Miscelánea Matemática **53** (2011) 139–151 SMM

Una visión breve sobre la teoría de Galois y cogalois

Fernando Barrera Mora

fbarrera10147@gmail.com

Universidad Autónoma del Estado de Hidalgo
Instituto de Ciencias Básicas e Ingeniería,
Área Académica de Matemáticas y Física

1. Introducción

En este año se está celebrando el aniversario número 200 del natalicio de Evaristo Galois (1811-1832), cuyo trabajo, sin lugar a dudas, ha sido uno de los pilares del desarrollo de diversas áreas de las matemáticas, entre las que destacan la teoría de grupos, la teoría de campos y la teoría algebraica de números.

De acuerdo con algunos autores ([**12**], pág. 41; [**8**], pág. 48), Galois tiene el mérito de haber introducido el término y el concepto de grupo, además de utilizarlo para resolver el problema más importante del álgebra de aquella época: caracterizar a las ecuaciones polinomiales en una variable que se pueden resolver por radicales. En lenguaje del propio Galois, este problema se enuncia en la forma: "Problema. ¿En qué caso una ecuación es soluble por radicales simples?" ([**8**], pág. 108). Desde una cierta perspectiva, este problema parece ser muy "práctico" y por ello se pudiese pensar que su solución no pasaría de ser un método que proporcionara una respuesta a la pregunta planteada, sin embargo la esencia y gran contribución del trabajo de Galois al abordar este problema radica en haber propuesto un método que, para los rbitros de esa época ([**16**], pág. 303) es lejos de ser práctico, como teoría matemática ha evolucionado de forma impactante estableciendo conexiones entre áreas de las matemáticas aparentemente ajenas como pueden ser la teoría de ecuaciones diferenciales y la teoría de campos. Respecto de esto me parece apropiado mencionar la opinión de A. Weyl, citado en ([**16**], págs. 304-305)

> Nada es más fructífero, como todos los matemáticos saben, que esas analogías obscuras, atisbos de niebla de una teoría con otra, esos contactos furtivos, esos revoltijos inexplicables; también nada da más placer al investigador. Un día llega cuando lo ilusorio se disipa; la vaguedad cambia en certeza; las teorías gemelas muestran su fuente común antes oculta,... La metafísica se ha transformado en matemáticas, lista para ser la sustancia de un tratado cuya belleza tranquila pudiera no movernos más.

Para adquirir una idea muy general de la esencia del trabajo de Galois y sus influyentes consecuencias en el desarrollo de las ideas matemáticas de esos días y del presente, me parece apropiado hacer un recuento breve de los trabajos previos a las aportaciones de Galois, así como una presentación, también breve, de una de las teorías algebraicas recientes: la *teoría de cogalois*, que tiene su origen en el artículo de Greither y Harrison [**10**], publicado en 1986. Este es el objetivo del presente trabajo. Seguramente la exposición de las ideas centrales no será exhaustiva, lo cual puede ser apropiado para que el lector interesado incursione en estas apasionantes áreas de las matemáticas. Para tal efecto le recomendamos consultar, entre otras, las que consideramos referencias apropiadas: [**1**], [**4**], [**8**], [**10**], [**11**], [**12**], [**16**] y [**17**].

2. Antecedentes de la teoría de Galois

Revisando los orígenes de la teoría de Galois e incluso algunos trabajos recientes ([**2**], pág. 25), se concluye que la teoría de Galois está basada en *Resolventes*, entonces es natural preguntar: ¿como surgen los resolventes y qué papel juegan en la solución por radicales de una ecuación del tipo:

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 = 0? \tag{1}$$

De acuerdo con Tignol ([**16**], pág. 67), el primero que aporta avances significativos para resolver la ecuación general es Tschirnhaus [**17**], partiendo de una idea muy simple: Dada la ecuación (1), haciendo el cambio de variable $y = x + \dfrac{a_{n-1}}{n}$, se obtiene una ecuación en y de grado n que no contiene el término de grado $n-1$. Esta idea lleva a Tschirnhaus a preguntarse por un cambio de variable más general, digamos de la forma

$$y = x^m + b_{m-1}x^{m-1} + \cdots + b_1x + b_0, \tag{2}$$

con $m < n$, para obtener una ecuación en y

$$y^n + c_{n-1}y^{n-1} + \cdots + c_1 y + c_0 = 0, \tag{3}$$

en la cual los coeficientes dependen de los m parámetros, $b_0, b_1, \ldots, b_{m-1}$; mediante una "elección adecuada" de esos, se "pueden" eliminar m de los coeficientes de (3). Tomando $m = n - 1$, se llegaría a la ecuación $y^n + c_0 = 0$, la cual se puede resolver por radicales; ahora sustituyendo este valor de y en (2), se ha de resolver una ecuación de grado menor que n. Un argumento inductivo sobre n probaría que la ecuación 1 se puede resolver por radicales. Esta idea parece ser prometedora, y tan lo es que Euler, Bezout y Lagrange la retoman más tarde, ([**16**], págs. 134-135). Es posible que estas ideas hayan llevado a Euler a conjeturar equivocadamente que las ecuaciones de grado general se pueden resolver por radicales; más precisamente, de acuerdo con Ayoub ([**4**], pág. 259) Euler escribió un artículo en el que, extrapolando los casos $2, 3$ y 4, conjeturó que las raíces de un polinomio de grado n son de la forma

$$\alpha = \sqrt[n]{A_1} + \cdots + \sqrt[n]{A_{n-1}}, \tag{4}$$

en donde A_i $(i = 1, \ldots, n-1)$ son raíces de algún polinomio $g(x)$ de grado $n - 1$. A este polinomio Euler le llamó un *resolvente* y a partir de esto a los polinomios auxiliares que se usan para encontrar las raíces de otros se les llama *resolventes*. Es importante aclarar que este no es exactamente el significado que después Lagrange y Galois dan al término resolvente, ellos llaman resolvente indistintamente a un polinomio auxiliar o a una de sus raíces. Una discusión detallada del método propuesto por Tschirnhaus se puede consultar en ([**16**], págs. 67-71).

Entre los trabajos que se pueden considerar antecesores directos del trabajo de Galois se encuentra el de Lagrange [**13**]. En este se hace un análisis de los métodos, conocidos hasta ese momento, para resolver ecuaciones de grado ≤ 4. Lo que Lagrange se plantea es identificar propiedades fundamentales (identificar patrones) con la finalidad de usarlos en la discusión de la ecuación general de grado n. En el análisis que hace de los diferentes métodos, pero de manera preponderante los propuestos por Euler y Bezout, que se asemejan al propuesto por Tschirnhaus, observa que las permutaciones de las raíces de una ecuación juegan un papel relevante. De manera más específica, para resolver las ecuaciones de grado tres introduce un elemento, $V = x_1 + \zeta x_2 + \zeta^2 x_3$, en donde ζ es una raíz cúbica de la unidad diferente de 1 y x_1, x_2 y x_3 son las raíces de la cúbica bajo análisis. Observa que al permutar las

raíces, V tiene 6 valores: $V = V_1, V_2, \ldots, V_6$, los que son solución de una ecuación de grado 6, que Lagrange llama resolvente:

$$g(X) = (X - V_1)(X - V_2)(X - V_3)(X - V_4)(X - V_5)(X - V_6) = 0, \quad (5)$$

cuyos coeficientes son simétricos en los 6 valores de V y por ende son simétricos en x_1, x_2 y x_3, por lo que son expresables en términos de los coeficientes de la ecuación original. Haciendo uso de la identidad $1 + \zeta + \zeta^2 = 0$, la ecuación (5) se reduce a $g(x) = X^6 - (V_1^3 + V_4^3)X^3 + (V_1V_4)^3 = 0$, que es una cuadrática en X^3 y se puede resolver.

Un procedimiento análogo se hace para una ecuación de grado 4, obteniendo como resolvente una ecuación de grado 24, que resulta ser la cuarta potencia de una ecuación de grado 6, y ésta a su vez se reduce a una cúbica que ya se sabe resolver.

Para el caso de ecuaciones de grado 5 el cambio es profundo, lo que lleva a Lagrange a identificar principios generales que permitan establecer la existencia de un resolvente a partir de cuyas raíces se puedan conocer las de la ecuación original.

En el lenguaje del propio Lagrange, citado en ([**16**], pág. 127) establece:

> Propongo en esta memoria examinar los diferentes métodos encontrados hasta ahora para obtener la solución algebraica de ecuaciones, y reducirlos a principios generales, y ver a priori por qué esos métodos tienen éxito para tercer y cuarto grado y fallan para grados superiores.
>
> Este examen tendrá una doble ventaja: por un lado, aportará gran visión a las soluciones conocidas de tercero y cuarto grado; por otro, será útil para aquellos que deseen abordar la solución de grados superiores, proveyéndoles de varios puntos de vista para ese fin y sobre todo ahorrándoles un gran número de pasos e intentos inútiles.

A manera de resumen, en lo que al trabajo de Lagrange concierne en la búsqueda de soluciones de ecuaciones de grado ≥ 5, podemos mencionar que Lagrange establece la existencia de un resolvente V que satisface:

1. V es expresable racionalmente en términos de las raíces de la ecuación y cantidades conocidas (números racionales, coeficientes de la ecuación y raíces de la unidad).

2. Recíprocamente, cada una de las raíces de la ecuación puede ser obtenida racionalmente en términos de V y cantidades conocidas.

Lagrange dejó pendiente contestar si el resolvente es raíz de una ecuación soluble por radicales. Este terreno fue propicio para que Ruffini (1799) y Abel (1824) probaran que la ecuación general de grado 5 no es soluble por radicales.

3. El trabajo de Galois

La teoría de Galois como se expone actualmente en la mayoría de los textos, muestra poco de lo que en realidad desarrolló Galois. Un ejemplo que ilustra bien esta afirmación, es la mera definición de lo que es el grupo de Galois de un polinomio. En términos actuales, la definición del grupo de Galois de un polinomio, se plantea como el grupo de automorfismos del campo de factorización del polinomio dado, que dejan fijo al campo base. También, pocas veces se menciona si el "Teorema Fundamental de la Teoría de Galois", que entre otras cosas establece una correspondencia biyectiva entre los subgrupos del grupo de Galois y los subcampos de la extensión, está relacionado con los resultados fundamentales que Galois demostró. Es natural pensar que la formulación actual de los resultados de Galois, por lo menos en cuanto a terminología y notación concierne, sea diferente de como los planteó el propio Galois, sin embargo parece apropiado que en toda exposición de la Teoría de Galois, se haga mención de los resultados y términos que Galois estableció. En lo que sigue expongo brevemente lo que considero las ideas fundamentales de Galois en torno al problema de solubilidad por radicales de una ecuación.

Primero, Galois retoma la idea de resolvente de una ecuación discutida por Lagrange y demuestra un par de resultados, que en lenguaje moderno equivalen a lo que se conoce como el *Teorema del Elemento Primitivo* para extensiones separables finitas. Después de esto prueba el Lema IV, que muestra la relación que existe entre los conjugados del resolvente V y las raíces de la ecuación original; estos resultados aparecen en [**8**], págs. 102-104.

Teorema 1 *(Lema II) Dada una ecuación con raíces diferentes* $a, b, c, \ldots$, *uno siempre puede formar una función* V *de las raíces tal que ningún par de valores que uno obtiene al permutar las raíces en esta función sean iguales. Por ejemplo, uno puede tomar* $V = Aa + Bb + Cc + \cdots$, *para algunos enteros apropiados* $A, B, C, \ldots$

Teorema 2 *(Lema III) Cuando la función* V *es elegida como se indicó antes, tendrá la propiedad de que todas las raíces de la ecuación dada pueden expresarse como funciones racionales de* V.

Teorema 3 *(Lema IV) Supongamos que uno ha obtenido la ecuación para V y ha tomado uno de sus factores irreducibles, así que V es raíz de una ecuación irreducible. Sean $V, V', V'', V''', \ldots$ las raíces de esta ecuación irreducible. Si $a = f(V)$ es una raíz de la ecuación dada, $f(V')$ será también raíz de la misma ecuación.*

En lenguaje actual este resultado se puede describir como sigue. Si V es un elemento primitivo para el campo de factorización de un polinomio $f(x)$; $V_1, V_2, V_3, \ldots, V_m$ son sus conjugados (raíces del irreducible de V) y $f_1(x), \ldots, f_n(x)$ son polinomios tales que $f_i(V)$ son las raíces de $f(x)$, entonces para todo $j = 1, 2, \ldots, m$, $f_1(V_j), f_2(V_j), \ldots, f_n(V_j)$ son las raíces de $f(x)$.

Estos tres resultados son la base para establecer lo que el mismo Galois llamó "nuestra teoría", ([**8**], pág. 104). El primer teorema consiste en sistematizar las ideas de Lagrange, vía la existencia del grupo de una ecuación, cuando usa permutaciones de las raíces de una ecuación en el proceso de solución.

Teorema 4 *(Proposición I) Dada una ecuación, cuyas m raíces son $a, b, c \ldots$ Siempre existe un grupo de permutaciones de las letras $a, b, c, \ldots$ el cual tiene las siguientes propiedades:*

1. *Toda función de las raíces, invariante bajo las sustituciones del grupo es racionalmente conocida;*

2. *Recíprocamente, toda función de las raíces, que puede ser expresada racionalmente, es invariante bajo esas sustituciones.*

Es importante notar que para Galois el término permutación y sustitución los utiliza como él mismo lo aclara:

> Es claro que en el grupo de permutaciones bajo consideración, el arreglo de letras no es importante, sino solamente las sustituciones de las letras, por las que nos movemos de una permutación a otra. [**12**], pág. 80.

Esto lleva a considerar que para Galois, sustitución es lo que en lenguaje actual entendemos como un elemento del grupo S_n.

En las proposiciones II-VIII ([**8**], págs. 106-113), Galois establece diversos resultados que expresan propiedades del grupo de una ecuación, particularmente, en la Proposición V, Ibid, pág. 108, la cual no es enunciada de manera explícita, Galois encuentra condiciones necesarias y suficientes para que una ecuación sea soluble por radicales. En

la proposición VII, Galois aplica sus resultados para determinar cómo debe ser el grupo de una ecuación de grado primo n, cuando es soluble por radicales. En lenguaje actual, el grupo es el producto semidirecto de los grupos cíclicos de órdenes n y $n-1$ respectivamente. Termina haciendo los cálculos explícitos para $n = 5$.

En la introducción de esta sección, mencioné que cuando se formula el *Teorema Fundamental de la Teoría de Galois*, no se establece la relación con los resultados de Galois, en particular, lo que concierne a la correspondencia entre los subgrupos del grupo de la ecuación y los subcampos del campo que se obtiene al adjuntar un resolvente. En los resultados de Galois no aparece de manera explícita esa correspondencia, aparece de manera oculta en la demostración de la proposición V, que es en donde establece condiciones necesarias y suficientes para resolver una ecuación por radicales.

3.1. La formulación de la teoría de Galois por E. Artin

> Desde mi juventud matemática he estado bajo la influencia del hechizo de la teoría clásica de Galois. Este encanto me ha forzado a regresar a ésta una y otra vez, y tratar de encontrar nuevas formas de probar sus teoremas fundamentales. *Artin*[1]

La cita anterior bien pudiera explicar lo que llevó a Artin a formular la teoría de Galois como la conocemos actualmente, sin embargo es importante mencionar que en el proceso que se inicia con el trabajo de Galois aparecen los trabajos de varios matemáticos del siglo XIX, entre los que destacan Dedekind y Weber, quienes hicieron grandes aportaciones a la teoría de números y de manera particular a la teoría de campos, usando como resolvente lo que hoy se conoce como un elemento primitivo. Estos avances no parecieron satisfacer a Artin, quien en las palabras de Kiernan lo menciona:

> Pero Artin tomó una visión revolucionaria de la teoría, y retomó el concepto implícitamente establecido por Galois y anunciado, sin ser escuchado, por Dedekind y Weber: La teoría se ocupa de la relación entre extensiones de campos y sus grupos de automorfismos. La solución algebraica

[1] "Remarques concernant la théorie de Galois," in Emil Artin Collected Papers, edited by Serge Lang & John T. Tate, Springer-Verlag, New York, Inc. 1965.

> de ecuaciones es solamente una aplicación. Entonces Artin buscó formular la teoría de manera independiente de las aplicaciones ([**12**], pág. 145).

Uno de los resultados de Artin que mejor ilustra el contenido de la cita es el siguiente:

Si G es un grupo finito de automorfismos de K y K^G denota al conjunto de elementos que dejan fijos los elementos de G entonces K/K^G es una extensión que es Galois en el sentido de Galois, es decir, el grupo G es el grupo de un polinomio con coeficientes en K^G, ([**14**], Teorema 1.8, pág. 302).

Como el mismo Artin lo establece en la cita introductoria, él buscaba la forma de probar los teoremas fundamentales de la teoría de Galois, lográndolo con la publicación de su libro ([**3**] págs. 46-49), en el que plantea su propuesta de la teoría de Galois como la conocemos hoy.

> Si $f(x)$ es un polinomio en un campo F, y E es su campo de factorización, entonces llamaremos al grupo de automorfismos de E sobre F el grupo de la ecuación $f(x) = 0$. Ahora llegamos al teorema conocido en álgebra como el *Teorema Fundamental de la Teoría de Galois* el cual establece la relación entre la estructura del campo de factorización y su grupo de automorfismos.
>
> Teorema (Teorema Fundamental). Si $p(x)$ es un polinomio separable en un campo F, y G es el grupo de la ecuación $p(x) = 0$, donde E es el campo de factorización de $p(x)$, entonces: (1) Cada campo intermedio B, es el campo fijo de un subgrupo G_B de G, y distintos subgrupos tienen distintos campos fijos. Decimos que B y G_B "se pertenecen" uno al otro. (2) El campo intermedio B es normal sobre F si y solo si el subgrupo G_B es subgrupo normal de G. En este caso el grupo de automorfismos de B que dejan fijo a F es isomorfo al grupo cociente G/G_B. (3) Para cada campo intermedio B, tenemos $[B : F]$ = índice de G_B, y $[E : B]$ = orden de G_B. *Ibid*, págs. 46-49.

4. Teoría de cogalois

La formulación de la teoría de Galois, hecha por Artin, abrió una ruta en la que se pueden abordar problemas relacionados con la red de subcampos de una extensión mediante un grupo de automorfismos. Con

este enfoque surge una pregunta natural, cuya respuesta podría aportar información valiosa para conocer la estructura de una extensión: *dada la extensión L/F, ¿se puede construir un grupo G, que dependa solamente de la extensión, de tal forma que la red de subcampos de L/F quede determinada por G?*

Otra pregunta de importancia relacionada con la red de subcampos de una extensión es: si K/F es una extensión radical, ¿se cumple que las subextensiones de K/F también lo son? Por ejemplo, tomemos la extensión $\mathbb{Q}(\zeta_7)/\mathbb{Q}$, la cual es radical cíclica de grado 6, por lo que contiene un subcampo L que tiene grado 3 sobre $\mathbb{Q}$ y no es radical, pues de otra forma $\zeta_3 \in L \subseteq \mathbb{Q}(\zeta_7)$, siendo esto imposible.

Esta última pregunta, y dado que las raíces de unidad juegan un papel importante en la descripción de las extensiones radicales, llevan a considerar las condiciones que debe satisfacer una extensión para que la red de subcampos tenga las mismas propiedades que la extensión original. Pudiera pensarse que en el ejemplo anterior, la respuesta negativa se debe a que $\mathbb{Q}(\zeta_7)$ y $\mathbb{Q}$ no tienen las mismas raíces de la unidad, por esta razón es natural considerar extensiones de $\mathbb{Q}$ generadas por radicales de la forma $\sqrt[r]{p}$, con p un número primo, o de manera más general, aquellas extensiones de la forma $\mathbb{Q}(\sqrt[n_1]{a_1}, \ldots, \sqrt[n_k]{a_k})$, para las cuales k, $a_1, a_2, \ldots, a_k$ y $n_1, n_2 \ldots, n_k$ son enteros positivos y los elementos a_i son libres de potencia n_i-ésima.

Este tipo de extensiones son los ejemplos clásicos de las extensiones que se denominan *extensiones cogalois*, término introducido por Greither y Harrison en [**10**].

En esta sección presentamos una descripción breve de la teoría de cogalois y su relación con la teoría de Galois; para una discusión completa del desarrollo de la teoría de cogalois, así como del proceso que ha seguido en los 25 años de su existencia, se recomienda consultar [**11**, Sección 1D]. Parte de la discusión que presentamos se refiere al contenido de [**5**].

4.1. Terminología y Notación

Iniciamos introduciendo los términos, notación y resultados básicos que utilizaremos en lo sucesivo. Supondremos que todas las extensiones de campos son separables.

Dado un campo F, denotaremos por: $F^* = F \setminus \{0\}$ al grupo de elementos no cero de F, $\mu(F)$ al grupo de raíces de la unidad, y para un entero positivo n, $\mu_n(F)$ representa al grupo de raíces n-ésimas de la unidad; cuando este grupo tiene orden n, ζ_n denotará a un generador fijo

de este. Si Ω/F es una extensión de Galois, $G = \mathrm{Gal}(\Omega/F)$ representa al grupo de Galois de la extensión. Una extensión de campos K/F se dice radical, si existe $\alpha \in K$ tal que $\alpha^n \in F$ para algún entero positivo n y $K = F(\alpha)$. Si $F \subseteq K$ y $S \subseteq K$, el mínimo campo que contiene a F y a S es representado por $F(S)$. Una extensión finita de los racionales se dice un campo numérico. Si K/F es una extensión de campos, $T(K/F) = \{\alpha \in K^* \ : \ \alpha^m \in F \text{ para algún entero positivo } m\}$ es el grupo de torsión de K^* sobre F^*; $\mathrm{cog}\,(K/F) = \dfrac{T(K/F)}{F^*}$ es el grupo de cogalois de la extensión y $[K : F]$ denota el grado de la extensión.

Definición 5 *[**10**, Greither y Harrison] Sea K/F una extensión de campos. Entonces K/F se dice:*

1. *conormal si* $|\mathrm{cog}\,(K/F)| = \left|\dfrac{T(K/F)}{F^*}\right| \leq [K : F]$,
2. *coseparable si $K = F(T(K/F))$, es decir, si K es generado por los elementos de torsión sobre F,*
3. *cogalois si K/F es conormal y coseparable.*

Para cada $U < \mathrm{cog}\,(K/F) = \dfrac{T(K/F)}{F^*}$, se denota a $F(\overline{U})$ por K_U, con $F^* < \overline{U} < T(K/F)$ y $U = \dfrac{\overline{U}}{F^*}$.

Definición 6 *Una extensión K/F se dice pura, si para cada primo p, $\zeta_{2p} \notin K \setminus F$.*

4.2. Resultados

El siguiente resultado es el análogo al *Teorema Fundamental de la Teoría de Galois* y justifica el nombre de la definición anterior, ésto en el sentido de la dualidad que existe entre las redes de subgrupos de $\mathrm{cog}\,(K/F) = \dfrac{T(K/F)}{F^*}$ y la de $\mathrm{Gal}\,(K/F)$, cuando la extensión es Galois y cogalois. Además, garantiza que los subcampos de una extensión generada por radicales también son generados por radicales.

Teorema 7 *[**6**, Teorema 2, (Greither y Harrison)] Sea K/F una extensión cogalois y E un subcampo intermedio $F \subseteq E \subseteq K$. Entonces:*

1. *Las extensiones K/E y E/F son extensiones cogalois,*

2. $E = K_{\mathrm{cog}\,(E/F)} = F(\overline{\mathrm{cog}\,(E/F)}) = F(T(E/F))$,

3. *para un subgrupo* U *de* $\mathrm{cog}\,(K/F)$, $\mathrm{cog}\,(K_U/F) = U$,

4. *las aplicaciones* $E \to \mathrm{cog}\,(E/F)$ *y* $U \to K_U$ *son isomorfismos inversos de redes,*

5. $\mathrm{cog}\,(K/E) \cong \dfrac{\mathrm{cog}\,(K/F)}{\mathrm{cog}\,(E/F)}$.

Un resultado importante de Greither y Harrison que caracteriza a las extensiones cogalois es:

Teorema 8 *[**6**, Teorema 4] Una extensión finita K/F es cogalois $\iff$ es coseparable, separable y pura.*

4.2.1. Problema Inverso en Teoría de Cogalois

Uno de los problemas más importantes en teoría de Galois es el que se conoce como: **Problema inverso de la teoría de Galois**, cuyo enunciado es: *dado un grupo finito G, ¿existe un campo numérico K tal que $Gal(K/\mathbb{Q}) = G$?* Hay avances muy importantes en la solución de este problema; el lector interesado puede encontrar una exposición del problema en [**15**]. Un caso sencillo pero interesante se tiene cuando G es abeliano y la respuesta se puede obtener usando extensiones ciclotómicas y el teorema de Dirichlet para sucesiones de primos en progresión aritmética.

En teoría de cogalois, el problema inverso se puede plantear de diferentes formas, pues lo primero que se nota es que el grupo de cogalois siempre es abeliano, esto lleva una restricción inicial, entonces algunas posibles preguntas son: dado un grupo abeliano finito G, ¿existe un campo numérico K tal que $K/\mathbb{Q}$ es cogalois y $\mathrm{cog}\,(K/\mathbb{Q}) = G$? Otra pregunta relacionada con la anterior es: Sea K/F una extensión abeliana y cogalois, ¿que relación hay entre $\mathrm{cog}\,(K/\mathbb{Q})$ y $\mathrm{Gal}\,(K/F)$?

En trabajos anteriores hemos abordado las preguntas planteadas, cuyas respuestas aparecen en los dos resultados siguientes:

Teorema 9 *[**6**, Teorema 12] Sea K/F una extensión abeliana y cogalois. Entonces $\mathrm{cog}\,(K/F) \cong Gal(K/F)$. En particular, si $Gal(K/F) \cong A \times B$, para algunos subgrupos A y B, entonces existen extensiones E/F y L/F tales que $\mathrm{cog}\,(E/F) \cong Gal(E/F) \cong A$ y $\mathrm{cog}\,(L/F) \cong Gal(L/F) \cong B$.*

Teorema 10 *[**6**, Teorema 23] Sean F un campo numérico y G un grupo abeliano finito, digamos $G \cong \overset{t}{\underset{i=1}{\oplus}}(\mathbb{Z}/n_i\mathbb{Z})$, con $n_1|n_2 \ldots |n_{t-1}|n_t$. Entonces existe una extensión Galois y cogalois K/F, con $Gal(K/F) \cong \operatorname{cog}(K/F) \cong G \iff \zeta_{n_{t-1}} \in F$ y $F(\zeta_{n_t})/F$ es pura.*

Si K/F es una extensión de Galois y cogalois a la vez, entonces por la dualidad que existe entre la red de subgrupos del grupo $\operatorname{cog}(K/F)$ y de $\operatorname{Gal}(K/F)$, surge una pregunta, cuya respuesta tiene por objetivo debilitar las hipótesis en el teorema anterior, es decir, ¿cuáles son las hipótesis más débiles que se pueden pedir a $\operatorname{Gal}(K/F)$ para garantizar la existencia de la extensión K/F, con F un campo numérico? La respuesta a esta pregunta se discute en [**7**] y se torna un tanto técnica, razón por la cual no presentamos su discusión en este trabajo.

Conclusión

Sin lugar a dudas, el trabajo de Galois es un pilar de la matemática ya, que ha establecido conexiones importantes entre diversas ramas de esta, mientras que en otras ha sustentado su desarrollo de manera permanente. Por ejemplo, Wiles en la demostración del *Último Teorema de Fermat* hace uso de manera preponderante de la teoría de Galois [**9**]. Por otro lado, la teoría de números algebraicos usa sistemáticamente resultados derivados del trabajo de Galois. Además, la teoría de grupos, cuyo origen es el trabajo de Galois, tiene aplicaciones importantes en disciplinas científicas tales como Química y Física.

Una visión retrospectiva de los avances de la teoría de Galois, lleva a concluir que en las diferentes épocas, las aportaciones fundamentales no se deben a un solo individuo, más bien son el resultado del trabjo de la comunidad matemática en su conjunto. Por ejemplo, los resultados de Lagrange están basados en los de: Tschirnhaus, Euler, Bezout, entre otros; así mismo, el trabajo de Galois tiene como antecedentes los avances logrados por Lagrange, Abel y Cauchy. De esta misma forma, en la segunda mitad del siglo XIX, los trabajos de Weber y Dedekind jugaron un papel central en la formulación de Artin de la teoría de Galois, lo que a la vez ha impulsado el desarrollo actual de la teoría.

Me parece apropiado mencionar que en este año se está cumpliendo el vigésimo quinto aniversario de la aparición de la teoría de cogalois, y en este corto periodo se ha consolidado como una teoría matemática que invita a ser estudiada. Esperamos que la teoría de cogalois siga su desarrollo y que las nuevas generaciones de matemáticos encuentren en

esta, motivaciones que les lleven a extenderla y aplicarla en la solución de los diversos problemas de la teoría de campos.

A manera de epílogo, si hoy tuviera que aprender nuevamente teoría de Galois, lo haría estudiando el libro de Artin [**3**].

Bibliografía

1. T. Albu, *Cogalois Theory*, Marcel Dekker, Inc., New York, Basel, 2003.
2. J. M. Arnaudiks y A. Valibouze, Lagrange resolvents, *Journal of Pure and Applied Algebra* **117-118** (1997) 23–40.
3. E. Artin, *Galois Theory*, first ed., University Notre Dame Press, Notre Dame London, 1942.
4. R. G. Ayoub, Paolo Ruffini's contributions to the quintic, *Arch. Hist. Exact Sci.* **23** (1980/81) 253–277.
5. F. Barrera-Mora, Extensiones radicales y teoría de cogalois, *Aportaciones Matemáticas* **42** (2011) 255–278.
6. F. Barrera-Mora, M. Rzedowski-Calderón, y G. Villa-Salvador, On cogalois extensions, *J. Pure Appl. Algebra* **76** (1991) 1–11.
7. ———, Allowable groups and cogalois theory, *Journal of Pure and Applied Algebra* **104** (1994) 123–147.
8. H. M. Edwards, *Galois Theory*, corrected third printing ed., Springer, New York Berlin Heidelberg, 1998.
9. G. Faltings, The Proof of Fermats Last Theorem by R. Taylor and A. Wiles, *Notices of the AMS* **42, Number 7** (1995) 743–746.
10. C. Greither y D. Harrison, A Galois correspondence for radical extensions of fields, *J. Pure Appl. Algebra* **43** (1986) 257–270.
11. M. Hazewinkel (Editor), *Handbook of Algebra: Vol. 5*, Elsevier, Amsterdam, Boston, Heidelberg, New York, Oxford, Paris y otros, 2008.
12. B. M. Kiernan, The development of Galois theory from Lagrange to Artin, *Arch. Hist. Exact Sci.* **8** (1971) 40–154.
13. J. L. Lagrange, Réflexions sur la résolution agébrique des équations, *Nouveaux Mémoires de l'Académie royale des Sciences et Belles-Lettres de Berlin* **3** (1770-1771) 205–421.
14. S. Lang, *Algebra*, second ed., Addison-Wesley Publishing Co., Massachusetts New York, 1984.
15. G. Malle y B. H. Matzat, *Inverse Galois Theory*, first ed., Springer-Verlag, Berlin, Heidelberg y otros, 1999.
16. J. P. Tignol., *Galois' Theory of Algebraic Equations*, World Scientific Publishing Co., Singapore, New Jersey, London Hong Kong, 2001.
17. E. W. Tschirnhausen, Methodus anferendi omnes terminos intermedios ex data aequatione, *Acta Eruditorum (Leipzig)* **2** (1683) 204–207.