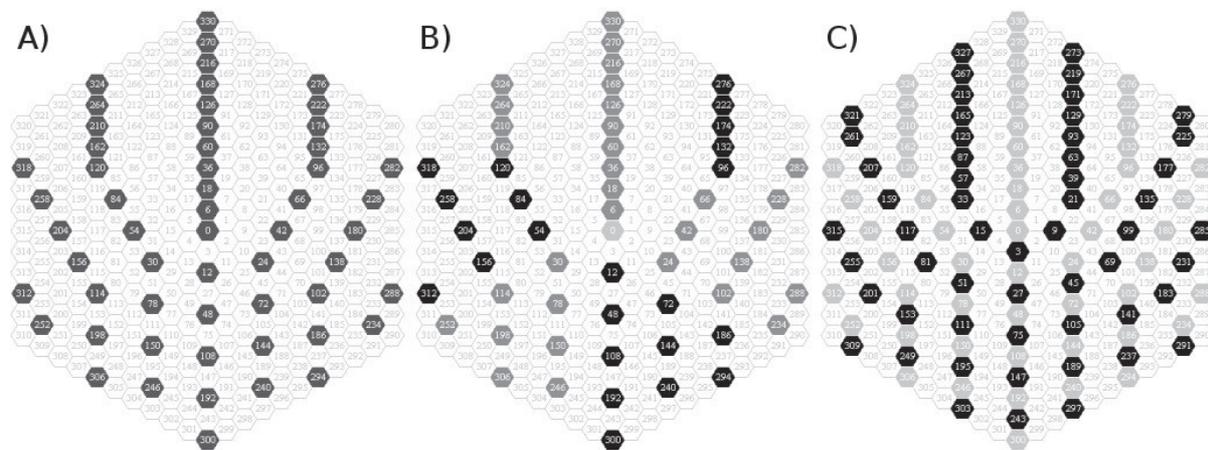


Figura 6: A) Múltiplos de 6 B) Múltiplos de 6 según los sectores C) Múltiplos de 6 dentro de los múltiplos de 3.

Al entender que estas espirales están separadas en  $k$  sectores evitamos caer en interpretaciones basadas solo en primeras impresiones. Retomando los múltiplos de 3 (Figura 7) al visualizar todo el conjunto sin separar los sectores, las observaciones pueden ser cuestión de óptica en lugar de análisis.

En esta figura se muestra un patrón en forma de cruz al marcar los múltiplos de 3. Puede resultar difícil de visualizar sin la diferenciación de tonos, aunque a fin de cuentas dicho patrón es una interpretación óptica que puede tener muy poco valor teórico. Al comparar el patrón en cruz con los múltiplos de 6, pese a tratarse de un subconjunto de los múltiplos de 3, no presenta un patrón afín con dicha cruz dado que la relación visual entre un conjunto y otro no se encuentra de esa manera.

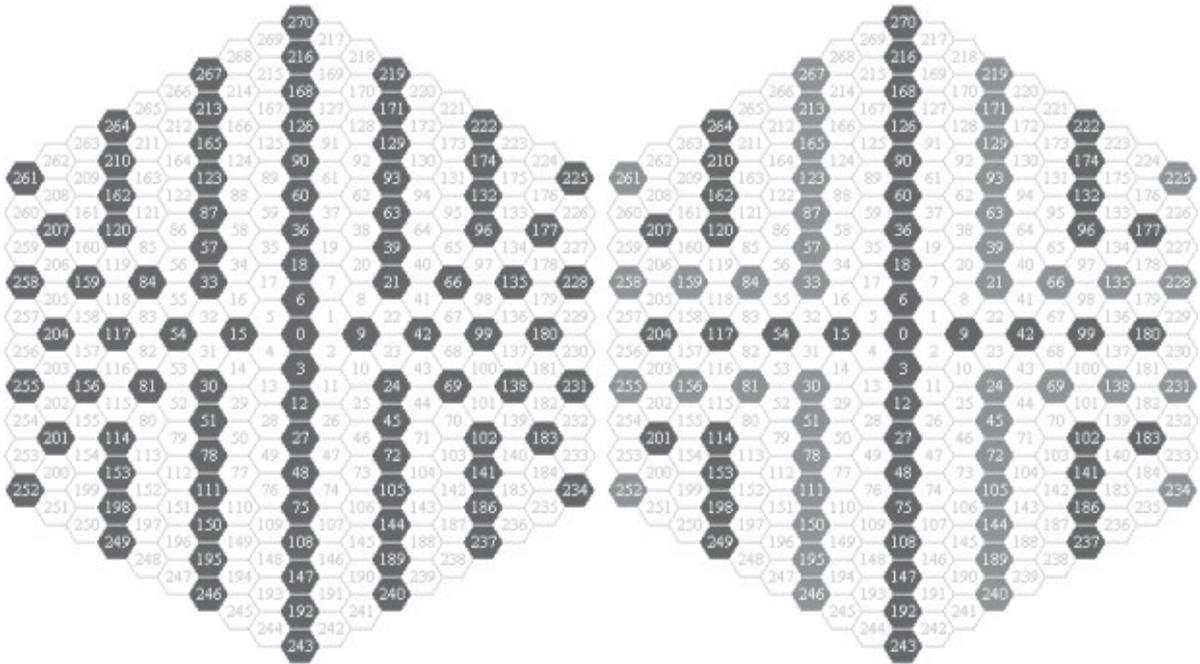


Figura 7: Múltiplos de 3, aparente patrón en cruz.

Se podrían iniciar las espirales desde enteros negativos y las propiedades de iniciar con un múltiplo de  $k$  para obtener patrones simétricos al marcar el conjunto persistirán, también los desfases provocados por los no múltiplos.

Una discusión importante a plantear es la posibilidad de emplear este tipo de espirales como una herramienta para analizar conjuntos bajo criterios de figura y fondo; por ejemplo, al haber marcado los múltiplos de 3 a su vez se genera una figura de fondo formada por los *no múltiplos de 3* y la unión de ambos conjuntos vuelve a formar los  $N$ .

Al elegir múltiplos de 5 y 7 que no se relacionan con  $k = 6$ , de la espiral hexagonal obtendremos otro tipo de patrones (Figura 8). Diferenciar los sectores permite observar patrones que de otro modo no serían nada fáciles visualizar.

En el caso A se encuentran los múltiplos de 5 y en cada agrupación de 5 elementos, tres de ellos forman una "semicircunferencia" dos más la extienden. En cada sector se visualiza claramente la peculiaridad de que la concavidad va rotando en sentido contrario al de las manecillas del reloj.

El caso B con los múltiplos de 7, observamos 7 elementos, similar a la agrupación que forman los múltiplos de 5, solo que con un elemento extra en cada costado. Algunos de ellos son tanto múltiplos de 5 como de 7, pero no en su mayoría y la concavidad de los sectores en este caso va cambiando de acuerdo a las manecillas del reloj.

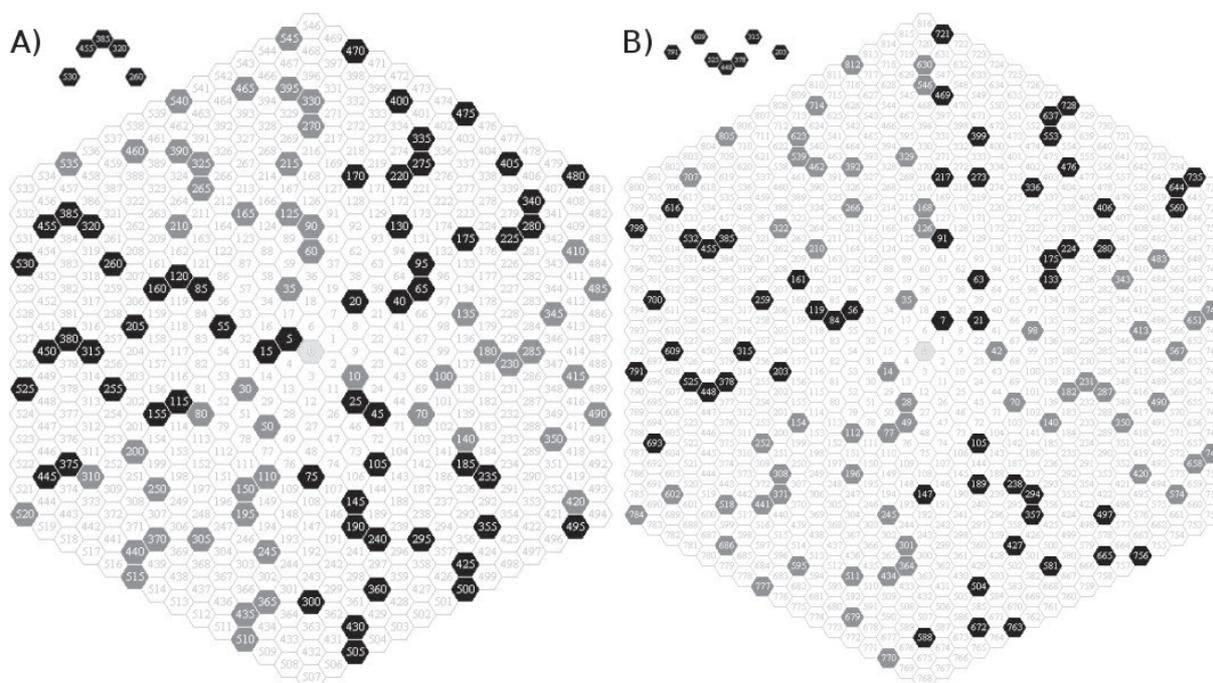


Figura 8: A) Múltiplos de 5 B) Múltiplos de 7.

Por otro lado el 5, el 7 y también el 3 que vimos anteriormente son números primos y se debe considerar que estos grupos poseen características especiales propias de ellos, que de alguna forma las van a heredar a sus subconjuntos. Si los múltiplos de 6 presentaron una característica especial fue porque  $k$  en la espiral hexagonal es 6, esto cambia según  $k$ .

### 3. Reinterpretando la espiral de Ulam

La espiral de Ulam no se construye acorde a las pautas sugeridas, pero el final de sus vueltas se puede obtener con  $CP(k, n)$  y el  $k$  correspondiente es 8. Ulam usó un procedimiento muy análogo en su destello de ocio creativo que es fácil de seguir, pero quizás por la ausencia de conceptos o secuencias (que se descubrieron posteriormente), su trabajo no dio con la relación de los números poligonales centrados. La espiral de Ulam no es otra cosa que un arreglo para los números octogonales centrados.

Ajustada la espiral mediante una ruta diferente, podemos obtener una columna de enteros que finalizan el nivel en la posición de las 12 horas (Figura 9). La ruta traza una diagonal a  $45^\circ$  desde el centro y los finales de cada nivel para luego dirigirse al inicio de la próxima vuelta. La forma cuadrada es solo una interpretación acorde con la distribución de números octogonales centrados. Pero al compararlo con el método empleado por Ulam, esta nueva ruta no resulta nada intuitiva.

Esta espiral cuadrada con  $k = 8$  no debe menospreciarse como un mero ajuste, en sí, la espiral de Ulam también es un ajuste, solo que no había noción de ello al crearse por más intuitivo que hubiera sido el proceso de construcción. Lo importante será la comparación de ambas para revelar el verdadero comportamiento en la distribución de los números, donde lo relevante es reconocer que la base  $k$ -gonal es 8 y no que la forma de la espiral sea cuadrada.

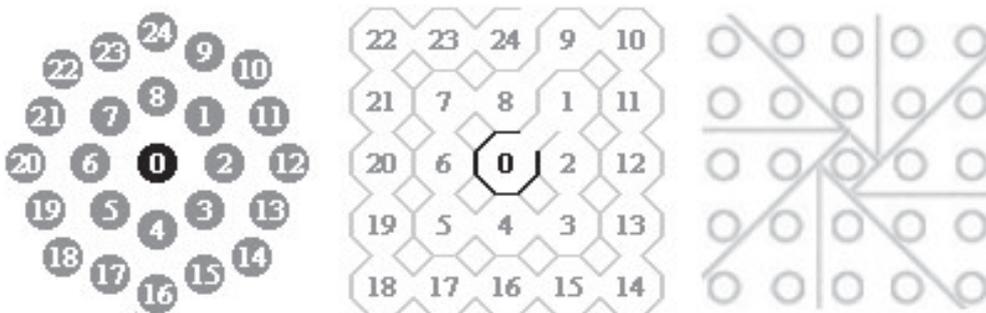


Figura 9: *Espiral octogonal, ruta ajustada para encajar con la espiral de Ulam y  $k = 8$  sectores.*

Al comparar la distribución de los múltiplos de 8 que corresponde a la base  $k$ -gonal de ambas espirales (Figura 10) podemos notar varias diferencias. Los números finales en la espiral de Ulam quedan en una diagonal inferior

derecha, como comienza de una los múltiplos de 8 se alinean con un ligero desfase en esa diagonal. Se podría creer que la diagonal que cruza la espiral de Ulam separa el patrón de los múltiplos de 8 en filas continuas y discontinuas.

La espiral cuadrada con base 8 presenta un patrón simétrico similar a la de los múltiplos de 6 en la espiral hexagonal y la columna de los números finales queda perfectamente reconocible en una columna central. Aunque la ruta no fuese intuitiva, ha permitido este acomodo agradable de los elementos. En la ilustración no se ha mostrado una diferenciación de los sectores, pero son éstos los que dan lugar a este patrón que depende de la base  $k$ -gonal que tenga la espiral. La misma explicación dada en el patrón de la espiral hexagonal es válida aquí también.

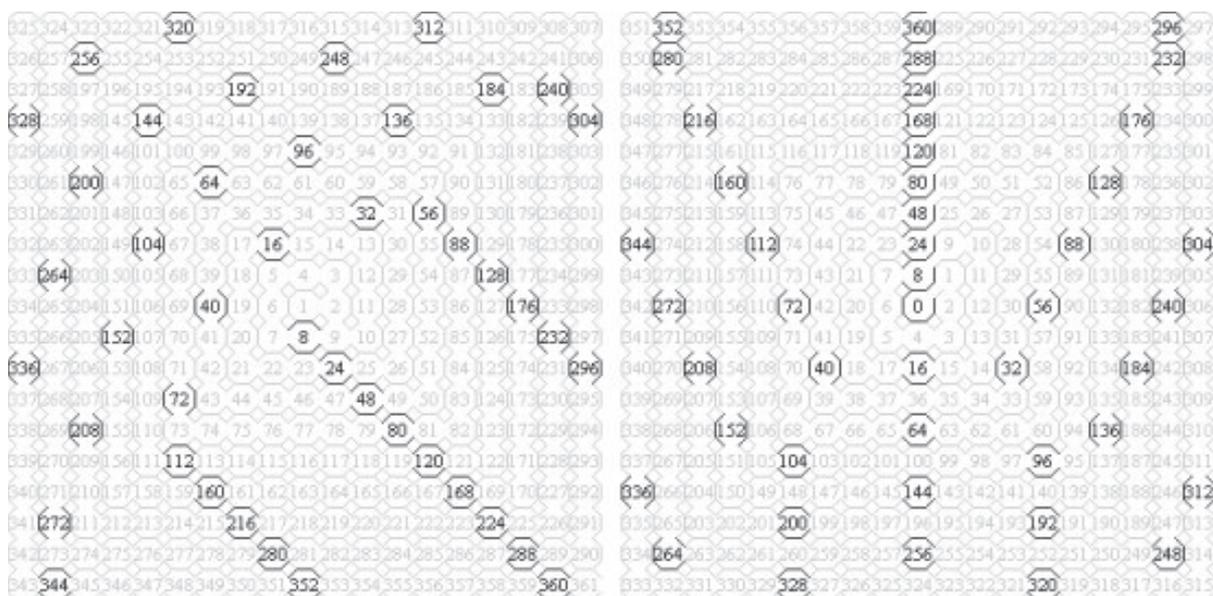


Figura 10: Múltiplos de 8. La parte izquierda de esta figura es relativa a la Espiral de Ulam y la derecha se refiere a la Espiral Cuadrada con Base Ocho.

Éste ha sido un ejemplo muy claro en el que se puede valorar las pautas dadas con el fin de tener resultados fáciles de analizar. La diferencia en la claridad con que se muestran los patrones es evidentemente favorable para la espiral que siguió las pautas. El cero evita los desfases al marcar los  $k$  múltiplos de distintas espirales, además de ser un múltiplo común para cualquier  $k$ . El entender que las espirales se relacionan con un número poligonal centrado ayuda a escoger estrategias para abordar los análisis, y que la orientación en los finales de vueltas sea la posición de las 12 horas facilita las observaciones.

## 4. Números primos dentro de las espirales

La distribución de los números primos es un problema que sigue inquietando a muchos matemáticos aún en nuestros días. Que Ulam diera con una malla de números que presentara cierta conducta despertó el interés de muchos investigadores que intentarían replicar resultados similares con otras espirales. Se creó una visión túnel donde lo único a observarse eran los números primos y algo elemental se pasó por alto.

### 4.1. Patrones de pares e impares

Dos conjuntos elementales de números naturales son los formados por los números pares e impares, respectivamente. Ambos grupos son figura y fondo uno del otro, por lo que es inevitable que al marcar los números pares en una espiral simultáneamente, se marquen los impares (Figura 10). En la espiral de Ulam la distribución es simple, se ve como una cuadrícula de ajedrez. En la espiral cuadrada con base 8 hay una cruz central compuesta por números pares intercalándose a modo de ondas con los números impares.

La diferencia recae en una interpretación de los números que finalizan las vueltas; en la espiral cuadrada con base 8 se posicionan en una recta a  $90^\circ$  y por el otro lado los finales se posicionan en una diagonal a  $45^\circ$ . Haciendo un marcado especial en la espiral de Ulam, el otro patrón aparece y todo se debe a que en realidad ambos casos son un arreglo de un número octagonal centrado con 8 esquinas de las cuales 4 sobresalen y las otras 4 se esconden entremedio por la forma cuadrada.



Figura 11: Múltiplos de 2 en tonos claros, números impares en tonos oscuros. La parte izquierda de este tríptico se refiere a la Espiral Cuadrada con Base Ocho y las otras dos figuras se refieren a la Espiral de Ulam.

Dado que todos los números primos mayores que 2 son impares, es evidente que todo patrón presente en un conjunto de números impares se verá reflejado en un patrón de números primos. Esto quiere decir que cuando los números primos se alinean en las diagonales de la espiral de Ulam lo hacen porque los números impares se alinean en diagonales. El patrón observado no es una conducta propia sino heredada.

La espiral de Ulam no es la única en presentar patrones notables al diferenciar números pares de impares pues todas las espirales  $k$ -gonales presentan patrones propios (Figura 11).

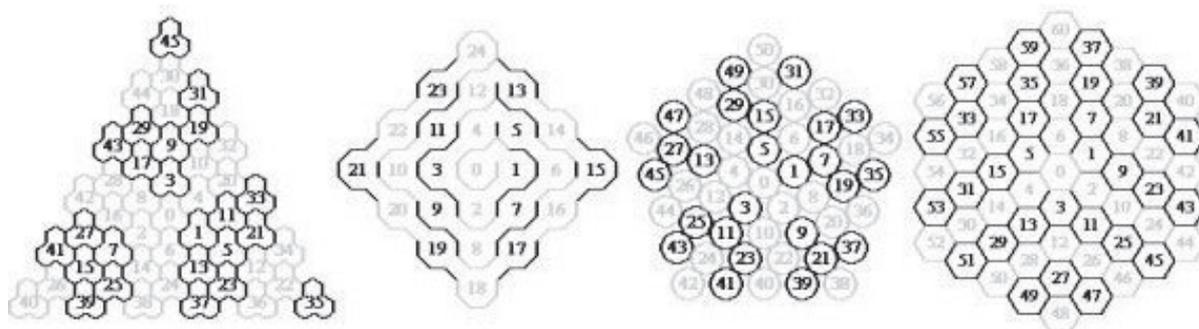


Figura 12: *Múltiplos de 2 en tonos claros, números impares en tonos oscuros.*

## 4.2. ¿Cuales son las expectativas?

Se pueden crear espirales  $k$ -gonales al infinito y podría suceder que alguna de un resultado directamente relevante con números primos, pero hay que tener en cuenta a otros conjuntos que pueden mostrar resultados con una importancia propia. Conjuntos con distribuciones complejas pueden estar dentro de conjuntos bastante sencillos de expresar por lo que hacer asociaciones de figura y fondo empleando este tipo de espirales es un camino abierto actualmente.

Como cualquier campo de las matemáticas, esta temática es digna de estudiar, es enorme, desconocido y ante la inmensidad lo importante es entender las bases, pero aún teniendo criterios para entender y crear espirales basadas en números poligonales centrados, los resultados al marcar patrones son inciertos. Este es un trabajo matemático con un alto potencial experimental y recreativo.

## Conclusiones

Las espirales basadas en números poligonales son un recurso gráfico que denota conductas en conjuntos enteros. Entender que los números primos están contenidos en los números impares salvo el 2 no es ninguna novedad; no obstante, observar el comportamiento de un subconjunto que está contenido en un conjunto más grande y entender la relación del comportamiento de ambos mediante un recurso gráfico puede aportar bastante al campo de teorías de conjuntos, o remarcar una relación no notable solo con ecuaciones.

Los análisis de figura y fondo en matemáticas necesitan de herramientas como ésta para denotar la interacción de un conjunto y el vacío que dejan, dado que recíprocamente el patrón también está presente en esos vacíos.

Entender el comportamiento de conjuntos básicos ayudará a analizar patrones en subconjuntos enteros más complejos. Ir directamente a evaluar conjuntos complejos puede hacer caer en observaciones de comportamientos ya presentes en conjuntos simples. También resulta mejor estudiar las espirales con bases poligonales pequeñas por ser fáciles de analizar, sirviendo así de modelos generales, que posteriormente podrán ser usados para analizar espirales alteradas que sean compatibles con esos modelos generales.

Se debe partir del número 0 como origen por ser consistente a la idea del punto de partida o eje central desde donde posteriormente se van nombrando las otras posiciones con una sucesión ordenada de enteros. Se puede partir de otros números, pero resulta lo mismo que cambiar de nombre a todas las posiciones. Para entender bien la naturaleza de las espirales hay que nombrar bien el origen, y aunque se pueda experimentar libremente con otros números, se debe justificar por qué se comienza con ellos o por lo menos tener claro cuál sería el nombramiento ideal.

Pensar que la forma de la espiral es primordial puede llevar a errores en las deducciones. Es la base de una espiral lo que importa en primera instancia. Por ejemplo, se pueden acomodar posiciones de una espiral con base 10 a una espiral de forma pentagonal, y seguramente se encontrarán patrones interesantes por la afinidad de la base con la forma de la espiral, pero esto es debido a que lo primero a analizar era la base y luego la forma con respecto a la base.

## Referencias

- [1] M. Gardner (1964), Mathematical Games: The Remarkable Lore of the Prime Number, *Scientific American*, **210**, 120-128.
- [2] M. Stein, S. Ulam (1967), An Observation on the Distribution of Primes, *American Mathematical Monthly*, **74**, 43-44.
- [3] N. Sloane, P. Simon (1995), The Encyclopedia of Integer Sequences. *San Diego: Academic Press*, Fig. M3826.
- [4] R. Sacks (2003), Number Spiral. *www.numberspiral.com*
- [5] H. Hahn (2008), The distribution of prime numbers on the square root spiral, *ArXiv*, **0801.1441**.

## Reseña de libros

BLANCO NIETO, LORENZO J.: Mirar la ciudad con ojos matemáticos (103 págs.). ISBN: 978-84-948824-5-6. Edita: Federación Española de Sociedades de Profesores de Matemáticas (FESPM) Colección Materiales y Recursos para el Aula. Primera edición: 2020.

El objetivo del libro es doble: dar a conocer la Historia de una ciudad a través de paseos por itinerarios interesantes desde un punto de vista histórico-monumental, a la vez que se van planteando sencillos ejercicios matemáticos relacionados con los monumentos que se van visitando y/o su ubicación. Por todo ello, pueden llamarse Itinerarios Matemáticos.

Los mencionados ejercicios tratan sobre identificación de figuras geométricas (polígonos regulares, ...), transformaciones (ejes de simetría, ...), cálculos de perímetros de polígonos, de número de teselas que recubren un mosaico, de volúmenes de cuerpos, de tiempo transcurrido desde la construcción de un monumento, de estimación de distancias entre monumentos visitados, etc.

Se presenta dividido en dos partes. En la primera se trata sobre el interés didáctico-matemático de paseos por la parte monumental de ciudades, mostrando numerosos ejemplos en ciudades españolas: Burgos, Santiago, Sevilla, Soria, Valladolid, Zaragoza,...

Y la segunda parte se dedica a itinerarios matemáticos por la ciudad de Badajoz: 1º) Puente Viejo y Puerta de Palmas; 2º) Plaza de la Soledad y sus monumentos; 3º) muralla de la Alcazaba y Museo Arqueológico Provincial; 4º) Plaza Alta (árabe), donde estuvo el edificio estilo eiffel del Mercado, trasladado después para ser usado como Biblioteca General de la Universidad; 5º) Plaza de San Juan con la Catedral y el Ayuntamiento; 6º) Plaza de San Andrés (hoy de Cervantes) con empedrado portugués de 1888 con motivos de polígonos irregulares semejantes; 7º) Plaza de San Francisco con solado moderno poligonal y enormes bancos con mosaicos relativos a los conquistadores extremeños.

Incluye numerosos enlaces a págs. Webs, que ofrecen descripciones detalladas sobre los itinerarios y lugares visitados.

El autor es un bien conocido Catedrático de Didáctica de las Matemáticas de la Universidad de Extremadura, autor de varios libros y numerosos artículos relacionados con su Área de Conocimiento.

**Eugenio Roanes Macías**

## Instrucciones para el envío de originales, para su publicación en el Boletín

Los originales de artículos, problemas, reseñas de libros, congresos, etc., deben enviarse *en formato electrónico*, del modo especificado a continuación.

### **Artículos**

Los artículos deberán ser organizados del siguiente modo:

*Encabezamiento*: comenzará con el título del artículo en inglés e, inmediatamente debajo, el título en español; a continuación el nombre del autor o autores; después la referencia al departamento y/o institución de trabajo de los autores; así como las direcciones de correo electrónico de los autores; y, finalmente el Abstract (Resumen) en inglés (estrechado a ambos lados un centímetro, respecto de la anchura del texto).

*Desarrollo*: comenzará con una sección de Introducción (que irá sin numerar), seguida de las demás secciones, cuyos títulos deben ir numerados. Las subsecciones se numerarán con dos dígitos separados por un punto.

*Terminación*: El artículo concluirá con unas Conclusiones, en que se comente brevemente lo más esencial o novedoso del contenido del artículo; y, finalmente, se incluirá la Bibliografía citada.

*Procesador*: Para facilitar la revisión, corrección e impresión es preferible utilizar  $\mu$ S-Word o LaTeX.

### **Respecto de las Figuras**

Las figuras deben ser de buena calidad (impresas desde ordenador, debiéndose evitar los bosquejos a mano alzada). Serán incluidas en el lugar apropiado del texto y en el tamaño en que deban ser impresas.

Las figuras deben llevar debajo numeración (Figura 1, Figura 2, ...), para referirse a ellas en el texto, y un breve descriptor.

No debe escribirse texto a ninguno de los dos lados de la figura, ni a la izquierda ni a la derecha (es decir, las figuras no deben intercalarse en el texto).

### **En caso de usar Word**

El formato de texto debe ser 17 cm (alto) x 12.8 cm (ancho). Para ello, hacer uso del *Diseño de página*, y en *Configurar Página*, elegir estos márgenes: superior 3 cm; inferior 9,7 cm; izquierdo 4,1 cm; derecho 4,1 cm; encuadernación 0 cm. Usar letra *Times New Roman* con “Interlineado sencillo” (no múltiple).

El título (en inglés y español) en minúsculas de 16 puntos; el nombre de autores en minúsculas de 12 puntos en estilo de letra negra; la referencia de departamento o institución de trabajo en 11 puntos en el mismo estilo de letra; y la dirección de correo electrónico en estilo de letra *Courier New* de 11 puntos.

La palabra Abstract (o Resumen), en minúsculas de 12 puntos en letra negra y su contenido, en inglés, en tamaño de letra de 11 puntos en estilo itálica o cursiva.

Los títulos de secciones en minúsculas de 12 puntos en letra negra, sin punto final. Las subsecciones en minúsculas negras en tamaño de letra de 11 puntos. La primera línea posterior al título de sección o subsección no se indentará (es decir, empezará al borde).

### **Plantilla para facilitar la redacción usando Word** (recomendado)

Entrando en la página web de la Sociedad, se puede descargar una plantilla que permite facilitar a los autores el seguimiento de las normas tipográficas anteriormente indicadas.

### **En caso de usar LaTeX**

El formato de texto debe ser 17 cm (alto) x 12.8 cm (ancho). Para ello, hacer uso del estilo "article", eligiendo:  $textheight=17cm$  (alto),  $textwidth=12.8cm$  (ancho) y  $hoffset=0.3cm$ . Por lo demás, tener en cuenta lo indicado anteriormente para usuarios de Word. Para direcciones de correo electrónico usar el tipo de letra `\texttt`.

Si se usan paquetes específicos de *Latex* distintos de los usuales, deberán adjuntarse los archivos correspondientes a esos paquetes.

### **Plantilla para facilitar la redacción usando LaTeX** (recomendado)

Entrando en la página web de la Sociedad, se puede descargar una plantilla que permite facilitar a los autores el seguimiento de las normas tipográficas anteriormente indicadas.

### Selección de originales

Los artículos recibidos para su publicación serán evaluados por miembros del Comité Editorial (mencionados en las páginas 4-5 de los últimos números del Boletín), que decidirán sobre la originalidad, calidad y ajuste del artículo a la línea general del Boletín.

En casos especiales, para efectuar la evaluación se acudirá a revisores externos (no incluidos en el Comité Editorial).

Si se considera oportuno, se pedirá a los autores que hagan modificaciones en el contenido de los artículos o en el modo de presentarlos.

Una vez concluido dicho proceso de revisión de un artículo y adaptación a las normas de publicación anteriormente indicadas, el artículo podrá ser aceptado para su publicación, lo que se comunicará a sus autores y se incluirá en la lista de artículos a publicar en nuestro Boletín.

## Adquisición de números atrasados de nuestro Boletín

Los números atrasados del Boletín, de los cuales existan ejemplares sobrantes, podrán ser adquiridos al precio de coste de diez euros ejemplar. Los números de los que aún quedan algunos ejemplares sobrantes son del 39 en adelante.

El importe puede ser abonado mediante transferencia a la nueva cuenta de la Sociedad, ES58 3025 0006 2114 3326 8241, domiciliada en la entidad bancaria *Caja de Ingenieros, c/. Carranza, 5 Madrid-28003* (o bien mediante un cheque a nombre de *la Sociedad*).

La carta o mensaje de correo electrónico de petición se enviará a la Sede de nuestra Sociedad, que figura en la página 2 de este número del Boletín. En ella se indicará el número o números a adquirir, incluyendo la *dirección* a donde se han de enviar y el correspondiente *cheque nominativo o resguardo de transferencia*.

**INSCRIPCION DE NUEVOS SOCIOS EN LA  
SOCIEDAD "PUIG ADAM" DE PROFESORES DE MATEMATICAS**

**SOLICITUD DE INSCRIPCIÓN**

D. .... Teléf.: .....

Dirección: .....

Ciudad: ..... Cod. Postal: ..... E-mail: .....

Centro de trabajo: .....

Solicita el ingreso como socio de número de la sociedad:

Con esta fecha autorizo al Banco: .....

Dirección de la Sucursal: .....

para que cargue en mi cuenta: ..... / ..... / ..... / .....

los recibos de las cuotas correspondientes al año 2021 y siguientes.

Fecha: ..... de ..... de 2021

Firma:

---

Dicha solicitud se enviará por correo postal a la dirección:  
Sociedad "Puig Adam" de Profesores de Matemáticas  
Facultad de Educación Despacho 3215 28040 Madrid  
o bien al email de la Sociedad: [puigadam@mat.ucm.es](mailto:puigadam@mat.ucm.es)

---

Los nuevos inscritos en la Sociedad que elijan abonar la cuota anual mediante domiciliación en su entidad bancaria, deberán comunicarlo a su banco, para que sean aceptados los recibos, que serán pasados en el mes de enero de cada año.

---

La cuota anual fue establecida en la Asamblea 2012 (véase el Boletín nº 91) en 51 euros para socios individuales y 62 para institucionales (que incluyen la cuota de la Federación de Sociedades, que envía a nuestros socios la revista SUMA).

---

Quienes prefieran abonar la cuota mediante transferencia pueden hacerlo a la c.c. de nuestra Sociedad, domiciliada en la entidad bancaria:

CAJA DE INGENIEROS c/. Carranza, 5 28004 Madrid  
cc. ES58 3025 0006 2114 3326 8241