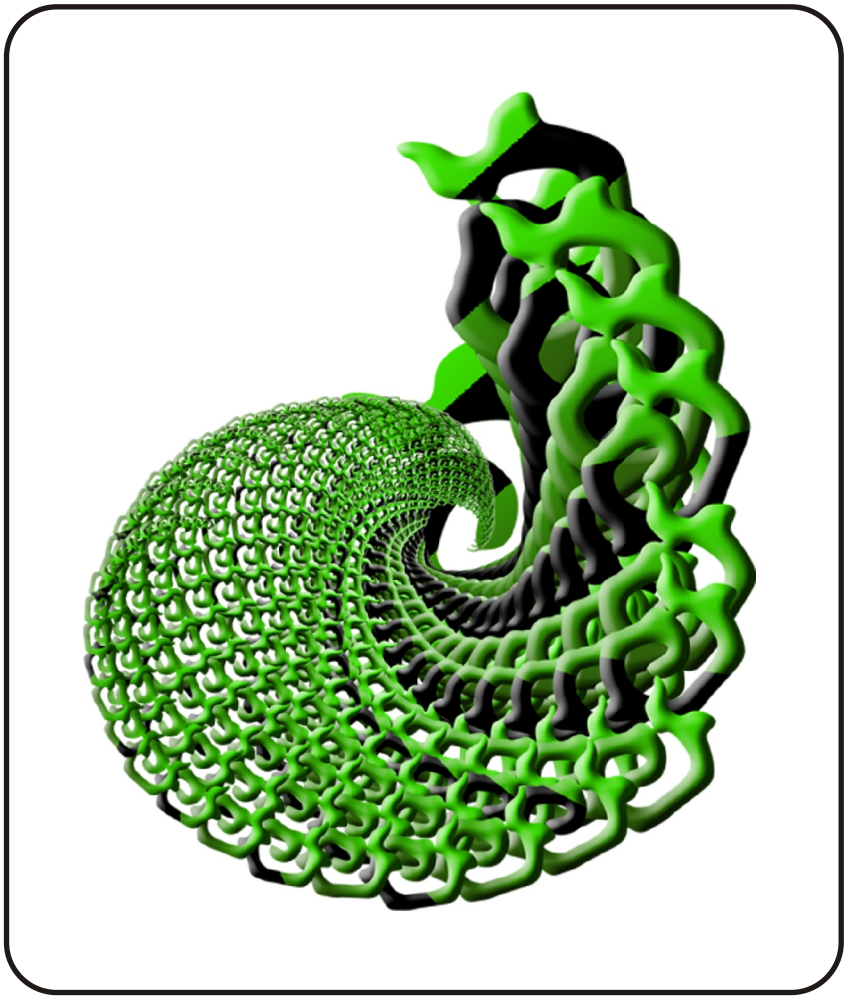
Mixba'al

ISSN:2007-7874

Mixba'al Revista Metropolitana de Matemáticas



Casa abierta al tiempo
UNIVERSIDAD AUTÓNOMA
METROPOLITANA
VOL X, No. 1,JULIO 2019

MIXBA'AL. Vol. X, No. 1, julio de 2019 a julio de 2020, es una publicación anual de la Universidad Autónoma Metropolitana a través de la Unidad Iztapalapa, División de Ciencias Básicas e Ingeniería, Departamento de Matemáticas.

Prolongación Canal de Miramontes 3855, Col. Ex Hacienda San Juan de Dios, Delegación Tlalpan, C.P. 14387, México, Ciudad de México y Av. San Rafael Atlixco, No. 186, Edificio AT, tercer piso, Col. Vicentina, Delegación Iztapalapa, C.P. 09340, México, Ciudad de México. Tel. 5804 4658.
Página electrónica de la revista: http://mat.izt.uam.mx/mat/index.php/revista-mixba-al.
Correos electrónicos: mixbaal2009@gmail.com, mixb@xanum.uam.mx.

Editor Responsable: Dr. Gustavo Izquierdo Buenrostro.
Certificado de Reserva de Derechos al Uso Exclusivo de Título No. 04-2010-072017382600-203, ISSN: 2007-7874, ambos otorgados por el Instituto Nacional del Derecho de Autor. Responsable de la última actualización de este número Dr. Gustavo Izquierdo Buenrostro, División de Ciencias Básicas e Ingeniería, Departamento de Matemáticas, Av. San Rafael Atlixco No. 186, Edificio AT, tercer piso, Coonia Vicentina, Delegación Iztapalap, C.P. 09340, México, Ciudad de México. Fecha de última modificación 5 de julio de 2019. Tamaño del archivo 1.4 MB.

Contacto:
Departamento de Matemáticas, Universidad Autónoma Metropolitana, Unidad Iztapalapa.
Tel: (01) 55 5804 4654 .
Fax: (01) 55 5804 4660.
e-mail: mixbaal2009@gmail.com.
Web revista: http://mat.izt.uam.mx/mat/index.php/revista-mixba-al.

Casa abierta al tiempo

Unidad Iztapalapa

Posgrados:
Maestría y Doctorado en Matemáticas

pmat@xanum.uam.mx
http://pmat.izt.uam.mx/

LÍNEAS DE INVESTIGACIÓN

Teoría de anillos y módulos.
Teoría de conjuntos y lógica.
Geometría algebraica.
Geometría diferencial y Riemanniana.
Teoría de números.
Teoría de códigos y criptografía.
Análisis geométrico.
Física matemática.
Análisis diferencial.
Matemáticas discretas, combinatoria y gráficas.
Dinámica de fluidos computacional.
Resolución numérica de ecuaciones en derivadas parciales.
Métodos matemáticos en finanzas y economía.
Control y sistemas dinámicos.
Mecánica celeste, sistemas hamiltonianos y aplicaciones a la física.
Control, estabilidad y robustez de sistemas estocásticos.
Metodología estadística.
Estadística asintótica.
Topología de conjuntos, grupos topológicos y Cp-teoría.
Métodos geométricos en mecánica. Dinámica de vórtices. Mecánica celeste.

Maestría en Ciencias Matemáticas Aplicadas e Industriales (MACMAI)

mvmg@xanum.uam.mx
http://mcmai.izt.uam.mx

LÍNEAS DE INVESTIGACIÓN

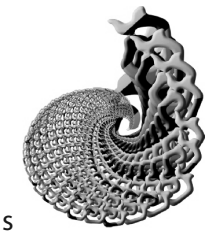
Códigos y Criptografía.
Control y Sistemas Dinámicos.
Combinatoria y Optimización.
Estadística.
Métodos Matemáticos en Finanzas.
Modelación y Simulación Computacional.

Casa abierta al tiempo
UNIVERSIDAD AUTÓNOMA METROPOLITANA
Unidad Iztapalapa

Contenido

Mixba'al

Revista Metropolitana de Matemáticas



Casa abierta al tiempo
UNIVERSIDAD AUTÓNOMA METROPOLITANA

A LOS AUTORES

Mixba'al es una publicación del Departamento de Matemáticas de la Universidad Autónoma Metropolitana, Unidad Iztapalapa. Está dirigida a la comunidad matemática.

Esta publicación está dedicada primordialmente a la divulgación, por lo que los artículos que se presenten deberán ser accesibles a estudiantes de posgrado y/o licenciatura versados en el tema. Los trabajos pueden ser sobre cualquier tópico de las matemáticas; por ejemplo, demostraciones nuevas de resultados conocidos, artículos panorámicos sobre un área de investigación, la presentación de una visión distinta de algún tema vinculado con la docencia, notas de cursos avanzados, aplicaciones de las matemáticas, historia y filosofía de las matemáticas y aspectos lúdicos de las mismas, entre otros

Los trabajos sometidos deben estar escritos en español, aunque en casos excepcionales podrán aceptarse artículos en inglés. El comité editorial tiene la responsabilidad de cuidar la calidad de la revista, tanto en su contenido como en su presentación, de acuerdo a los lineamientos, tipografía y corrección de lenguaje (ortografía, estilo, etcétera). Asimismo, el comité editorial decidirá si el trabajo es acorde a la línea editorial de la revista, y en caso de que así sea, lo enviara a arbitraje, sin excepción.

La versión preliminar de los trabajos sometidos a la revista deberá enviarse en formato pdf. al correo electrónico mixbaal2009@gmail.com. Puesto que la presentación final de los trabajos se hará en Latex2ε, aquellos autores cuyos trabajos sean aceptados, deberán enviarlos, para su publicación final, con el formato y macros que la revista les proporcionará. Las fotografías o gráficos que acompañen al texto deberán ser enviados, por separado, en formao pdf con la calidad y resolución adecuados para una buena reproducción impresa, además deberán contar con los correspondientes derechos de autor. Se recomienda que la extensión de los trabajos no exceda de 20 páginas.

Gustavo Izquierdo Buenrostro
Coordinador

Presentación

Mixba'al es una revista de divulgación en matemáticas en el sentido más amplio, concebida con el propósito de apoyar la comunicación entre la comunidad matemática de habla hispana.

El primer artículo de este número es un trabajo de Aura Carina Márquez Martínez y Roberto Quezada sobre el espectro de Gelfand de matrices circulantes.

El segundo artículo es una colaboración de Karla Adriana Ortega Gallegos y Gustavo Izquierdo sobre algunos hechos histórico de las funciones seno y coseno .

La intención es continuar con este formato y la revista invita a someter contribuciones de esta índole en el idioma español, aunque ocasionalmente pueden aceptarse contribuciones en inglés. Inicialmente se publicará al menos un número al año.

Toda comunicación debe ser dirigida al comité editorial, al correo electrónico: mixbaal2009@gmail.com.

Mixba'al
Revista Metropolitana de Matateáticas
No. 1, Vol. X, Julio de 2019, 7–19

NÚCLEOS EN DIGRÁFICAS CIRCULANTES, UN PROBLEMA ABIERTO DE TEORÍA DE GRÁFICAS

MARIANA LADRÓN DE GUEVARA FUENTES

Resumen. En este artículo se analizará el problema de caracterizar las digráficas circulantes que tienen núcleo; un problema abierto de teoría de gráficas. Se dará una caracterización para una familia infinita de digráficas circulantes usando para su demostración algunos resultados la teoría aditiva de números y se establece una conjetura para motivar la investigación en este campo.

1. Introducción

La teoría de gráficas tiene aplicaciones en muchas áreas, no sólo en las matemáticas puras y aplicadas, también en otras ciencias: química, física, ciencias sociales, informática, etc. Muchas estructuras pueden ser representadas mediante una gráfica: relaciones entre personas, redes de telecomunicación, circuitos eléctricos unidos por puentes, enlaces entre moléculas o partículas, etc. Para representar una relación entre los elementos de cualquier conjunto finito de objetos, siempre podemos usar una (di)gráfica. Los elementos se representan por vértices y las relaciones entre ellos se dan mediante aristas (en gráficas), arcos o flechas (en el caso de las digráficas).

En matemáticas, al trabajar con conjuntos, es usual querer encontrar un subconjunto, relativamente pequeño, que nos revele información del conjunto total. En teoría de gráficas, el núcleo de una digráfica (ver pág.6), es un subconjunto de los vértices que muestra propiedades importantes de la gráfica en cuestión y nos permite ver cómo se comporta. Es por esto que encontrar el núcleo de una gráfica dirigida o digráfica, se ha hecho un objeto de estudio para muchos matemáticos en diversas partes del mundo, y se han obtenido grandes avances que se pueden apreciar en múltiples artículos (ver [17], [4], [5], [6], [12], [13]). La idea de núcleos fue introducida por primera vez por John von Neumann y Oskar Morgenstern en 1944 [16], como una generalización de las SOLUCIONES-NM, un concepto que se usó para resolver un tipo de problemas de teoría de juegos aplicada a la economía. Se define el núcleo desde esta perspectiva para describir la victoria en un juego posicional entre dos personas (ver [6]). Von Neumann y Morgenstern también probaron que en una digráfica acíclica, existe un único núcleo y además puede obtenerse en tiempo lineal [6]. De aquí, se comenzaron a ver aplicaciones para obtener las soluciones en otros tipos de juegos, como los "juegos sin retorno"; que son una generalización de los juegos tipo NIM (un juego de estrategia entre dos personas, en el que intercaladamente, cada persona debe ir quitando objetos de entre dos montones y gana aquél que se queda sin objetos o con un objeto), en los cuales es posible encontrar un núcleo en tiempo polinomial, así lo probaron Jack Edmonds y Vladimir Gurvich [11]. También se han visto aplicaciones en áreas como lógica, inteligencia artificial, teoría de gráficas y análisis combinatorio [3], [8].

En general, el problema de encontrar un núcleo en una gráfica es un problema del que se sabe relativamente poco, pese a su extensa investigación. Hasta ahora, se ha demostrado, por ejemplo, que probar la existencia de un núcleo, en una digráfica en

2010 *Mathematics Subject Classification.* MSC 2000: 5C20, 11B25.
Palabras clave. Teoría de Gráficas; Teoría Aditiva de Números; Núcleos.

general con un número finito de vértices, es un problema NP-completo [1] [8]. También se sabe que todos los ciclos dirigidos de longitud par y la mayoría de los torneos no tienen núcleo [4] [2]. Además, una gráfica finita cuyos ciclos sean todos de longitud impar, tiene núcleo [19].

En el presente artículo se estudia el problema de caracterizar a las digráficas circulantes que tienen núcleo. Es un problema NP-completo sin resolver, propuesto en el libro de J. Bang-Jensen and G. Gutin [2]. Transformaremos este problema de teoría de digráficas a uno más simple de teoría aditiva de números, para ser abordado desde esta perspectiva. Se dará en primer lugar, un panorama preliminar acompañado de algunos ejemplos que familiarizarán al lector con el problema. Se abordarán los elementos necesarios para ver el problema como un problema de teoría aditiva de números, la cual se usará para probar una caracterización para una familia infinita de digráficas circulantes.

Las digráficas circulantes tienen una fuerte aplicación en el área de informática. En la computadora ILLIAC IV, por ejemplo, el arreglo PE (que consiste de una CPU y una memoria local), puede funcionar como una digráfica circulante. Cada PE de la red ILLIAC IV está contectado a un número fijo de otras PE's. Cada nodo i está conectado con los nodos $i \pm 1$ y $i \pm s$ módulo n [20]. La llamada "memoria circular" tiene también esta estructura. En el diseño e implementación de redes de área local, es común que se use la estructura de un ciclo dirigido para que la transferencia de información llegue a todos los nodos. Esta estructura es "económica" y fácil de manejar, por su simplicidad y simetría. Sin embargo, por su débil conexidad, es susceptible a fallos. Dado que las digráficas circulantes, además de ser simétricas y regulares, son siempre fuertemente conexas, resultan ser más adecuadas para este tipo de redes.

2. Preliminares

2.1. Teoría aditiva de números. La teoría aditiva de números es el estudio de la suma o sustracción (ver (ec1), (ec2)) entre conjuntos finitos de enteros, extendiendo su análisis a grupos abelianos y semigrupos conmutativos. La primera aplicación que se conoce de la teoría aditiva de números, fuera del campo de las matemáticas teóricas, fue en ingeniería eléctrica en 1945, para resolver el siguiente problema: Se tiene una resistencia que debe ser siempre de 30 ohms. Esta resistencia está compuesta por un conjunto de puntos fijos de contacto, tales que cada resistencia integral de $1, 2, 3, \ldots, 30$ ohms puede ser obtenida conectando dos puntos fijos de contacto. Se usó la teoría aditiva de números para obtener el menor número posible de puntos fijos que puedan realizar esta tarea (ver [7]).

En la teoría aditiva de números se examinan dos tipos de problemas: directos e indirectos. En los primeros, el objetivo es conocer el comportamiento del conjunto que resulta de sumar dos o más conjuntos, conociendo propiedades de los sumandos que lo componen. Mientras que en el segundo tipo de problemas, se extraen propiedades de los conjuntos que componen un conjunto suma, conociendo la estructura del mismo.

[1] En teoría de la complejidad computacional, NP es el acrónimo en inglés de nondeterministic polynomial time ("tiempo polinomial no determinista"). Es el conjunto de problemas que pueden ser resueltos en tiempo polinómico por una máquina de Turing no determinista.
Un problema de decisión C es NP-completo si:

1. C está contenido en el conjunto NP, y
2. Todo problema de NP es reducible a C en tiempo polinomial.

Sea $h \geq 2$, y sean $A_1, A_2, \ldots, A_h$ conjuntos de enteros. Se define el **conjunto suma** como

$$A_1 + A_2 + \ldots + A_h = \{a_1 + a_2 + \ldots + a_h \ : \ a_i \in A_i \text{ para todo } i = 1, 2, \ldots, h\}. \tag{1}$$

Denotamos la cardinalidad de A como $|A|$. Sean $A, B \subseteq \mathbb{Z}$, entonces el **conjunto resta** se define como

$$A - B = \{a - b \ : \ a \in A \text{ y } b \in B\}. \tag{2}$$

Para cada $c \in \mathbb{Z}$, se definen los siguientes conjuntos

$$\begin{aligned} c + A = \{c\} + A = \{c + a \in : \ a \in A\}, \\ c - A = \{c\} - A = \{c - a \in : \ a \in A\}. \end{aligned} \tag{3}$$

Sea $A \subseteq \mathbb{Z}$ cualquier conjunto, decimos que A es **libre de sumas** (*sum free*) si

$$(A + A) \cap A = \emptyset. \tag{4}$$

Sea G un conjunto y $M \subseteq G$. Si M es libre se sumas y para todo conjunto $B \subseteq G$ que sea libre se sumas se cumple que $|B| \leq |M|$, entonces se dice que M es **libre de sumas maximal**.

Para cualquier conjunto A, denotaremos a su complemento con $\overline{A}$.

2.2. Teoría de gráficas. Una **digráfica** o gráfica dirigida D es un par ordenado $(V(D), A(D))$, donde $V(D) \subseteq \mathbb{N}$ es el conjunto de **vértices**, y $A(D) \subseteq V(D) \times V(D)$ es el conjunto de **arcos o flechas**. Decimos que un par ordenado (u, v) está en $A(D)$, si y solo si, existe una flecha que va de u a v, dicho de otro modo

$$(u, v) \in A(D) \iff u \to v. \tag{5}$$

Dada una flecha (u, v), al primer vértice u lo llamaremos **origen** y al segundo v **destino**; también se puede decir que "u llega a v", o que "v sale de u". Sean $u, v \in V(D)$, entonces u y v son **adyacentes** si alguna, (u, v) o (v, u), es una flecha en D.

Para una digráfica D y para cualquier $v \in V(D)$ se definen los conjuntos

$$N_D^+(v) = \{u \in V(D) \backslash \{v\} \ : \ (v, u) \in A(D)\} \tag{6}$$

y

$$N_D^-(v) = \{u \in V(D) \backslash \{v\} \ : \ (u, v) \in A(D)\}, \tag{7}$$

a los que llamaremos **exvecindad** (todos lo vértices de la gráfica que salen de v) e **invecindad** (todos lo vértices de la gráfica que llegan a v) de v, respectivamente. Se define la **vecindad de** v como

$$N_D(v) = N_D^+(v) \bigcup N_D^-(v). \tag{8}$$

Se dice que una digráfica G es **k-regular** si para todo $v \in (V(J))$, se cumple que $|N_D^+(v)| = |N_D^-(v)| = k$.

Para cualquier entero $n \geq 2$ y cualquier conjunto $J \subseteq \{1, 2, \ldots, n-1\}$, una digráfica cuyo conjunto de vértices es isomorfo al de clases laterales $\mathbb{Z}_n$ (es decir, que tiene n vértices etiquetados con representantes de 0 a $n-1$), decimos que es una **digráfica circulante** $\overrightarrow{C}_n(J)$ si toda flecha $a \to b$ está en $A(\overrightarrow{C}_n(J))$ si y solo si $b - a$ (mod n) es un elemento de J. Dicho de otro modo, una digráfica es circulante si su conjunto de arcos o flechas es de la forma

$$A(\overrightarrow{C}_n(J)) = \{i \to i + j(\text{mod n}) \ : \ 0 \leq i \leq n-1, j \in J\}. \tag{9}$$

Al conjunto J se le llama **conjunto de saltos** *(jumps)*, porque denota la cantidad de saltos que se dan de un vértice a los siguientes vértices adyacentes a él.

Cabe mencionar que para fines de este artículo, en nuestras digráficas circulantes se excluyen todas aquellas digráficas con lazos o flechas simétricas, esto es;

1. Para todo $u \in V(\overrightarrow{C}_n(J))$, $(u,u) \notin A(\overrightarrow{C}_n(J))$.
2. Para todo $u, v \in V(\overrightarrow{C}_n(J))$, si $(u,v) \in A(\overrightarrow{C}_n(J))$, entonces $(v,u) \notin A(\overrightarrow{C}_n(J))$.

Ejemplo 1. La digráfica circulante $\overrightarrow{C}_{15}(3,5)$ es la digráfica de 15 vértices y saltos 3 y 5. Ver Figura 1.

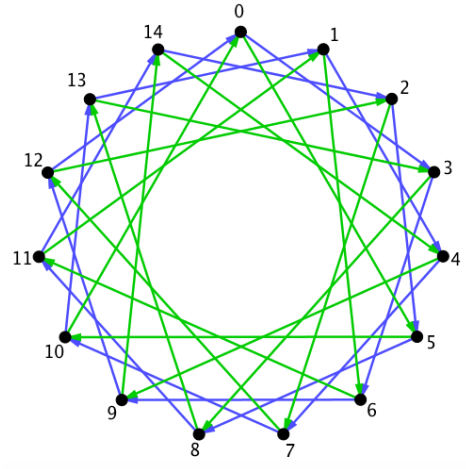


FIGURA 1. Gráfica $\vec{C}_{15}(3,5)$. Las flechas en azul indican el salto 3 y las que están en verde el salto 5.

Como $J = \{j_1, j_2, \ldots, j_k\}$, entonces para cada $i \in V(\overrightarrow{C}_n(J)) = \mathbb{Z}_n$

$$N_G^+(i) = \{i + j_t \ : \ 1 \leq t \leq k\} \quad \text{y} \quad N_G^-(i) = \{i - j_t \ : \ 1 \leq t \leq k\}. \tag{10}$$

Se sigue que $|N_G^+(i)| = |N_G^-(i)| = |J|$.

Por lo anterior, podemos decir que toda digráfica circulante $\overrightarrow{C}_n(J)$ es $|J|-regular$.

Ejemplo 2. A la gráfica $\overrightarrow{C}_{15}(3,5,8)$, le corresponde el conjunto de saltos $J = \{3,5,8\}$. Por lo tanto es 3-*regular*, porque de cada vértice en la gráfica salen tres flechas, la misma cantidad de flechas que llegan a él. Esto es, para todo $v \in V(\overrightarrow{C}_{15}(3,5,8))$, $|N_G^+(v)| = |N_G^-(v)| = 3$.

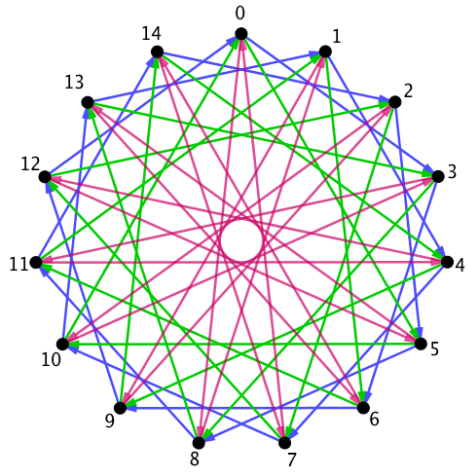


FIGURA 2. Gráfica $\vec{C}_{15}(3,5,8)$. . Las flechas en azul indican el salto 3 y las que están en verde el salto 5 y las de rosa corresponden al salto 8.

Sea G una gráfica y sea $K \subset V(G)$. Se dice que K es un **núcleo** de G si

1. Es **independiente**; si para cualesquiera $u, v \in K$, entonces, $(u,v),(v,u) \notin A(G)$.
2. Es **absorbente**; si para toda $x \in V(G)\backslash K$, existe $v \in K$, tal que $(x,v) \in A(G)$.

Dicho de otro modo, K es núcleo si no tiene pares de vértices adyacentes entre sí (independencia) y si cada elemento de su complemento "llega a" algún elemento de K (absorbencia).

Ejemplo 3. Sea $\overrightarrow{C}_{10}(1,4)$. Si tomamos $K = \{1,3,6,8\}$, observamos que K es independiente y absorbente. Por lo tanto, K es un núcleo de $\overrightarrow{C}_{10}(1,4)$. Ver Figura 3.

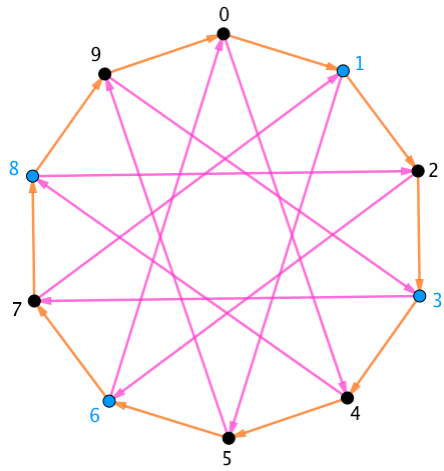


FIGURA 3. Gráfica $\vec{C}_{10}(1,4)$. Las flechas en amarillo indican el salto 1 y las que están en rosa el salto 4.

PROPOSICIÓN 1. *Sea $J \subseteq \mathbb{Z}_n \backslash \{0\}$. Si $n \leq 2|J|+1$, entonces $\overrightarrow{C}_n(J)$ no tiene conjuntos absorbentes.*

Demostración. Tener una gráfica $|J|-regular$ significa que para todo $x \in V(\overrightarrow{C}_n(J))$, $|J|$ elementos diferentes salen de x y $|J|$ elementos diferentes llegan a x; es decir, x es adyacente a $2|J|$ vértices distintos de $V(\overrightarrow{C}_n(J))$. Por lo tanto, tiene que haber al menos $|J|+1$ vértices además de x, para que pueda existir un vértice no adyacente a él. □

Como se ha mencionado anteriormente, el problema que se quiere resolver es el de caracterizar las digráficas circulantes que tienen núcleo. Sin embargo, aún con la poca teoría que se tiene hasta ahora, es posible caracterizar familias específicas de digráficas circulantes. La siguiente proposición es ejemplo de una caracterización de este tipo.

PROPOSICIÓN 2. *La digráfica $\overrightarrow{C}_n(1,2)$ tiene núcleo K, si y sólo si, $3 \mid n$ y $K = 3\mathbb{Z}_n$.*

Demostración. Por la Proposición 4, podemos asumir que $n \geq 6$. Supongamos por contradicción que $\overrightarrow{C}_n(1,2)$ tiene núcleo N pero que $n \nmid 3$. Entonces $n = 3r+1$ ó $n = 3r+2$ para algún $r \in \mathbb{N}$. Sea $a \in N$, por definición de $\overrightarrow{C}_n(1,2)$, a es adyacente a los dos vértices $a+1$ y $a+2$, y sería independiente al vértice $a+3$. De esto podemos afirmar que al menos uno de cada tres vértices de $\overrightarrow{C}_n(1,2)$ está contenido en N. Se sigue que

$$|N| \leq \lfloor\ frac|G|3\rfloor = \lfloor \frac{n}{3} \rfloor. \tag{11}$$

Entonces

$$|N| = r, \tag{12}$$

y

$$|\overline{N}| = 2r+1 \quad \text{ó} \quad |\overline{N}| = 2r+2. \tag{13}$$

Sea R el conjunto de todos los elementos de $V(\overrightarrow{C}_n(1,2))$ que son absorbidos por N. Es fácil verificar que N y R son disjuntos ya que N es independiente, y al ser $\overrightarrow{C}_n(1,2)$

un gráfica $2-regular$, se tiene que

$$|R| = |\{x \in \overline{N} \ : \ (x,a) \in A(\overrightarrow{C}_n(1,2)); a \in N\}| \leq 2r < 2r+i, \tag{14}$$

para toda $i \in \mathbb{N}$. [2] Así, $\overline{N} \neq R$. Por lo tanto, N no es núcleo. Se sigue que $n = 3r$, para algún $r \in \mathbb{N}$. Como todo lo anterior es válido para todo $a \in N$, se tiene que $a + 3(i) \in N$ para toda $i \in \{0, 1, \ldots, r\}$. Por lo tanto, los conjuntos N y $\{a + 3(i) \ : \ a \in N; 1 \leq i \leq r\}$ son isomorfos, *i. e.,*

$$N \cong \{a + 3(i) \ : \ a \in N; 1 \leq i \leq r\} \cong \{3(i) \ : \ 1 \leq i \leq r\} = 3\mathbb{Z}_n. \tag{15}$$

Supongamos ahora que $n = 3r$ para algún $r \in \mathbb{N}$. Si $N \cong 3Z_n$, entonces $|K| = r$. Como N es subgrupo de Z_n y $J = \{1, 2\}$, se sigue que la suma o diferencia entre cualesquiera dos elementos de N no estaría en J, por lo que N es un conjunto independiente. Así

$$|R| = |\{a \in \overline{N} \ : \ (a,x) \in A(V(\overrightarrow{C}_n(1,2))); x \in N\}| = 2r. \tag{16}$$

Recordemos que R y N son disjuntos. Se sigue que

$$|N| + |R| = r + 2r = 3r = n. \tag{17}$$

En consecuencia $R = \overline{N}$, es decir, N es absorbente. Por lo tanto, N es núcleo.

□

El siguiente ejemplo ilustra la proposición anterior.

Ejemplo 4. Sea la digráfica $\vec{C}_9(1,2)$. Si tomamos el conjnto $K = \{0, 3, 6\}$ podemos observar que es un núcleo (ver Figura 4). Por la acción del grupo $\mathbb{Z}_n$ sobre el conjunto de vértices de la gráfica [3], los conjuntos $\{0+i, 3+i, 6+i\}$ con $i \in \{1, 2\}$, también son núcleos de $\vec{C}_9(1,2)$, pero son isomorfos a K.

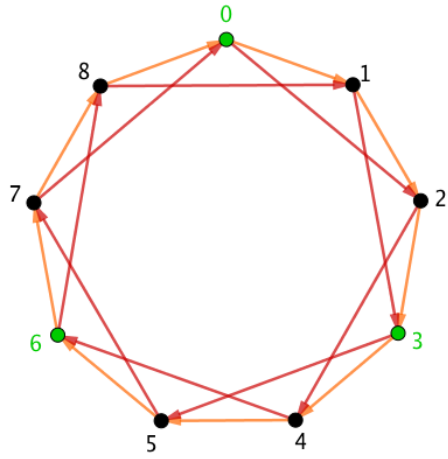


FIGURA 4. Gráfica $\vec{C}_9(1,2)$: los vértices en verde representan el conjunto K

Ya vimos que con poca teoría se pueden caracterizar algunas familias específicas de digráficas circulantes, pero la herramienta que nos va a ayudar a dar un acercamiento a una caracterización más general es la teoría aditiva de los números. El siguiente lema

[2] En este artículo $0 \notin \mathbb{N}$

[3] El grupo $\mathbb{Z}_n$ actúa sobre $V(\overrightarrow{C}_n(J))$ mediante la aplicación

$$\begin{aligned} \phi : (\mathbb{Z}_n \times V(\overrightarrow{C}_n(J))) &\longrightarrow V(\overrightarrow{C}_n(J)) \\ (i,x) &\longrightarrow i + x \end{aligned} \tag{18}$$

es el puente que nos llevará del mundo de la teoría de gráficas al mundo de la teoría aditiva de los números y viceversa.

LEMA 3. *Sean $J \subseteq \mathbb{Z}_n \backslash \{0\}$ finito y $n > 2|J| + 1$. Sea $\overrightarrow{C}_n(J)$ una digráfica circulante. Entonces*

1. *$K \subset V(\overrightarrow{C}_n(J))$ es independiente $\iff$ $(K + J) \cap K = \emptyset$.*
2. *$N \subset V(\overrightarrow{C}_n(J))$ es absorbente $\iff$ $\overline{N} = N - J$.*

Demostración. 1. Sea $k \in K$. Por definición de $\overrightarrow{C}_n(J)$, $(k, k + j) \in A(\overrightarrow{C}_n(J))$. Ya que K es independiente, $k + j \notin K$ para todo $j \in J$. Por lo tanto, $(K + J) \cap K = \emptyset$.

2. Como N absorbente, $x \in \overline{N}$ si y solo si existe $k \in N$ tal que $(x, k) \in A(\overrightarrow{C}_n(J))$ y por la definición de flecha en una digráfica circulante, eso pasa si y solo si, $k = x + j$, para alguna $j \in J$. Así,

$$k = x + j \iff x = k - j \iff x \in N - J \iff \overline{N} = N - J. \tag{19}$$

□

El siguiente teorema, aunque es muy simple, es una herramienta muy útil para la caracterización de familias más generales de digráficas $\overrightarrow{C}_n(J)$ con núcleos. Este nos permite simplificar la búsqueda de núcleos reduciendo el número de propiedades que se le debe pedir al conjunto. Para saber si una digráfica circulante tiene núcleo, basta con saber si su conjunto de vértices contiene un conjunto absorbente. Veremos primero el Lema de Vosper, un lema previo al teorema que nos ayudará con su demostración.

LEMA 4 (Lema de Vosper). *Sea G cualquier grupo abeliano, y sean $A, B, C \subseteq G$ finitos y no vacíos, entonces*

$$(A + B) \cap C = \emptyset \iff A \cap (C - B) = \emptyset. \tag{20}$$

Demostración. Si, $A \cap (C - B) \neq \emptyset$, entonces existe x tal que $x \in A$ y $x \in C - B$, sí y sólo si existen $a \in A$, $b \in B$ y $c \in C$, tales que $x = a$ y $x = c - b$. Pero

$$a = c - b \iff a + b = c \iff c \in A + B \cap C \iff (A + B) \cap C \neq \emptyset \tag{21}$$

□

TEOREMA 5. *Sea G un grupo abeliano finito, entonces para cualesquiera $K, J \subset G$ no vacíos,*

$$\overline{K} = K - J \implies (K + J) \cap K = \emptyset. \tag{22}$$

Demostración. Como

$$\begin{aligned} \overline{K} = K - J &\implies K - J \subseteq \overline{K} \\ &\implies (K - J) \cap K = \emptyset. \end{aligned} \tag{23}$$

Aplicando el Lema 4, se concluye que

$$(K + J) \cap K = \emptyset. \tag{24}$$

□

3. RESULTADOS

A continuación, usaremos los resultados de la sección anterior para establecer las condiciones que nos permitan caracterizar una familia de digráficas circulantes más general. Se probará una condición suficiente para que una digráfica circulante, con saltos $J = \{1, k\}$, tenga núcleo.

TEOREMA 6. *Para cualquier digráfica circulante $\overrightarrow{C}_n(1, k)$ se cumplen las siguientes afirmaciones:*

1. *Si k es par, entonces $\overrightarrow{C}_n(1, k)$ tiene núcleo si $(k + 1) \mid n$.*

2. *Si k es impar, entonces $\overrightarrow{C}_n(1,k)$ tiene núcleo si n es par.*

Demostración. 1. Como k es par y $(k+1)|n$, podemos escribir a k y n como $k=2r$ y $n=(k+1)t$ con $r,t\in\mathbb{Z}^+$. Para cada entero $q\in[0,t-1]$, definamos

$$\begin{aligned} H_q &= \{(k+1)q+p\,:\,2\mid p\ ,\ 0\le p\le k-2\} \\ &= \left\{(k+1)q+2s\ :\ 0\le s\le \frac{k-2}{2}\right\} \end{aligned} \tag{25}$$

y

$$H=\bigcup_{q=0}^{t-1} H_q. \tag{26}$$

Sea $H_k=\{(k+1)q+k : 0\le q\le t-1\}$. Afirmamos que

$$\overline{H}=(H+1)\cup H_k. \tag{27}$$

En efecto, observemos que por construcción, para toda $q\in[0,t-1]$, $H_q\ \subseteq\ \{\overline{2i}\ :\ 0\le i\le r-1\}\ \subseteq\ \mathbb{Z}_{k+1}$. Además, sabemos que

$$\begin{aligned} H+1 &= \bigcup_{q=0}^{t-1} H_q+1 \\ &= \bigcup_{q=0}^{t-1}(H_q+1) \\ &= \bigcup_{q=0}^{t-1}\left\{(k+1)q+(2s+1) : 0\le s\le \frac{k-2}{2}\right\}. \end{aligned} \tag{28}$$

Así, $H+1\subseteq\{\overline{2i+1}\ :\ 0\le i\le r-1\}\in\mathbb{Z}_{k+1}$. Por último,

$$H_k=\{(k+1)q+k : 0\le q\le t-1\}\subseteq\overline{k}\in\mathbb{Z}_{k+1}. \tag{29}$$

Por lo tanto, los conjuntos $H, H+1$ y H_k son disjuntos dos a dos. Finalmente, verificaremos que su unión es $\mathbb{Z}_n$. Por la definición de los conjuntos, podemos calcular las cardinalidades de cada conjunto

$$\begin{aligned} |H| &= \sum_{q=0}^{t-1}|H_q| = \sum_{q=0}^{t-1}\big(\frac{k-2}{2}+1\big) = t\frac{k}{2}, \\ |H+1| &= |H| = t\frac{k}{2}, \\ |H_k| &= t. \end{aligned} \tag{30}$$

Sumando las cardinalidades tenemos que

$$|H|+|H+1|+|H_k| = 2\big(t\frac{k}{2}\big)+t = t(k+1)=n. \tag{31}$$

Ahora probaremos que, para $J=\{1,k\}$, se cumple

$$\overline{H}=H-J, \tag{32}$$

lo cual sucede si y solo si $\overline{H}\subseteq H-J\quad y\quad H-J\subseteq\overline{H}$

$\subseteq$) Sea $x\in\overline{H}$. Entonces $x\in H+1$ ó $x\in H_k$.

- Si $x\in H+1$, entonces existen $q\in[0,t-1]$ y s par con $0\le s\le k-2$, tales que

$$x=(k+1)q+s+1 \qquad \text{con} \qquad s\le k-2. \tag{33}$$

Si $s<k-2$ se sigue que $s\le k-4$, así podemos expresar a s como $s=2s'$ con $s'<k-4$. Entonces

$$\begin{aligned} x &= (k+1)q+2s'+1 \\ &= (k+1)q+(2s'+2)+1-2 = (k+1)q+2(s'+1)-1. \end{aligned} \tag{34}$$

Por lo tanto, $x \in H - \{1\} \subseteq H - J$. Si $s = k - 2$, entonces

$$x = (k+1)q + s + 1 = kq + q + (k-2) + 1 + k - k = (q+1)(k+1) + (k-2) - k, \tag{35}$$

con $q \leq t - 1$ entonces $q + 1 \leq t$. Pero si $q + 1 = t$. Entonces

$$(q+1)(k+1) = t(k+1) = 0. \tag{36}$$

Así $q + 1 \leq t - 1$ y por lo tanto, $x \in H - \{k\} \subseteq H - J$.

- Si $x \in H_k$, entonces para alguna $q \in [0, t-1]$

$$\begin{aligned} x &= (k+1)q + k \\ &= k(q+1) + (q+1) - 1 = (k+1)(q+1) - 1 \in H - 1 \subseteq H - J. \end{aligned} \tag{37}$$

Por lo tanto, $\overline{H} \subseteq H - J$.

$\supseteq$) Procedemos análogamente para esta contención. Sea $y \in H - J$. Entonces tenemos que $y \in H - \{1\}$ ó $y \in H - \{k\}$.

- Si $y \in H - \{1\}$, entonces existen $p \in [0, t-1]$ y $s \in [0, r-1]$ tales que

$$\begin{aligned} y &= (k+1)q + 2s - 1 \\ &= (k+1)q + 2s - 1 + 2 - 2 \\ &= (k+1)q + 2(s-1) + 1 \in H + 1 \subseteq \overline{H}. \end{aligned} \tag{38}$$

- Si $y \in H - \{k\}$, entonces y es de la forma $y = (k+1)q + 2s - k$. Si $s = 0$, entonces $y \in H_k \subset \overline{H}$. Si $s \neq 0$, entonces

$$y = kq + q + 2s - k + 1 - 1 = (k+1)(q-1) + 2s + 1 \in H + 1 \subseteq \overline{H}. \tag{39}$$

En ambos casos $y \in \overline{H}$. Así $H - J \subseteq \overline{H}$. Por lo tanto, $\overline{H} = H - J$.

2. Sabemos que n es par y k es impar. Definamos $N = \{2, 4, \ldots, n\}$. Afirmamos que N es núcleo. En efecto, ya que k es impar y debido a que cualquier $x \in \overline{N}$ es impar, entonces $x + j \in N$, para todo $j \in J = \{1, k\}$. Así $(x, x+j) \in A(\overrightarrow{C}_n(J))$ y por lo tanto N es absorbente y en consecuencia independiente. Por lo tanto, N es núcleo de $\overrightarrow{C}_n(J)$.

□

En el siguiente ejemplo, podemos observar cómo funciona el conjunto H_q propuesto para demostrar el resultado anterior.

Ejemplo 5. En la gráfica $\vec{C}_{15}(1, 4)$, el conjunto $H_q = \{0, 2, 5, 7, 10, 12\}$ es núcleo. (Ver Figura 5).

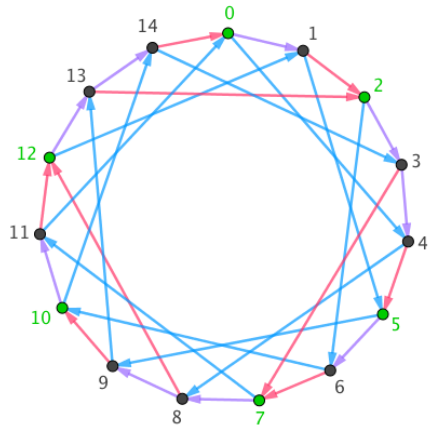


FIGURA 5. Gráfica $\vec{C}_{15}(1,4)$. Los vértices en verde son un núcleo. Las flechas en rosa indican cómo el complemento es absorbido por el núcleo, mientras que las flechas en color lila indican los saltos 1 y las azules el salto 4.

La afirmación inversa del Caso 2 del teorema anterior (para una k chica), es falsa. Un contraejemplo es la digráfica $\overrightarrow{C}_n(1,5)$, la cual no sólo tiene núcleo cuando n es par, también tiene núcleo al ser n un múltiplo de 3. Para probar esta afirmación, sea $n = 3t$ para alguna $t \in \mathbb{Z}^+$, y tomemos el conjunto $K = \{0, 3, \ldots, 3t\}$. Entonces toda $x \in \overline{K}$ es de la forma

$$x = 3r + i \quad \text{con} \quad r \in [0, t-1] \quad \text{y} \quad r \in \{1, 2\}. \tag{40}$$

Si $x = 3r + 1$, entonces, $x + 5 = 3r + 6 = 3(r + 2) \in K$. Si $x = 3r + 2$, entonces, $x + 1 = 3r + 3 = 3(r + 1) \in K$. Como $A(\overrightarrow{C}_n(1,5)) = \{(x, x + j) \ : \ j \in J = \{1, 5\}\}$, se sigue que K es absorbente y por lo tanto, núcleo.

Ejemplo 6. Observamos que en la gráfica $\overrightarrow{C}_{15}(1,5)$, el conjunto $K = \{0, 3, 6, 9, 12\} \subset V(\overrightarrow{C}_{15}(1,5))$ es un núcleo, así mismo, el conjunto $N = \{0, 2, 4, 6, 8, 10, 12, 14\} \subset V(\overrightarrow{C}_n(1,5))$ es otro núcleo no isomorfo a K. Ver Figura 6.

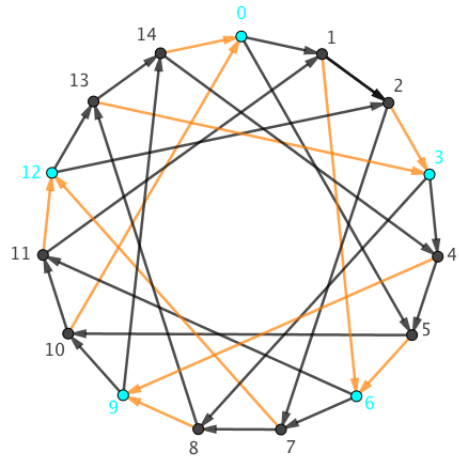


FIGURA 6. Gráfica $\vec{C}_{15}(1,5)$. Los puntos en verde forman un núcleo, mientras que las flechas en naranja indican cómo absorben al complemento.

El estudio de núcleos en digráfica circulantes es reciente y se tienen pocos resultados al respecto. Estos son algunos de ellos [13]:

1. Sea $J \subseteq \{1, 2, \ldots, n-1\}$ tal que $n-j \in J$ para toda $j \in J$. Entonces la digráfica circulante $\overrightarrow{C}_n(J)$ tiene núcleo.
2. Si n es impar y si J es un subconjunto de números pares en $\{1, 2, \ldots, n-1\}$. Entonces $\overrightarrow{C}_n(J)$, tiene núcleo.
3. Si n es par y si S_1 y S_2 son los conjuntos de todos los números pares y todos los números impares en $\{1, 2, \ldots, n-1\}$, respectivamente. Entonces ambos S_1 y S_2 no tienen núcleo.
4. Si $i + j \neq n$, entonces la digráfica $\overrightarrow{C}_n(i, j)$ tiene núcleo.

Hasta ahora podemos afirmar que no todas las gráficas circulantes tienen núcleo, y las que tienen, no siempre es único (salvo isomorfismos). Por lo que se ha podido observar de repetidos ejemplos, hemos llegado a la siguiente conjetura:

Conjetura: *Si una digráfica circulante tiene núcleo, entonces existe un conjunto independiente maximal que también es núcleo*

Debido a la variedad de resultados que ya existen sobre conjuntos libres de sumas maximales en $\mathbb{Z}_n$ y $\mathbb{F}_p$ (ver [21], [14], [22], [10], [18]), probar esta conjetura nos abriría la oportunidad de conocer las cardinalidades de una variedad mucho más amplia de digráficas circulantes, problema que creemos puede ser estudiado para un futuro proyecto de investigación.

4. Conclusión

El problema que se abordó es este artículo, podrá plantearse de manera muy simple, pero es amplio y complejo. Aunque se pudo obtener una condición suficiente para caracterizar las digráficas de la familia $\overrightarrow{C}_n(1, k)$ con núcleo, aún no se pudo establecer si la condición necesaria es cierta y para cuáles n hay excepciones. Y esta es sólo una pequeña familia de digráficas circulantes, recordemos que el problema es caracterizar cuáles digráficas circulantes $\overrightarrow{C}_n(J)$ con $J \subseteq \{1, 2, \ldots, n-1\}$ tienen núcleo, por lo que aún falta mucho que estudiar, investigar y analizar en este tema.

5. Agradecimientos

Quiero agradecer a mis profesores el Dr. Bernardo Llano y el Dr. Gabriel Bengochea porque gracias a sus enseñanzas, comentarios y su motivación, he podido realizar este artículo. Y extiendo el agradecimiento al árbitro anónimo, cuyos comentarios ayudaron a mejorar la calidad y presentación de este trabajo.

También quiero hacer un agradecimiento especial al Dr. Mario Pineda por su apoyo durante mi formación como Matemática y por su confianza al invitarme a formar parte de este proyecto.

Referencias

[1] A. Apartsin, E. Ferapontova, and V. Gurvich, *A circular graph - counter example to the Duchet kernel conjecture*, Discrete Math, 178 (1998), 229-231.

[2] J. Bang-Jensen, and G. Gutin, *Digraphs: Theory, Algorithms and Applications*, 2nd ed., Springer-Verlag, London, 2009.

[3] C. Berge, *Nouvelles extensions du noyau dâun graphe et ses applications en théorie des jeux*, Publ. Economé 6 (1977).

[4] C. Berge and P. Duchet, *Recent problems and results about kernels in directed graphs*, Discrete Math, 86 [1-3], (1990), 27-31.

[5] E. Boros, and V. Gurvich, *A corrected version of the Duchet kernel conjecture.* Discrete Mathematics, 179, (1998), 231-233.

[6] E.Boros, and V. Gurvich, *Perfect graphs, kernels, and cores of cooperative games*, Discrete Mathematics, 306, (2006), 2336-2354.
[7] A. Brauer, *A problem of Additive Number Theory and its application in Electrical Engineering*, Journal of the Mitchell Society, 61 [1/2], (1945), 55-66 .
[8] V. Chvàtal, *On the computational complexity of finding a kernel*, Centre de Recherches Mathematiques-Universite de Montreal, Report No. CRM-300, (1973).
[9] H. Davenport, *On the addition of residue clases.* Journal of the London Mathematical Society, s1-10, (1935), 30-32.
[10] P.H. Diananda, and H.P. Yap, *Maximal sum-free sets of elements of finite groups*, Proc. Japan Academy, 45 (1969), 1-5.
[11] J. Edmonds, and V. Gurvich. *Games of no return.* Turner Research Report. 4-2010.
[12] Galeana-Sánchez, B. Llano, and J. J. Montellano-Ballesteros. *k-colored kernels in semicomplete multipartite digraphs*, Discrete Applied Mathematics, 158 (2010), 461-466.
[13] R. Lakshmi, and S. Vidhyapriya. *Kernels in circulant digraphs*, Transactions on Combinatorics, 3 [2], 2014, 45-49.
[14] B. Llano, Notas personales.
[15] M. B. Nathanson, *Additive Number Theory. Inverse Problems and the Geometry of Sumsets, Garduate Texts in Mathematics*, Springer-Verlag, 165, 1996.
[16] J. von Neumann and O. Morgenstein, *Theory of games and economic behavior*, Princeton University Press. 1953.
[17] A. Ramoul, and M. Blidia. *A new generalization of kernels in digraphs*, Discrete Applied Mathematics, 217 [3], (2017), 673-684.
[18] A.H. Rhemtulla and A.P. Street. *Maximal sum-free sets in finite abelian p-groups*, Bulletin of the Australian Mathematical Society, 2 (1970), 289-297.
[19] M. Richardson, *Solutions of irreflexible relations*, Ann. Math., 58 (1953), 573-590.
[20] A. Survey, and J.C. Bermond, *Distributed Loop Computer Networks*, Journal of Parallel and Distributed Computig, 24 (1995), 2-10.
[21] A. G. Vosper, *The critical pairs of sumset of a gruop of prime order*, J. London Math. Soc. 31 (1956) 200-205.
[22] H.P. Yap, *Maximal sum-free sets on group elements*, Bull. Austral. Math. Soc., 4 (1971), 217-223.

Dirección de la autora:
Universidad Autónoma Metropolitana,
Unidad Iztapalapa,
División de Ciencias Básicas e Ingeniería,
Departamento de Matemáticas.
Av. San Rafael Atlixco 186, Col. Vicentina
Del. Iztapalapa, C.P. 09340 Ciudad de México
e-mail: `marladron.mat@xanum.uam.mx`

Mixba'al
Revista Metropolitana de Matateáticas
No. 1, Vol. X, Julio de 2019, 21–32

GRUPOS DE GALOIS DE POLINOMIOS IRREDUCIBLES DE GRADO 4 EN CARACTERÍSTICA DISTINTA DE 2

EDGAR GUTIÉRREZ SUÁREZ

RESUMEN. El objetivo de este trabajo es conocer de forma precisa el grupo de Galois de polinomios irreducibles de grado ≤ 4 y dar una clasificación detallada del grupo de Galois de un polinomio irreducible, separable de grado 4 en cualquier campo de característica distinta de 2. Se eliminará la ambigüedad que tradicionalmente se presenta en dos de los cinco posibles grupos de Galois en dicha clasificación en grado 4.

INTRODUCCIÓN

El objetivo central de este trabajo es usar la Teoría de Galois para clasificar el grupo de Galois G_f de un polinomio $f(x)$ irreducible o reducible de grado ≤ 4 en campos de caraterística $\neq 2$ ya que se sabe que $G_f \subseteq A_4$ si y solo sí la raíz del discriminante de $f(x)$ es un cuadrado en su campo base. Esto falla en característica 2 porque $-1 \equiv 1 \pmod 2$, lo cual implica que la raíz cuadrada del discriminante de cualquier polinomio queda invariante bajo la acción de cualquier $\sigma \in G_f$. Para polinomios de grado 2 o 3 la tarea es relativamente sencilla como se verá en su momento. El caso de estudio de polinomios de grado 4 es más interesante, nada trivial y está inspirado en los artículos [2] y [6].

Se sabe que el grupo de Galois de un polinomio irreducible, separable y de grado $n > 0$ es un subgrupo transitivo de S_n, en particular, en grado 4, los únicos subgrupos transitivos de S_4 son: el grupo cíclico $Z/4\mathbb{Z}$, el grupo diédrico D_8, el grupo de Klein V, el grupo alternante A_4 y el grupo simétrico S_4. Asímismo, se verá que en los últimos tres casos es relativamente fácil identificar cada grupo, sin embargo, en los casos cíclico y diédrico serán un poco más delicado distinguir G_f. En estos dos casos, se darán condiciones necesarias y suficientes para decidir cada caso.

Se verá que para determinar el grupo de Galois de un polinomio $f(x) \in K[x]$ irreducible de grado 4 se necesita asociarle un polinomio cúbico muy peculiar, mejor conocido como la resolvente cúbica de $f(x)$ y verficar si el discriminante de $f(x)$ es o no un cuadrado en K. También se verá que la resolvente tiene coeficientes en $K[x]$ y su campo de descomposición es subcampo del campo de descomposición de $f(x)$, así que su grupo de Galois es isomorfo a un grupo cociente de G_f, de manera que, conociendo la acción de G_f en las raíces de la resolvente, se obtiene información relevante acerca de G_f.

Finalmente, como aplicación de lo anterior, se estudiará la familia de polinomios irreducibles bicuadráticos $f(x) = x^4 + bx^2 + c$ que corresponden a la familia de campos de la forma $K = K(\sqrt{m}, \sqrt{n})$, con m, n enteros libres de cuadrados. Se verá que para esta familia de polinomios, G_f solo puede ser $Z/4\mathbb{Z}, D_8$ ó V.

1. GRUPO DE GALOIS Y PERMUTACIONES

Suponga que L es el campo de descomposición de un polinomio separable $f(x) \in K[x]$. Se escribirá G_f para indicar al grupo de Galois de $f(x)$.

Recuerde que un grupo G que actúa sobre un conjunto X se dice que la acción de G sobre X es transitiva si para $x, y \in X$, existe $g \in G$ tal que $g \cdot x = y$. En particular, si se considera el campo de descomposición $L = K(\alpha_1, \alpha_2, \ldots, \alpha_n)$ de un polinomio separable $f(x) \in K[x]$ de grado $n > 0$, entonces la acción transitiva de G_f sobre las raíces $\alpha_1, \alpha_2, \ldots, \alpha_n$ de $f(x)$ está dada por $\sigma(\alpha_i) = \alpha_{\sigma(i)}$, $\sigma \in G_f$.

2010 *Mathematics Subject Classification.* 13B0.
Palabras clave. Grupos de Galois, resultante, discriminante, irreducibilidad.

El siguiente teorema caracteriza al grupo de Galois de cualquier polinomio irreducible separable $f(x) \in K[x]$ de grado $n > 0$.

TEOREMA 1. *Sean $f(x) \in K[x]$ un polinomio separable de grado n, $\alpha_1, \ldots, \alpha_n$ las raíces de $f(x)$ y $L = K(\alpha_1, \ldots, \alpha_n)$ su campo de descomposición. Entonces $f(x)$ es irreducible en $K[x]$ si y solo si G_f es un subgrupo transitivo de S_n.*

Demostración. Vea [3], pág 134. □

Una consecuencia del Teorema anterior es el siguiente:

COROLARIO 2. *Sea L el campo de descomposición de un polinomio separable $f(x) \in K[x]$ de grado n. Si $f(x)$ es irreducible sobre K, entonces el subgrupo de S_n correspondiente al grupo de Galois de $f(x)$ tiene orden divisible por n.*

Se sabe de manera precisa que para el caso de un polinomio cuadrático irreducible y separable su grupo de Galois es S_2 pues es el único subgrupo transitivo de S_2. En el caso cúbico, considerando campos K de característica distinta de 2, de los resultados previos se sabe que su grupo de Galois es S_3 ó A_3. Para saber de manera precisa no solo el caso $n = 3$ sino también en el caso $n = 4$, se introduce la siguiente definición que nos es familiar en el caso $n = 2$.

DEFINICIÓN 3. *Sean K un campo tal que* Car$(K) \neq 2$, *$f(x) \in K[x]$ un polinomio mónico, separable de grado $n > 0$ y $\alpha_1, \alpha_2, \ldots, \alpha_n$ las raíces de $f(x)$. Se define el discriminante de $f(x)$ como $disc(f(x)) = \prod_{i<j}(\alpha_i - \alpha_j)^2$.*

Note que $disc(f(x))$ es un elemento de K pues es un polinomio simétrico en las raíces de $f(x) \in K[x]$. Más aún, $disc(f(x))$ se puede escribir en términos de los coeficientes de $f(x)$.

TEOREMA 4. *Sean K un campo de característica $\neq 2$, $f(x) \in K[x]$ separable y mónico (no necesariamente irreducible) de grado $n > 0$, $L = K(\alpha_1, \alpha_2, \ldots, \alpha_n)$ su campo de descomposición y G_f su grupo de Galois. Si $\Delta = disc(f(x))$, entonces $G_f \subseteq A_n$ si y solo si $\sqrt{\Delta} \in K$.*

Demostración. Ver [3], pág 168. □

Se sabe de la teoría de grupos que si H y N son subgrupos de G y $N \triangleleft G$, entonces $H \cap N \triangleleft H$. En particular, si $f(x) \in K[x]$ separable y G_f su grupo de Galois, si $H = G_f$, $N = A_n$, $G = S_n$ resulta que $G_f \cap A_n \triangleleft G_f$. Una consecuencia inmediata del teorema y el párrafo anterior, es el siguiente:

COROLARIO 5. *Si $f(x) \in K[x]$ es separable de grado $n > 0$, con* Car$(K) \neq 2$, *$\Delta =$ disc $(f(x))$, L el campo de descomposición de $f(x)$ y G_f su grupo de Galois, entonces el subgrupo de G_f que fija al campo $K(\Delta)$ es $G_f \cap A_n$.*

Demostración. Puesto que $L/K(\Delta)$ es una extensión de Galois, se tiene

$$\text{Gal}(L/K(\Delta)) = \{\sigma \in G_f | \sigma(\alpha) = \alpha \text{ para todo } \alpha \in K(\sqrt{\Delta})\}.$$

Se quiere demostrar que Gal$(L/K(\sqrt{\Delta})) = G_f \cap A_n$. Si $\sigma \in G_f \cap A_n$, entonces σ es par. Por el Teorema 4 se tiene que $\sigma(\sqrt{\Delta}) = \sqrt{\Delta}$ y por tanto $G_f \cap A_n \subseteq$ Gal$(L/K(\sqrt{\Delta})$. Recíprocamente, $\tau \in$ Gal$(L/K(\sqrt{\Delta}))$ significa $\tau(\alpha) = \alpha$ para todo $\alpha \in K(\sqrt{\Delta})$. En particular, $\tau(\sqrt{\Delta}) = \sqrt{\Delta}$ y por tanto $\tau \in A_n \cap G_f$.

□

2. GRUPOS DE GALOIS EN GRADO 3

Si $f(x) \in K[x]$ es un polinomio cúbico y separable, entonces $G_f \leq S_3$. Es fácil verificar que los únicos subgrupos transitivos de S_3 son S_3 y A_3. Por lo anterior, $f(x)$ es irreducible en $K[x]$ si y solo si $G_f \cong A_3, S_3$ y por tanto, $[L : K] = 3, 6$. A continuación se describirá el campo de descomposición de $f(x)$ en términos de una raíz conocida y su discriminante, de paso, se aclarará cuándo $G_f \cong A_3$ ó S_3. De ahora en adelante se denotará $\Delta = disc(f(x))$.

TEOREMA 6. *Sean $f(x) \in K[x]$ cúbico irreducible separable y L su campo de descomposición con* $\mathrm{Car}(K) \neq 2$. *Suponga que α es una raíz cualquiera de $f(x)$. Entonces*

$$L = K(\alpha, \sqrt{\Delta}).$$

Si $\sqrt{\Delta} \in K$, entonces $[L : K] = 3$ y $G_f \cong A_3$. Si $\sqrt{\Delta} \notin K$, entonces $[L : K] = 6$ y $G_f \cong S_3$.

Demostración. Suponga que $f(x) = x^3 + ax^2 + bx + c \in K[x]$ es mónico, separable e irreducible y L su campo de descomposición y sea α una raíz cualquiera de $f(x)$. Observe que $\Delta \neq 0$ porque $f(x)$ es separable y $\sqrt{\Delta} \in L$. Así

$$K(\alpha, \sqrt{\Delta}) \subseteq L.$$

Para la otra contención se trabajará en dos casos: $\sqrt{\Delta} \in K$ y $\sqrt{\Delta} \notin K$. Si $\sqrt{\Delta} \in K$, entonces cualquier $\sigma \in G_f$ satisface $\sigma(\sqrt{\Delta}) = \sqrt{\Delta}$. Si $\sigma = (i, j)$ es una transposición, podemos suponer sin pérdida de generalidad que $\sigma = (1, 2)$. Entonces

$$\begin{aligned}\sigma(\sqrt{\Delta}) &= \sigma((\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)(\alpha_2 - \alpha_3)) \\ &= (\alpha_2 - \alpha_1)(\alpha_2 - \alpha_3)(\alpha_1 - \alpha_3) \\ &= -\sqrt{\Delta}\end{aligned}$$

Por tanto, G_f no contiene transposiciones y por consiguiente $G \cong A_3$. Ahora, si $\sqrt{\Delta} \notin K$, se tiene que $[K(\sqrt{\Delta}) : K] = 2$ y por lo tanto

$$[K(\alpha, \sqrt{\Delta}) : K] = 6.$$

En consecuencia, $L = K(\alpha, \sqrt{\Delta})$ y $G_f \cong S_3$. □

En el caso particular $K = \mathbb{Q}$, si $\sqrt{\Delta} \notin \mathbb{Q}$ y $\Delta < 0$, entonces $\sqrt{\Delta} = a + bi$ y por lo tanto, $L = \mathbb{Q}(\alpha, a + bi)$, así que $f(x)$ tiene una raíz real y dos raices complejas. Si $\Delta > 0$, entonces $\sqrt{\Delta} \in \mathbb{R}$, y puesto que α es cualquier raíz de $f(x)$, se puede elegir $\alpha \in \mathbb{R}$. Por lo anterior, $L \subseteq \mathbb{R}$ y $f(x)$ tiene todas sus raices reales.

Después de analizar el caso $f(x)$ irreducible, la pregunta natural que se hace es: ¿Cuál es el grupo de Galois para un polinomio cúbico reducible? La respuesta es fácil después de analizar los siguientes casos: $f(x)$ tiene sus tres raíces en K o $f(x)$ solo tiene una raíz en K. Sea L el campo de descomposición de $f(x)$. Si $f(x)$ tiene sus tres raíces en K, entonces $L = K$ y así $G_f = \{id\}$. Si $f(x)$ solo tiene una raíz en K, entonces se factoriza como sigue:

$$f(x) = (x - \alpha_1)(x^2 + a_1 x + a_0) \in K[x],$$

donde $\alpha_1 \in K$ y el término cuadrático es irreducible sobre K. Por lo anterior, G_f es transitivo en dos raíces de $f(x)$ y por lo tanto, $G_f \cong S_2$.

Excepto en característica 2, se verá que calcular el grupo de Galois de un polinomio cubíco $f(x) \in K[x]$ separable e irreducible se reduce a calcular Δ y verificar cuándo $\sqrt{\Delta}$ es o no un elemento de K.

COROLARIO 7. *Sean K un campo, $f(x) \in K[x]$ cúbico, separable e irreducible, Δ, G_f, L como en el teorema anterior. Entonces*

1. *$G_f \cong A_3$ si y solo si $\sqrt{\Delta} \in K$.*
2. *$G_f \cong S_3$ si y solo si $\sqrt{\Delta} \notin K$.*

Demostración. Como $f(x) \in K[x]$ es separable e irreducible, por el Corolario 2, se tiene que $[L : K] = o(G_f)$ es divisible por 3. Más aún, por el Teorema 1, se tiene que G_f es isomorfo a un subgrupo transitivo de S_3, los cuales son A_3 y S_3, de orden 3 y 6, respectivamente. De acuerdo al Teorema 4, se infiere que $G_f \cong A_3$ si y solo si $\sqrt{\Delta} \in K$, y por tanto, $G_f \cong S_3$ si y solo si $\sqrt{\Delta} \notin K$. □

3. Clasificación en grado 4 sobre K

El propósito de esta sección es dar criterios específicos y reconocer el grupo de Galois de polinomios irreducibles de grado 4 en $K[x]$, con $\text{Car}(K) \neq 2$.

El Teorema 1 establece que el grupo de Galois de un polinomio irreducible de grado 4 es isomorfo a un subgrupo transitivo de S_4 y es divisible por 4. De acuerdo a Butler-McKay ([1] pp 871-872), los subgrupos transitivos de S_4 son:

$$C_4, \quad D_8, \quad S_4, \quad A_4, \quad V,$$

en donde C_4 es el grupo cíclico de orden 4, D_8 es el grupo diédrico de orden 8, V es el 4-grupo de Klein, A_4 y S_4 son el grupo alternante y el grupo simétrico de grado 4, respectivamente. En [2], Conrad menciona que S_4 contiene 3 subgrupos cíclicos C_4 de orden 4, al menos dos grupos de Klein, solo uno de ellos transitivo, hay tres grupos transitivos conjugados e isomorfos a D_8. El grupo de Klein que no es transitivo es $V' = \{id, (12), (34), (12)(34)\}$, y claramente no puede ocurrir como grupo de Galois de algún polinomio irreducible de grado 4. Los grupos transitivos que se usarán son los siguientes:

1. $C_4 = \{id, (1423), (12)(34), (1324)\} = \langle (1324) \rangle$.
2. $D_8 = \{id, (12), (12)(34), (13)(24), (14)(23), (34), (1423), (1324)\}$
3. $V = \{id, (12)(34), (13)(24), (14)(23)\}$.
4. $A_4 = \langle (123), (134) \rangle$.
5. $S_4 = \langle (12), (1234) \rangle$.

El grupo de Galois de cualquier polinomio $f(x)$ de grado 4, irreducible y separable depende del comportamiento de un polinomio cúbico asociado que resulta ser, precisamente, la resolvente cúbica que aparece cuando se resuelve la ecuación $f(x) = 0$ por el método descrito por Ferrari. Esta resolvente, en la literatura, se le conoce como *la resolvente de Ferrari*.

Definición 8. *Sea K un campo con* $\text{Car}(K) \neq 2$ *y $f(x) = x^4 + ax^3 + bx^2 + cx + d \in K[x]$ separable con raíces r_1, r_2, r_3, r_4. La resolvente cúbica $R_3(x)$ asociado a $f(x)$ es*

$$R_3(x) = x^3 - bx^2 + (ac - 4d)x - (a^2d + c^2 - 4bd) \in K[x]. \tag{1}$$

Observe que las raíces de $R_3(x)$ son

$$\theta_1 = r_1r_2 + r_3r_4, \quad \theta_2 = r_1r_3 + r_2r_4, \quad \theta_3 = r_1r_4 + r_2r_3$$

y se verifica fácilmente, a partir de la definición 3, que $disc(f(x)) = disc(R_3(x))$. Por tanto, como $f(x)$ es separable, entonces $R_3(x)$ también lo es. El grupo de Galois de $R_3(x)$ es un subgrupo de S_3 y se denotará por G_{R_3}.

Note que si $\theta_1, \theta_2, \theta_3$ son como antes, entonces el campo de descomposición E de $R_3(x)$ es subcampo del campo de descomposición de $f(x)$, es decir

$$E = K(\theta_1, \theta_2, \theta_3) \subset L = K(r_1, r_2, r_3, r_4).$$

Lo que no resulta tan evidente pero no es difícil probar es que G_{R_3} es isomorfo al grupo cociente $G_f/(G_f \cap V)$.

Lema 9. *Sean $K, f(x), L, r_1, r_2, r_3\ \ r_4, \theta_1, \theta_2, \theta_3, G_f, R_3(x)$ como antes. Entonces, el subcampo $K(\theta_1, \theta_2, \theta_3)$ está en correspondencia con el grupo normal $G_f \cap V$ de G_f. En consecuencia, $K(\theta_1, \theta_2, \theta_3)$ es una extensión de Galois de K y $G_{R_3} \cong G_f/(G_f \cap V)$.*

Demostración. Solo se justificará la última afirmación. Puesto que $V \lhd A_4 \lhd S_4$, se sigue que $G_f \cap V \lhd G_f$. Por tanto, $G_{R_3} \cong G_f/(G_f \cap V)$. □

Finalmente, uno se encuentra en posición de determinar el grupo de Galois de cualquier polinomio $f(x) = x^4 + ax^3 + bx^2 + cx + d \in K[x]$ irreducible y separable con $\text{Car}(K) \neq 2$.

Teorema 10. *Sea K un campo tal que* $\text{Car}(K) \neq 2$. *Si $f(x) = x^4 + ax^3 + bx^2 + cx + d \in K[x]$ es irreducible y separable, $L, G_f, R_3(x)$, E, G_{R_3} son como antes y $\Delta = disc(f(x)) = disc(R_3(x))$, entonces*

1. *$G_f = S_4$ si y solo si $R_3(x)$ es irreducible en $K[x]$ y $\sqrt{\Delta} \notin K$.*

2. $G_f = A_4$ *si y solo si* $R_3(x)$ *es irreducible en* $K[x]$ *y* $\sqrt{\Delta} \in K$.
3. $G_f = V$ *si y solo si* $R_3(x)$ *se descompone en* $K[x]$ *y* $\sqrt{\Delta} \in K$.
4. $G_f = C_4$ *ó* D_8 *si y solo si* $R_3(x)$ *tiene exactamente una raíz* $\theta \in K$ *y* $\sqrt{\Delta} \notin K$.

Demostración. 1. Suponga que $R_3(x)$ es irreducible sobre K y $\sqrt{\Delta} \notin K$. Por el Corolario 7 se tiene que $G_{R_3} \cong S_3$. Por tanto,

$$o(G_{R_3}) = o(G_f/(G_f \cap V)) = o(G_f)/o(G_f \cap V) = 6$$

implica que $o(G_f) = 12$ ó 24. Si $o(G_f) = 12$, entonces $G_f = A_4$. Por consiguiente, $o(A_4/(A_4 \cap V)) = 3$, lo cual es una contradicción. Debe suceder que $o(G_f) = 24$. Así que $G_f = S_4$. Recíprocamente, suponga que $G_f = S_4$, entonces $G_f \cap V = S_4 \cap V = V$. En consecuencia,

$$o(G_f/(G_f \cap V)) = o(S_4/V) = o(S_4)/o(V) = 24/4 = 6 = o(G_{R_3}).$$

Se sigue que $G_{R_3} \cong S_3$. Por el Teorema 1 y por el Corolario 7 se obtiene que $R_3(x)$ es irreducible en $K[x]$ y$\sqrt{\Delta} \notin K$, respectivamente.

2. Suponga que $R_3(x)$ es irreducible en $K[x]$ y $\sqrt{\Delta} \in K$. Entonces por el Corolario 7 se tiene que $G_{R_3} \cong A_3$, así

$$o(G_{R_3}) = o(G_f/G_f \cap V) = o(G_f)/o(G_f \cap V) = 3,$$

y puesto que $f(x)$ es irreducible y $4 \mid o(G_f)$, se tiene que $o(G_f) = 12$. Por lo anterior $G_f = A_4$. Recíprocamente, supóngase $G_f = A_4$. Por tanto, $G_f \cap V = V$. Esto implica que

$$o(G_{R_3}) = o(G_f/o(G_f \cap V)) = o(A_4/o(V)) = o(A_4)/o(V) = 12/4 = 3.$$

De aquí se sigue que $G_{R_3} \cong A_3$. Por el Teorema 1 y el por el Corolario 7 se concluye que $R_3(x)$ es irreducible en $K[x]$ y $\sqrt{\Delta} \in K$, respectivamente.

3. Si $R_3(x)$ tiene todas sus raices en K, entonces

$$L^{G_f \cap V} = K(\theta_1, \theta_2, \theta_3) = K = L^{G_f}.$$

En consecuencia, $G_f \cap V = G_f$ si y solo si $G_f \subseteq V$ y como $4 \mid o(G_f)$, se sigue que $G_f = V$. Recíprocamente, si $G_f = V$, entonces $G_f \cap V = V$ significa que

$$o(G_{R_3}) = o(G_f/(G_f \cap V)) = o(V/V) = 1.$$

Por el Teorema Fundamental de la Teoría de Galois, se infiere que

$$o(G_{R_3}) = 1 = [K(\theta_i, \sqrt{\Delta}) : K] = [K(\theta_1, \theta_2, \theta_3) : K],$$

si y solo si $\theta_1, \theta_2, \theta_3 \in K$. Por tanto, $R_3(x)$ se descompone sobre K.

4. Supóngase que $R_3(x)$ tiene exactamente una raíz $\theta \in K$ y $\sqrt{\Delta} \notin K$. El hecho de que $\sqrt{\Delta} \notin K$ por el Teorema 4 implica que $G_f \not\subseteq A_4$. Así que $G_f = C_4, D_8$ ó S_4. Sin embargo, $R_3(x)$ tiene exactamente una raíz en K, es decir, $R_3(x)$ es reducible en $K[x]$ y por el inciso 1, se obtiene que $G_f \neq S_4$. Por lo anterior $G_f = C_4$ ó D_8. Recíprocamente, supóngase que $G_f = C_4$ ó D_8. Si $G_f = C_4$, entonces

$$G_f \cap V \cong \{id, (12)(34)\}.$$

Por lo tanto

$$o(G_f/(G_f \cap V)) = o(G_f)/o(G_F \cap V) = 2 = o(G_{R_3}).$$

Ahora, si $G_f = D_8$, entonces $G_f \cap V \cong \{id, (12)(34), (13)(24), (14)(23)\}$. Por tanto

$$o(G_f/(G_f \cap V)) = o(G_f)/o(G_f \cap V) = 2 = o(G_{R_3}).$$

En ambos casos se tiene que $o(G_{R_3}) = 2$. Por otra parte, se sabe que el campo de descomposición de $R_3(x)$ es de la forma $K(\theta, \sqrt{\Delta})$, donde θ es cualquier raíz de $R_3(x)$. Si $\theta \in K$, entonces $K(\theta, \sqrt{\Delta}) = K(\sqrt{\Delta})$. Puesto que $o(G_{R_3}) = 2$, se tiene

$$[K(\sqrt{\Delta}) : K] = 2 \text{ si y solo si } \sqrt{\Delta} \notin K.$$

Por hipótesis $\theta \in K$, así que $R_3(x)$ es reducible en $K[x]$. Resta probar que $R_3(x)$ tiene exactamente una raíz en K. Se verá qué sucede si $R_3(x)$ tiene dos raíces en K ó tres

raíces en K. Si tiene 2 raíces, entonces tiene todas y $R_3(x)$ se descompone totalmente en $K[x]$, en consecuencia, por el inciso 3, $G_f = V$, lo cual es una contradicción. Por tanto, $R_3(x)$ tiene exactamente una raíz en K.

□

La afirmación 4 del Teorema anterior no permite distinguir cuándo $G_f = C_4$ ó $G_f = D_8$. El siguiente resultado ayudará a distinguir cada caso.

TEOREMA 11. *Sean $K, f(x) = x^4 + ax^3 + bx^2 + cx + d \in K[x]$, L, $R_3(x)$, Δ, G_f y G_{R_3} como en el teorema anterior. Suponga que $\sqrt{\Delta} \notin K$ y $R_3(x)$ tiene exactamente una raíz $\theta \in K$. Sean $g(x) = (x^2 + ax + (b - \theta))(x^2 - \theta x + d) \in K[x]$ y M el campo de descomposición de $g(x)$. Entonces*

1. *$G_f = C_4$ si y solo si $g(x)$ se descompone en $K(\sqrt{\Delta})[x] = M[x]$.*
2. *$G_f = D_8$ si y solo si $g(x)$ no se descompone en $K(\sqrt{\Delta})[x]$, en particular, $K(\sqrt{\Delta}) \neq M$.*

Demostración. Sea θ la única raíz de $R_3(x)$ en K. Reetiquetando las raíces de $f(x)$, si fuera necesario, se puede suponer que $\theta = r_1r_2 + r_3r_4 \in K$. Recuerde que se ha establecido lo siguiente:

$$C_4 = \{id, (1324), (1423), (12)(34)\}.$$

$$D_8 = \{id, (12), (12)(34), (13)(24), (14)(23), (34), (1423), (1324)\}.$$

Observe que si $\sigma \in G_f$, entonces $\sigma(\theta) = \sigma(r_1r_2 + r_3r_4) = r_1r_2 + r_3r_4$, pues $\theta \in K$. Sean $\tau = (34),\ \sigma = (1324)$. Es claro que:

1. Si $G_f = C_4$, entonces $G_f = \langle\sigma\rangle = \langle(1324)\rangle$.
2. Si $G_f = D_8$, entonces $G_f = \langle\tau, \sigma\rangle = \langle(34), (1324)\rangle$.

Si $G_f = C_4 = \langle\sigma\rangle$, por Teoría de Galois, la correspondencia entre los subgrupos de $\langle\sigma\rangle$ y los subcampos de L está descrita en el siguiente diagrama:

$$\begin{array}{ccc} \{id\} & \longleftrightarrow & L = K(r_1, r_2, r_3, r_4) \\ | & & | \\ \langle\sigma^2\rangle & \longleftrightarrow & K(\sqrt{\Delta}) \\ | & & | \\ \langle\sigma\rangle & \longleftrightarrow & K \end{array}$$

Observe que $[L : K] = 4 = [L : K(r_1)][K(r_1) : K]$ y por tanto $L = K(r_1) = K(r_1, r_2, r_3, r_4)$. En este caso se mostrará que $M = K(\sqrt{\Delta})$. Recuerde que se tienen relaciones entre los coeficientes de $f(x)$ y r_1, r_2, r_3, r_4 :

$$\begin{aligned} a &= -(r_1 + r_2 + r_3 + r_4), \\ b &= r_1r_2 + r_1r_3 + r_1r_4 + r_2r_3 + r_2r_4 + r_3r_4, \\ c &= -(r_1r_2r_3 + r_1r_2r_4 + r_1r_3r_4 + r_2r_3r_4), \\ d &= r_1r_2r_3r_4. \end{aligned}$$

Sean $g_1(x) = x^2 + ax + (b - \theta) \in K[x]$ y α_1, β_1 las raíces de $g_1(x)$. Observe que

$$(x - (r_1 + r_2))(x - (r_3 + r_4)) = x^2 - (\sum_{i=1}^{4} r_i)x + (r_1 + r_2)(r_3 + r_4) = x^2 + ax + (b - \theta),$$

así, se puede suponer, sin pérdida de generalidad que

$$\alpha_1 = r_1 + r_2 \quad \text{y} \quad \beta_1 = r_3 + r_4.$$

Por lo anterior, $\alpha_1, \beta_1 \in L$. Análogamente, si $g_2(x) = x^2 - \theta x + d$ y α_2, β_2 son las raíces de $g_2(x)$, entonces:

$$(x - r_1r_2)(x - r_3r_4) = x^2 - (r_3r_4 + r_1r_2)x + r_1r_2r_3r_4 = x^2 - \theta x + d,$$

así que

$$\alpha_2 = r_1r_2 \quad \text{y} \quad \beta_2 = r_3r_4.$$

Puesto que $M = K(\alpha_1, \beta_1, \alpha_2, \beta_2)$, es claro que $K \subseteq M \subseteq L$. Se verá que las contenciones son propias. Si $K = M$, entonces $r_1r_2, r_3r_4, r_1 + r_2, r_3 + r_4 \in K$, y además se tiene que

$$f(x) = (x^2 - (r_1 + r_2)x + r_1r_2)(x^2 - (r_3 + r_4)x + r_3r_4) \in M[x],$$

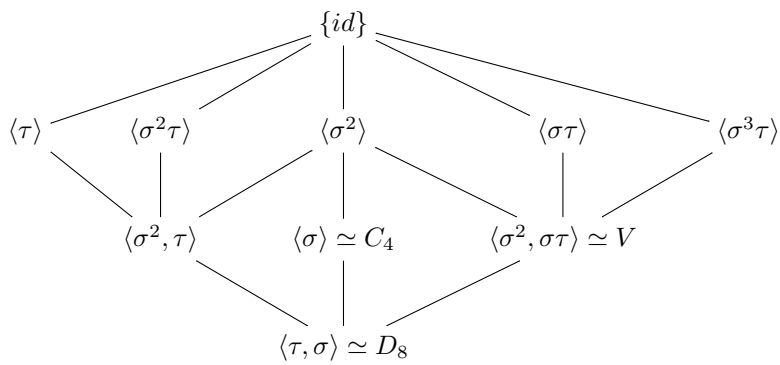
lo cual significa que $f(x)$ es reducible en $M[x] = K[x]$, lo cual no es posible porque por hipótesis $f(x)$ es irreducible en $K[x]$. Por tanto, $K \subset M$. Finalmente, para ver que L contiene propiamente a M, suponga que $L = M$. Puesto que M es el campo de descomposición de $g(x) = (x^2 + ax + (b - \theta))(x^2 - \theta x + d) \in K[x]$, se tiene que

$$K(\alpha_1, \alpha_2, \beta_1, \beta_2) = M = L = K(r_1, r_2, r_3, r_4),$$

en particular, $K(\alpha_1) \subseteq M$. También sucede que $M \subseteq K(\alpha_1)$. En efecto, observe que $[K(\alpha_1) : K] \leq 2$. Si $[K(\alpha_1) : K] = 1$, entonces $K = K(\alpha_1)$ y $\alpha_1, \beta_1 \in K$. En consecuencia, $M = K(\alpha_1, \alpha_2, \beta_1, \beta_2) = K(\alpha_2, \beta_2)$. Por tanto, $[L : K] = [M : K] \leq 2$ lo cual no es posible pues se sabe L/K es Galois y $G_f = C_4$, es decir $[L : K] = 4$. Por lo anterior, $[K(\alpha_1) : K] = 2$. Análogamente, se prueba que $[K(\beta_1) : K] = 2$. Por el Teorema Fundamental de la Teoría de Galois, se tiene que $K(\alpha_1) = K(\beta_1)$ pues C_4 solo contiene un subgrupo de orden 2. En particular, $\beta_1 \in K(\alpha_1)$ y también $\beta_2 \in K(\alpha_1)$, es decir, $\alpha_1, \alpha_2, \beta_1, \beta_2 \in K(\alpha_1)$. Así, $M \subseteq K(\alpha_1)$. En consecuencia, $M = K(\alpha_1)$ lo cual no es posible pues $[K(\alpha_1) : K] \leq 2$ y $[L : K] = 4$. Por consiguiente, se sigue que M está contenido propiamente en L. Lo anterior muestra que si $G_f = C_4$, entonces $M = K(\sqrt{\Delta})$. Por lo anterior, si $G_f = C_4$, entonces $g(x)$ se descompone en $K(\sqrt{\Delta})[x]$. Más aún, por el Teorema Fundamental de la Teoría de Galois, se tiene que M está en correspondencia con $\langle \sigma^2 \rangle$.

Inversamente, suponga que $g(x) = (x^2 + ax + (b - \theta))(x^2 - \theta x + d) \in K[x]$ se descompone en $K(\sqrt{\Delta})[x]$, así que $r_1 + r_2,\ r_1r_2,\ r_3 + r_4,\ r_3r_4 \in K(\sqrt{\Delta})$. Sean $h(x) = x^2 - (r_1 + r_2)x + r_1r_2 \in K(\sqrt{\Delta})[x]$ y F su campo de descomposición sobre $K(\sqrt{\Delta})$, así $K \subseteq K(\sqrt{\Delta}) \subseteq F \subseteq L$. Observe que $h(r_1) = h(r_2) = 0$, por tanto $r_1, r_2 \in F$. Note que $[F : K(\sqrt{\Delta})] = 2$. Como $r_1 - r_2 \neq 0$ y $\theta_2, \theta_3 \in K(\sqrt{\Delta}) \subset F$, se sigue que $r_3 - r_4 = \dfrac{\theta_2 - \theta_3}{r_1 - r_2} \in F$. La igualdad $2r_3 = (r_3 + r_4) + (r_3 - r_4) \in F$ implica que $r_3 \in F$ y por lo tanto $r_4 \in F$. Por lo anterior $F = L$ y $[L : K] = 4$. Finalmente, por la afirmación 4 del Teorema 10, se sigue que $G_f = C_4$.

En el caso $G_f = D_8$, primero se va a construir la retícula de subgrupos de D_8 y más adelante, la correpondiente retícula de campos intermedios de la extensión L/K, la cual será de utilidad para demostrar la afirmación 2 del teorema en curso. En lo que sigue se muestra la retícula de subgrupos de D_8 :



A continuación se va a construir la retícula de subcampos que corresponde a cada subgrupo de D_8. En la siguiente tabla se proporcionan explícitamente los elementos del grupo D_8 :

id	σ	σ^2	σ^3	τ	$\sigma\tau$	$\sigma^2\tau$	$\sigma^3\tau$
(1)	(1324)	(12)(34)	(1423)	(34)	(13)(24)	(12)	(14)(23)

Note que exactamente como se argumentó en el caso C_4 se tiene que M contiene propiamente a K.

De acuerdo a la tabla anterior, es claro que id y τ son los únicos elementos de D_8 que fijan a r_1 y r_2. Por tanto $L^{\langle\tau\rangle} = K(r_1, r_2)$. Ahora, como $K(r_1) \subset K(r_1, r_2)$ y $[K(r_1, r_2, r_3, r_4) : K(r_1, r_2)] = o(\langle\tau\rangle) = 2$, entonces

$$4 = [K(r_1, r_2) : K] = [K(r_1, r_2) : K(r_1)][K(r_1) : K].$$

Pero $4 = gr(f(x)) = [K(r_1) : K]$, así que $[K(r_1, r_2) : K(r_1)] = 1$ y por tanto $K(r_1, r_2) = K(r_1)$. Más aún, $r_2 \in K(r_1)$ y $K(r_2) \subset K(r_1)$. Análogamente, $K(r_1) \subset K(r_2)$, así que $K(r_1) = K(r_2)$. Se ha probado que

$$L^{\langle\tau\rangle} = K(r_1, r_2) = K(r_1) = K(r_2).$$

Similarmente, observe que $L^{\langle\sigma^2\tau\rangle} = K(r_3, r_4)$. De la misma manera que en el caso anterior se tiene

$$L^{\langle\sigma^2\tau\rangle} = K(r_3, r_4) = K(r_3) = K(r_4).$$

Puesto que $\langle\tau\rangle, \langle\sigma^2\tau\rangle \leqslant \langle\sigma, \tau\rangle$ con campos fijos $L^{\langle\tau\rangle}$, $L^{\langle\sigma^2\tau\rangle}$ respectivamente, entonces por el Teorema Fundamental de la Teoría de Galois, se sigue que

$$L^{\langle\sigma,\tau\rangle} \subseteq L^{\langle\tau\rangle} = K(r_1) \quad \text{y} \quad L^{\langle\sigma,\tau\rangle} \subseteq L^{\langle\sigma^2\tau\rangle} = K(r_3).$$

Observe que σ^2, τ fijan a $\alpha_1, \alpha_2, \beta_1, \beta_2$. Por tanto $\text{Gal}(L/M) = \langle\sigma^2, \tau\rangle$. Por otro lado $\langle\tau\rangle \subset \langle\sigma^2, \tau\rangle$. Así

$$M \subset K(r_1) \quad \text{y} \quad M \subset K(r_3).$$

Por hipótesis $\sqrt{\Delta} \notin K$, entonces $[K(\sqrt{\Delta}) : K] = 2$. Puesto que $\sigma^2, \sigma\tau$ fijan a $\sqrt{\Delta}$, se sigue que

$$\text{Gal}(L/K(\sqrt{\Delta})) = \langle\sigma^2, \sigma\tau\rangle.$$

Observe que:

$$\begin{aligned}\sigma^2(\sqrt{\Delta}) &= \sigma^2((r_1 - r_2)(r_1 - r_3)(r_1 - r_4)(r_2 - r_3)(r_2 - r_4)(r_3 - r_4)) \\ &= (r_2 - r_1)(r_2 - r_4)(r_2 - r_3)(r_1 - r_4)(r_1 - r_3)(r_4 - r_3) \\ &= \sqrt{\Delta}.\end{aligned}$$

También,

$$\begin{aligned}\sigma^2(\alpha_1) &= \sigma^2(r_1 + r_2) = r_2 + r_1 = \alpha_1, \\ \sigma^2(\alpha_2) &= \sigma^2(r_1 r_2) = r_2 r_1 = \alpha_2, \\ \sigma^2(\beta_1) &= \sigma^2(r_3 + r_4) = r_4 + r_3 = \beta_1, \\ \sigma^2(\beta_2) &= \sigma^2(r_3 r_4) = r_4 r_3 = \beta_2.\end{aligned}$$

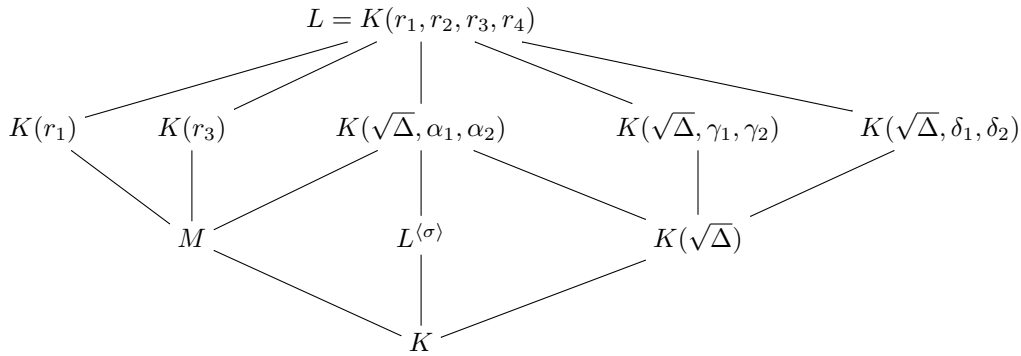
Puesto que $K(\sqrt{\Delta}, \alpha_1, \alpha_2, \beta_1, \beta_2) = K(\sqrt{\Delta}, \alpha_1, \alpha_2)$, se tiene

$$\text{Gal}(L/K(\sqrt{\Delta}, \alpha_1, \alpha_2)) = \langle\sigma^2\rangle.$$

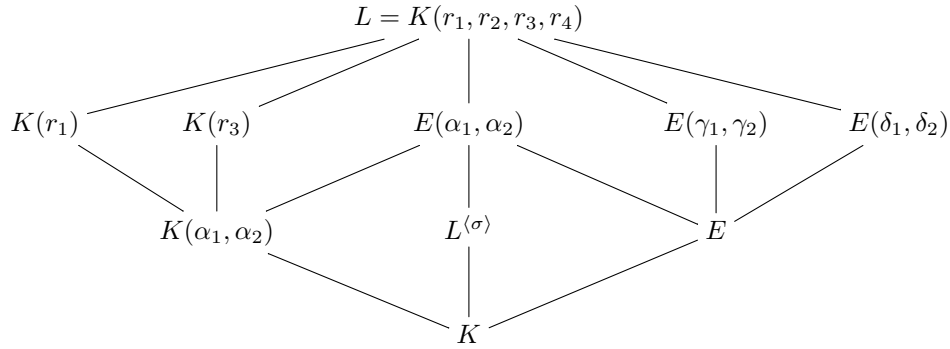
Si $\gamma_1 = r_1 + r_3$, $\gamma_2 = r_1 r_3$, $\delta_1 = r_1 + r_4$, $\delta_2 = r_1 r_4$, se verifica fácilmente que

$$\text{Gal}(L/K(\sqrt{\Delta}, \gamma_1, \gamma_2)) = \langle\sigma\tau\rangle \quad \text{y} \quad \text{Gal}(L/K(\sqrt{\Delta}, \delta_1, \delta_2)) = \langle\sigma^3\tau\rangle.$$

Con lo anterior se tiene la retícula de subcampos de L/K correspondiente a la retícula de subgrupos de $G_f = \langle\tau, \sigma\rangle$:



Siguiendo la notación del Teorema 10, si E es el campo de descomposición de $R_3(x)$, y como disc $(R_3(x)) = \Delta =$ disc $(f(x))$, es claro que $E = K(\sqrt{\Delta})$. Por consiguiente la retícula de subcampos queda como sigue:



Ahora se probará la afirmación 2 del teorema. Si $g(x)$ se descompone en $K(\sqrt{\Delta})$, entonces $M \subseteq K(\sqrt{\Delta})$. Por hipótesis, $\sqrt{\Delta} \notin K$, así $[K(\sqrt{\Delta}) : K] = 2$ y por tanto

$$[K(\sqrt{\Delta}) : M] = 1 \text{ y } [M : K] = 2 \quad \text{ó} \quad [K(\sqrt{\Delta}) : M] = 2 \text{ y } [M : K] = 1.$$

En el primer caso, si $M = K(\sqrt{\Delta})$, entonces $g(x)$ se descompone en $K(\sqrt{\Delta})$ y por la afirmación 1 de este teorema $G_f = C_4 \neq D_8$. En el segundo caso, si $M = K(\alpha_1, \alpha_2) = K$, entonces $r_1 + r_2, r_1 r_2 \in K$. El polinomio

$$h(x) = x^2 - (r_1 + r_2)x + r_1 r_2 \in K[x]$$

es irreducible en $K[x]$ pues $h(r_1) = h(r_2) = 0$ y $r_1, r_2 \notin K$. Por lo anterior $[K(r_1) : K] = 2$, lo cual no es posible porque $f(x)$ es irreducible en $K[x]$ y $4 = \text{grad}(f(x))$. Por tanto $g(x)$ no se descompone en $K(\sqrt{\Delta})[x]$.

Inversamente, si $G_f \neq D_8$, puesto que $\sqrt{\Delta} \notin K$ y $R_3(x)$ tiene sólo una raíz $\theta \in K$, entonces por la afirmación 4 del Teorema 10, $G_f = C_4$ y por la afirmación 1 de este teorema, $g(x)$ se descompone en $K(\sqrt{\Delta})[x]$. □

Una vez que se ha determinado el grupo de Galois de polinomios irreducibles separables de grado 4, también se puede estudiar el grupo de Galois de polinomios reducibles.

Considere $f(x) = x^4 + ax^3 + bx^2 + cx + d \in K[x]$ separable y reducible. Sea L el campo de descomposición de $f(x)$ y G_f su grupo de Galois. El caso más sencillo es cuando $f(x)$ tiene todas sus raíces en K. En este caso $L = K$ y por tanto $G_f = \{id\}$. Ahora suponga que $f(x)$ tiene exactamente una raíz α en K. Entonces

$$f(x) = (x - \alpha)q(x),$$

en donde $q(x) \in K[x]$ es un polinomio cúbico irreducible. Si $L_{q(x)}$ es el campo de descomposición de $q(x)$, entonces $L = L_{q(x)}$ y de acuerdo al Teorema 6 se sigue que

$$G_f = G_{q(x)} = A_3, S_3.$$

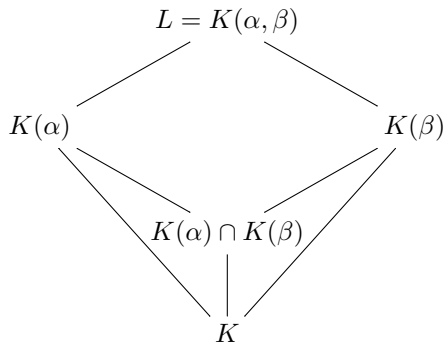
Ahora suponga que $f(x) = p(x)q(x)$, donde $p(x)$ y $q(x)$ son cuadráticos e irreducibles sobre K; asuma que α es una raíz de $p(x)$ y que β es una raíz de $q(x)$. En consecuencia, $K(\alpha)$ es el campo de descomposición de $p(x)$; $K(\beta)$ el de $q(x)$. Considere dos casos:

$$K \subset K(\alpha) \cap K(\beta) \quad \text{y} \quad K(\alpha) \cap K(\beta) = K.$$

Si $K \subset K(\alpha) \cap K(\beta)$, entonces

$$K \subset K(\alpha) \cap K(\beta) \subset K(\alpha) \quad \text{y} \quad K \subset K(\alpha) \cap K(\beta) \subset K(\beta).$$

Puesto que $[K(\alpha) : K] = [K(\beta) : K] = 2$, se tiene $K(\alpha) = K(\beta)$. Por lo anterior, $L = K(\alpha) = K(\beta)$ y así $G_f = \mathbb{Z}_2$.



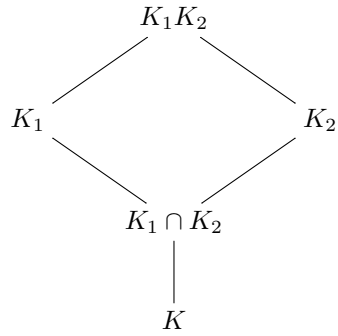
En el caso $K(\alpha) \cap K(\beta) = K$, se tiene que $G_f = V$. cuya prueba se seguirá del siguiente resultado:

TEOREMA 12. *Sean $K_1/K, K_2/K$ extensiones de Galois, donde K_1, K_2 son subcampos de algún campo. Entonces*

1. *$K/K_1 \cap K_2$ es Galois sobre K.*
2. *La composición K_1K_2 es Galois sobre K y*

$$\text{Gal}(K_1K_2/K) \cong H = \{(\sigma, \tau) : \sigma|_{K_1 \cap K_2} = \tau|_{K_1 \cap K_2}\} \leq \text{Gal}(K_1/K) \times \text{Gal}(K_2/K)$$

3. *Si $K(\alpha) \cap K(\beta) = K$, entonces* $\text{Gal}(K_1K_2/K) \cong \text{Gal}(K_1/K) \times \text{Gal}(K_2/K)$.



Demostración. Vea Theorem 1.14. en [7]. □

Regresando a nuestro caso, observe que $\text{Gal}(K(\alpha)/K) = \text{Gal}(K(\beta)/K) \cong \mathbb{Z}_2$, y por tanto, $G_f = \text{Gal}(L/K) \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \cong V$. Teorema 10 se sigue que $G_f = S_4$. Si p=3, entonces es fácil ver que

3.1. Polinomios bicuadráticos. Como una aplicación de los resultados obtenidos en la sección anterior, se estudiarán polinomios cuárticos de la forma $f(x) = x^4 + bx^2 + d \in K[x]$, con $\text{Car}(K) \neq 2$ y que son conocidos en la literatura como polinomios bicuadráticos. En lo que sigue, se mostrará que para polinomios bicuadráticos, la resolvente cúbica $R_3(x)$ es reducible sobre K y por las afirmaciones 3 y 4 del Teorema 10 se sigue que $G_f = V, C_4, D_8$. Concretamente:

COROLARIO 13. *Sean K con $\text{Car}(K) \neq 2$, $f(x) = x^4 + bx^2 + d \in K[x]$ irreducible y separable, con raíces $\pm\alpha, \pm\beta$, $L = K(\alpha, \beta)$ su campo de descomposición, $R_3(x)$, G_f, Δ como en el Teorema 10. Entonces $R_3(x)$ es reducible en $K[x]$ y en consecuencia, $G_f = V, D_8, C_4$ de acuerdo con lo siguiente:*

(1) *$G_f = V$ si y solo si $\sqrt{d} \in K$ si y solo si $\alpha\beta \in K$.*
(2) *$G_f = C_4$ si y solo si $\sqrt{d} \notin K$ y $\sqrt{d(b^2 - 4d)} \in K$ si y solo si $K(\alpha\beta) = K(\alpha^2)$.*
(3) *$G_f = D_8$ si y solo si $\sqrt{d} \notin K$ y $\sqrt{d(b^2 - 4d)} \notin K$ si y solo si $\alpha\beta \notin K(\alpha^2)$.*

Demostración. Suponga que $f(x) = x^4 + bx^2 + d = x^4 - (\alpha^2 + \beta^2)x^2 + \alpha^2\beta^2$ es irreducible sobre K. Ahora, la resolvente cúbica de $f(x)$ es

$$R_3(x) = x^3 - bx^2 - 4dx + 4bd = x(x^2 - 4d) - b(x^2 - 4d) = (x - b)(x^2 - 4d),$$

el cual es reducible en $K[x]$ con $\theta = b \in K$ como raíz. Por consiguiente, por las afirmaciones 3 y 4 del Teorema 10, $G_f = V, D_8, C_4$. Además, observe que

$$\begin{aligned}
\Delta &= disc(x^3 - bx^2 - 4dx + 4bd) \\
&= disc(x^4 + bx^2 + d) \\
&= -128b^2d^2 + 16b^4d + 256d^3 \\
&= 4^2d(4^2d^2 - 8b^2d + b^4) \\
&= 4^2d(b^2 - 4d)^2.
\end{aligned}$$

Para demostrar la afirmación (1), observe lo siguiente:

$$\sqrt{\Delta} \in K \quad \text{si y solo si} \quad \sqrt{d} \in K.$$

En consecuencia,

$$R_3(x) = (x - b)(x - 2\sqrt{d})(x + 2\sqrt{d}) \in K[x]$$

se descompone en $K[x]$. Así, por el Teorema 10 y por lo anterior, se tiene que $G_f = V$ si y solo si $\sqrt{d} \in K$ si y solo si $\sqrt{d} = \alpha\beta \in K$. Esto prueba la primera afirmación.

Ahora, para demostrar las afirmaciones (2) y (3), primero recuerde que $\sqrt{\Delta} \in K$ si y solo si $\sqrt{d} \in K$. Equivalentemente, $\sqrt{d} \notin K$ si y solo si $\sqrt{\Delta} \notin K$. Por lo anterior, en las afirmaciones (2) y (3), aplicando el Teorema 10, $G_f = D_8, C_4$. Considere $g(x)$ del Teorema 11. Observe que en este caso $a = 0$ y $b = \theta$, es decir,

$$g(x) = (x^2 + ax + (b - \theta))(x^2 - \theta x + d) = x^2(x^2 - \theta x + d) = x^2(x^2 - bx + d),$$

donde las raices de $x^2 - bx + d$ están dadas por

$$\gamma, \delta = \frac{b \pm \sqrt{b^2 - 4d}}{2} = -\Big(\frac{-b \mp \sqrt{b^2 - 4d}}{2}\Big) = -\alpha^2, -\beta^2,$$

en donde α, β son las raíces de $f(x)$. Además, $M = K(\sqrt{b^2 - 4d})$ es el campo de descomposición de $g(x)$. Ahora, para demostrar la afirmación (2) suponga que $\sqrt{d} \notin K$ y $\sqrt{d(b^2 - 4d)} \in K$. Entonces $K(\sqrt{d}) = K(\sqrt{b^2 - 4d})$ ya que

$$\sqrt{d} = \frac{\sqrt{d}\sqrt{b^2 - 4d}}{\sqrt{b^2 - 4d}} = \frac{\sqrt{d(b^2 - 4d)}}{\sqrt{b^2 - 4d}} \in K(\sqrt{b^2 - 4d}),$$

y

$$\sqrt{b^2 - 4d} = \frac{\sqrt{d}\sqrt{b^2 - 4d}}{\sqrt{d}} = \frac{\sqrt{d(b^2 - 4d)}}{\sqrt{d}} \in K(\sqrt{d}).$$

También es claro que si $K(\sqrt{d}) = K(\sqrt{b^2-4d})$, entonces $\sqrt{d} \notin K$ y $\sqrt{d(b^2-4d)} \in K$. Por lo anterior,

$$M = K(\sqrt{d}) = K(\sqrt{\Delta}).$$

Por otro lado, como $\sqrt{\Delta} = 4(b^2-4d)\sqrt{d}$, entonces por la afirmación 1 del Teorema 11, se tiene que

$$\begin{aligned} G_f = C_4 \quad &\text{si y solo si} \quad g(x) \quad \text{se descompone sobre} \quad K(\sqrt{\Delta}) \\ &\text{si y solo si} \quad g(x) \quad \text{se descompone sobre} \quad K(\sqrt{d}) = K(\sqrt{b^2-4d}) \\ &\text{si y solo si} \quad \sqrt{d(b^2-4d)} \in K. \end{aligned}$$

Finalmente, usando la relación $d = \alpha^2\beta^2$, se sigue fácilmente que $K(\sqrt{d}) = K(\sqrt{b^2-4d})$ es equivalente a $K(\alpha\beta) = K(\alpha^2)$ pues

$$K(\alpha^2) = K\Big(\frac{b+\sqrt{b^2-4d}}{2}\Big) = K(\sqrt{b^2-4d}\,) = K(\sqrt{d}\,) = K(\alpha\beta).$$

Con esto, se termina la demostración de la afirmación (2), y la afirmación (3) se sigue de manera análoga. □

AGRADECIMIENTOS

Quisiera agredcer al arbitro anónimo por las obrservaciones hechas a este trabajo.

REFERENCIAS

[1] Butler, G and John McKay., *The transitive groups of degree up to eleven*. in Algebra 11(8) (1983): 863-911.
[2] Conrad, K., *Galois Groups of Cubics and Quartics (not in Characteristic 2)*. <www.math.uconn.edu/ kconrad/blurbs/galoistheory/cubicquartic.pdf>.
[3] Cox, D., *Galois Theory*. Second Edition. Pure and applied Mathematics. Wiley, 2012.
[4] Dummit, D, and Foote, R., *Abstract Algebra*. Third Edition. John Wiley and Sons, Inc. 2004.
[5] *Évariste Galois, Oeuvres Mathématiques.* Éditions Jacques Gabay, 1989.
[6] Kappe, L. C. and Warren B., An *elementary Test for the Galois Group of a Quartic Polynomial*. American Mathematical Monthly, Vol. 96 No. 2 (1989): 133-137.
[7] Lang, S., *Algebra*, Third Edition. Addison-Wesley, 1994.
[8] Steven, R., *Field Theory*. Second Edition. Garduate Texts in Mathematics. Springer, 1994.

Dirección del autor:
Universidad Autónoma Metropolitana,
Unidad Iztapalapa,
División de Ciencias Básicas e Ingeniería,
Departamento de Matemáticas.
Av. San Rafael Atlixco 186, Col. Vicentina
Del. Iztapalapa, C.P. 09340, Ciudad de México
e-mail: edgargutierrez221@gmail.com