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

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

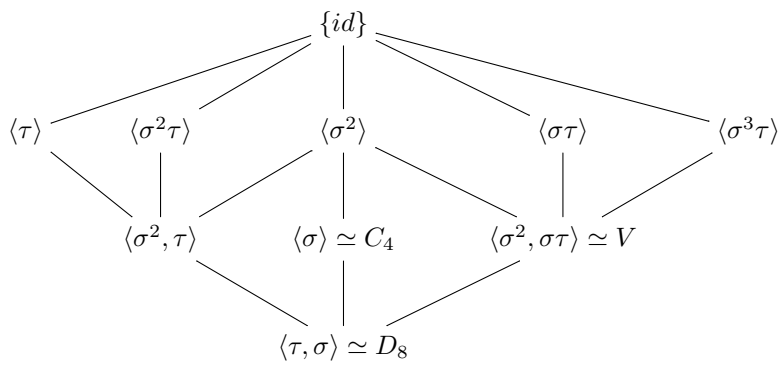
lo cual significa que $f(x)$ es reducible en $M[x] = K[x]$, lo cual no es posible porque por hipótesis $f(x)$ es irreducible en $K[x]$. Por tanto, $K \subset M$. Finalmente, para ver que L contiene propiamente a M, suponga que $L = M$. Puesto que M es el campo de descomposición de $g(x) = (x^2 + ax +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

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

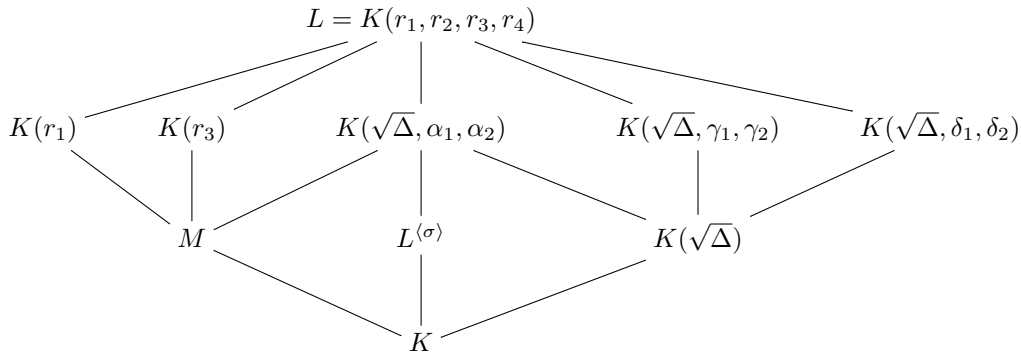
Puesto que $K(\sqrt{\Delta}, \alpha_1, \alpha_2, \beta_1, \beta_2) = K(\sqrt{\Delta}, \alpha_1, \alpha_2)$, se tiene

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

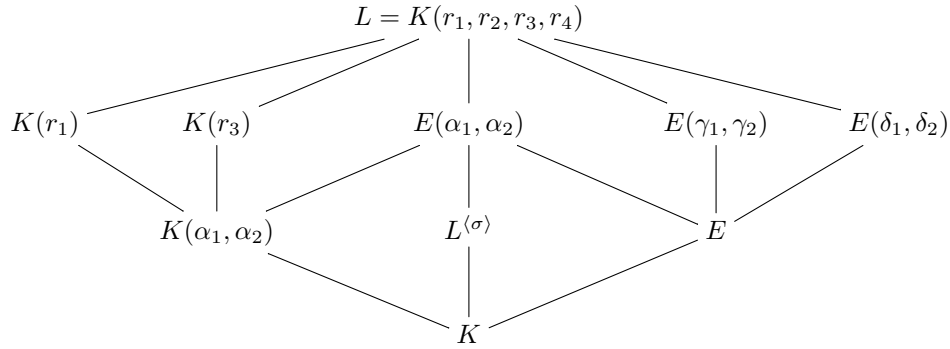
Si $\gamma_1 = r_1 + r_3$, $\gamma_2 = r_1 r_3$, $\delta_1 = r_1 + r_4$, $\delta_2 = r_1 r_4$, se verifica fácilmente que

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

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

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

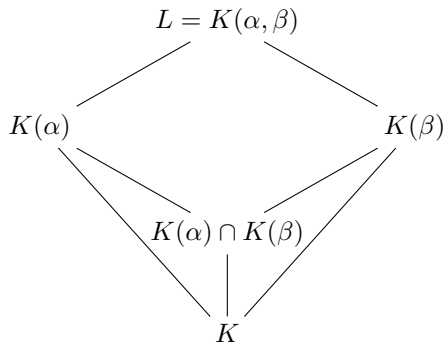
Ahora suponga que $f(x) = p(x)q(x)$, donde $p(x)$ y $q(x)$ son cuadráticos e irreducibles sobre K; asuma que α es una raíz de $p(x)$ y que β es una raíz de $q(x)$. En consecuencia, $K(\alpha)$ es el campo de descomposición de $p(x)$; $K(\beta)$ el de $q(x)$. Considere dos casos:

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

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 $G_f = \mathbb{Z}_2$.



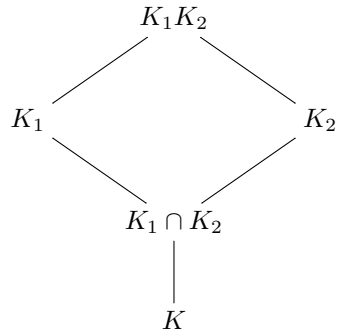
En el caso $K(\alpha) \cap K(\beta) = K$, se tiene que $G_f = V$. cuya prueba se seguirá del siguiente resultado:

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