Sección de Matemáticas
Universidad de La Laguna

Alejandro Jiménez Pérez

Elementos algebraicos y ecuaciones polinomiales de grado pequeño

Algebraic elements and small degree polynomial equations

Trabajo Fin de Grado
Grado en Matemáticas
La Laguna, Junio de 2020

Dirigido por
Ignacio García Marco

Ignacio García Marco
Matemáticas, Estadistica e Investigación Operativa
Universidad de La Laguna
38200 La Laguna, Tenerife

Agradecimientos

A Nacho, por su inestimable ayuda para realizar este trabajo y sobre todo por contagiarme una pequeña pizca de su inmensa pasión por las matemáticas.

A mi familia y de forma especial a mis padres por enseñarme a mirar el mundo con curiosidad y darme siempre el ánimo y el apoyo para seguir creciendo.

Alejandro Jiménez Pérez
La Laguna, 2 de junio de 2020

Resumen · Abstract

Resumen

El objetivo principal de esta memoria es tratar de profundizar en algunos conceptos de la Teoría de Galois. En primer lugar, comenzaremos probando la existencia de números trascendentes de forma no constructiva utilizando la equipotencia de conjuntos y de forma constructiva, demostrando explícitamente que el número de Euler es trascendente. Luego usaremos la resultante de dos polinomios para demostrar de forma constructiva que la suma y el producto de elementos algebraicos es también algebraico. También presentamos un método alternativo de resolución de las ecuaciones de tercer y cuarto grado gracias a las Transformaciones de Tschirnhaus. Finalmente, clasificaremos los grupos de Galois de cúbicas y cuárticas y caracterizaremos cuándo un polinomios de grado cinco es resoluble.

Palabras clave: *Teoría de Galois – Números trascendentes – Resultante – Polinomio mínimo – Transformaciones de Tschirnhaus.*

Abstract

The main goal of this memory is to delve into the study of some concepts in Galois Theory. Firstly, we prove the existence of transcendental numbers both with a non-constructive argument, applying equinumerosity, and explicitly, proving that Euler's number is transcendental. Afterwards, we use the resultant of two polynomials to prove constructively that the addition and product of algebraic elements is algebraic. We also see an alternative method to solve the third and fourth-degree equations by means of the Tschirnhaus transformations. Finally, we classify the Galois groups of cubic and quartics and characterize when a quintic is solvable.

Keywords: *Galois theory– Trascendental numbers –Resultant – Minimal polynomial – Tschirnhaus transformation.*

Contenido

Introducción

La resolución de ecuaciones algebraicas ha sido objeto de estudio desde la Antigüedad. Los Babilonios ya conocían desde el 1700 a. de C. la fórmula para las ecuaciones de segundo grado. Hubo que esperar al Renacimiento para encontrar los métodos de resolución para ecuaciones cúbicas, descubierto por Tartaglia y publicada por Cardano, y cuárticas, que se lo debemos a Ferrari. Pero la quíntica seguía sin estar resuelta. En 1824 el matemático noruego Abel demostró que para polinomios de grado mayor o igual que cinco no existe una formula general para obtener las raíces de un polinomio mediante sumas, productos, potencias o raíces; el denominado Teorema de Abel-Ruffini: "*El polinomio universal de grado mayor e igual a 5 no es resoluble por radicales*".

Gracias a la teoría desarrollada por Évariste Galois, antes de su prematura muerte a causa de un duelo en 1832 cuando solo tenía 20 años y que conocemos gracias a las cartas que escribió antes de morir, podemos determinar cuándo un polinomio será resoluble por radicales o no.

El objeto de central de la Teoría de Galois es el denominado grupo de Galois de un polinomio. Más concretamente, a cada polinomio de grado n se le asocia un subgrupo del grupo simétrico S_n de tal forma que el polinomio es resoluble por radicales si y solo si el correspondiente grupo de Galois es resoluble. Este resultado explica perfectamente por qué los polinomios de grado menor o igual a 4 son siempre resolubles, ya que los subgrupos de S_n con $n \leq 4$ son siempre resolubles. Asimismo, da una elegante prueba alternativa del Teorema de Abel-Ruffini: como para todo n hay un polinomio de ese grado cuyo grupo de Galois es S_n y este grupo no es resoluble para $n \geq 5$, entonces no puede haber una fórmula general (por radicales) para las raíces de un polinomio de grado ≥ 5.

El objetivo de esta memoria es profundizar en algunos aspectos de la Teoría de Galois, haciendo especial énfasis en la Teoría de Galois sobre los racionales. Este trabajo lo hemos estructurado en cinco capítulos.

En el primero probamos la existencia de elementos trascendentes sobre $\mathbb{Q}$ mediante una prueba no constructiva, es decir, demostramos que hay números

trascendentes sin aportar un elemento trascendente explícito. La prueba que presentamos está basada en el estudio de la relación de equipotencia entre conjuntos iniciada por Cantor, quién, probó en 1874 que el conjunto de los números algebraicos es numerable y que el de los números complejos no lo es pudo concluir, concluyendo que hay más trascendentes que algebraicos. También aportamos una prueba constructiva, pues demostramos que el número e es trascendente. La prueba original es de Hermite, pero nosotros hemos incluido una de David Hilbert.

En el segundo capítulo introducimos la resultante como herramienta para determinar polinomios que se anulan en la suma y el producto elementos algebraicos de los que conocemos su polinomio mínimo. Esto aporta una demostración alternativa a la usual y constructiva de que la suma y el producto de algebraicos es algebraico.

En el tercer capítulo, como otra aplicación del uso de la resultante vemos cómo resolver las ecuaciones de tercer y cuarto grado mediante cambios de variable polinomiales. El matemático alemán Tschirnhaus descubrió en el siglo XVII un método para reducir polinomios con el creyó haber resuelto la ecuación quíntica; aunque más tarde Leibniz encontró errores en sus argumentos. No obstante, las transformaciones de Tschirnhaus sí permiten resolver las ecuaciones cúbicas y cuárticas. Con ello proponemos una alternativa a los métodos de Cardano y Ferrari.

En el capítulo cuarto clasificamos el grupo de Galois de cúbicas y cuárticas de polinomios con coeficientes racionales en función de estos. Además, vemos cómo esto aporta una solución al problema inverso de Galois sobre $\mathbb{Q}$ para polinomios de grado tres y cuatro.

En el quinto capítulo estudiaremos cómo determinar si un polinomio de quinto grado es resoluble o no, además de presentar una familia de quínticas que sí es resoluble por radicales.

Nuestra principal aportación a la memoria ha sido el estudio de la bibliografía, así como su estructuración y presentación de forma ordenada. Debemos destacar la forma de detallar algunas pruebas que en la bibliografía aparecían de forma muy escueta. En el plano matemático cabe mencionar que, en el segundo capítulo presentamos una variante de la prueba del Teorema del elemento primitivo que describe otros elementos primitivos. Haciendo uso de esta variante, aportamos en la Proposición 2.24 condiciones suficientes para que cierto polinomio sea irreducible y, por ende, el polinomio mínimo de sus raíces. En el cuarto y quinto capítulo resaltamos que hemos reescrito las pruebas encontradas en la literatura para no tener que utilizar la teoría de acción de grupo sobre un conjunto.

1

Elementos trascendentes

Vamos a comenzar demostrando la existencia de elementos trascendentes sobre $\mathbb{Q}$. Para ello recurriremos a un argumento no constructivo basado en el concepto de cardinal de un conjunto, concepto que generaliza el de número de elementos de un conjunto finito. Posteriormente veremos relaciones entre conjuntos según su cardinal, para terminar dando una prueba constructiva de que e es trascendente.

1.1. Cardinal de un conjunto

En esta sección estudiaremos la equipotencia de conjuntos para luego clasificar estos según su cardinal en numerables o no numerables. En buena medida los conceptos básicos de esta sección provienen de [12].

1.1.1. Relación de equipotencia entre conjuntos

Empecemos definiendo la relación de equipotencia entre conjuntos resaltando que dos conjuntos finitos son equipotentes si tienen el mismo número de elementos. Para generalizar la equipotencia a conjuntos infinitos nos será de ayuda el Teorema de Cantor-Bernstein-Schröder.

Definición 1.1. *Sean A y B conjuntos. Decimos que* $\mathrm{Card}(A) \leq \mathrm{Card}(B)$ *si existe una aplicación inyectiva $f : A \hookrightarrow B$.*

Podemos apreciar que la relación binaria que acabamos de definir cumple las propiedades reflexiva y transitiva, pues tanto la aplicación identidad como la composición de aplicaciones inyectivas son inyectivas; por lo tanto, estamos ante una relación binaria de preorden.

Proposición 1.2. *Sean A, B dos conjuntos. Existe una aplicación $f : A \hookrightarrow B$ inyectiva si y solo si existe una aplicación $g : B \twoheadrightarrow A$ sobreyectiva.*

Demostración. Sea $f : A \to B$ una aplicación inyectiva, Fijamos $b_0 \in B$ y definimos la aplicación $g : B \to A$ tal que para todo $b \in B$,

$$g(b) = \begin{cases} f^{-1}(b) \; si \;\; b = f(a) \\ \\ b_0 \qquad si \; b \notin \mathrm{Im}(f). \end{cases}$$

Como f es inyectiva, se tiene que g está bien definida, además, es evidentemente sobreyectiva. Recíprocamente, si $g : B \to A$ es una aplicación sobreyectiva, entonces, para todo $a \in A$ existe $b \in B$ tal que $g(a) = b$. Sabemos que $g^{-1}(a) = \{b \in B \,|\, g(b) = a\} \neq \emptyset$. Elegimos, mediante el Axioma de Elección, para cada $a \in A$ un $b_a \in g^{-1}(a)$ y obtenemos que la aplicación $f : A \to B$ con $f(a) = b_a$ es inyectiva. □

Gracias a la proposición que acabamos de demostrar obtenemos una definición equivalente a la primera: existe una aplicación sobreyectiva entre B y A, si y solo si $\mathrm{Card}(A) \leq \mathrm{Card}(B)$. A continuación, nos centraremos en probar el Teorema de Cantor-Bernstein-Schröder, para ello demostraremos el siguiente lema, que afirma que toda aplicación entre las partes de un conjunto A que preserva la relación de inclusión tiene un punto fijo.

Lema 1.3. *Sea A conjunto, $K : \mathcal{P}(A) \to \mathcal{P}(A)$ cumpliendo que para todo X, Y tales que $X \subseteq Y \subseteq A$, se tiene que $K(X) \subseteq K(Y)$. Entonces, existe $Z \in \mathcal{P}(A)$ tal que $K(Z) = Z$.*

Demostración. Sean $C := \{X \in \mathcal{P}(A) \,|\, X \subseteq K(X)\}$ y $Z = \bigcup_{X \in C} X$. Para terminar la prueba veamos que $K(Z) = Z$. Tomamos un $X \in C$, como K preserva la relación de inclusión y $X \subseteq Z$, entonces $X \subseteq K(X) \subseteq K(Z)$ por lo tanto, $Z = \bigcup_{X \in C} X \subseteq K(Z)$. Veamos ahora la otra inclusión. Como $Z \subseteq K(Z) \Rightarrow K(Z) \subseteq K(K(Z))$, entonces $K(Z) \in C$ luego $K(Z) \subseteq \bigcup_{X \in C} X = Z$. □

Teorema 1.4 (Teorema de Cantor-Bernstein-Schröder). *Sean A, B conjuntos. Existen $f : A \hookrightarrow B$ y $g : B \hookrightarrow A$ aplicaciones inyectivas si y solo si existe una aplicación $h : A \leftrightarrow B$ biyectiva.*

Demostración. Sean $f : A \hookrightarrow B, g : B \hookrightarrow A$ inyectivas. Definimos primero $K : \mathcal{P}(A) \to \mathcal{P}(A)$ con $K(C) \subseteq A - g(B - f(C))$. Se aprecia que K está bien definida. Veamos que preserva la relación de inclusión, para ello, tomamos $C_1, C_2 \in \mathcal{P}(A)$ con $C_1 \subseteq C_2$ y como f y g son aplicaciones

$$K(C_1) = A - g(B - f(C_1)) = A - g(B - f(C_2)) = K(C_2).$$

Aplicando el lema anterior existe $D \subseteq A$ tal que $K(D) = D$, por lo tanto

$$A - D = g(B - f(D)).$$

Definimos ahora la aplicación $H : A \to B$

$$H(x) = \begin{cases} f(x) & si\ x \in D \\ \\ g^{-1}(x)\ si\ x \notin D. \end{cases}$$

Se aprecia H que está bien definida pues si $x \neq D$ entonces, $x \in \mathrm{Im}(g)$ y g es inyectiva. Comprobemos la inyectividad de H. Para ello tomamos $x, y \in A$ tales que $H(x) = H(y)$; distinguimos tres casos:

1. Si $x, y \in D$ tenemos que $H(z) = f(z), \forall z \in D$ y como f es inyectiva $x = y$.
2. Si $x, y \notin D$, $g^{-1}(x) = g^{-1}(y)$.
3. Si $x \in D$ e $y \notin D$. Si $H(x) = H(y)$ entonces $f(x) = g^{-1}(y)$ lo que es contradictorio porque $g^{-1}(y) \notin f(D)$ y $f(x) \in f(D)$.

Luego H es inyectiva. Comprobemos que es sobreyectiva. Sea $b \in B$. Si $y \in f(D)$ entonces y es imagen de algún elemento de A. Si $y \notin f(D)$ entonces $y \in B - f(D)$ por lo tanto será la imagen de algún elemento, $g(y) \in A - D$. Concluimos de esta manera que H es una biyección. □

Dos conjuntos infinitos son equipotentes si existe una biyección entre ambos. Luego que A y B sean equipotentes equivale a probar, gracias a el teorema anterior, que $\mathrm{Card}(A) \leq \mathrm{Card}(B)$ y $\mathrm{Card}(B) \leq \mathrm{Card}(A)$.

Teorema 1.5 (Teorema de Cantor). *Sea A un conjunto cualquiera, entonces $\mathrm{Card}(A) \leq \mathrm{Card}(\mathcal{P}(A))$, pero no son equipotentes.*

Denotaremos $\mathrm{Card}(A) < \mathrm{Card}(B)$ cuando dos conjuntos no sean equipotentes pero existe una aplicación inyectiva entre ambos.

Demostración. Como la inclusión es una aplicación inyectiva de A a $\mathcal{P}$ se tiene que $\mathrm{Card}(A) \leq \mathrm{Card}(\mathcal{P})$. Procederemos por reducción al absurdo. Supongamos que $\mathrm{Card}(\mathcal{P}(A)) \leq \mathrm{Card}(A)$ entonces existe $f : A \to \mathcal{P}(A)$ aplicación sobreyectiva. Consideramos el conjunto $B := \{a \in A \,|\, a \notin f(a)\} \subseteq A$. Como f es sobreyectiva entonces, $B \in \mathrm{Im}(f)$ luego existe $a \in A$ tal que $f(a) = B$. Si $a \in f(a) = B$ tenemos que $a \notin f(a)$ lo que es contradictorio. Por lo tanto $\mathrm{Card}(A) < \mathrm{Card}(\mathcal{P}(A))$. □

1.1.2. Conjuntos numerables y no numerables

Definición 1.6 (Conjunto numerable). *Sea A un conjunto, A es numerable si existe una aplicación inyectiva $f : A \hookrightarrow \mathbb{N}$.*

A continuación veremos algunos ejemplos de conjuntos numerables: los números racionales, la unión numerable de numerables o el anillo de polinomios con coeficientes racionales y no numerables como los reales o los complejos.

Proposición 1.7. *La unión numerable de conjuntos numerables es numerable.*

Demostración. Sean $(A_i)_{i\in\mathbb{N}}$, conjuntos numerables, entonces existen aplicaciones inyectivas $f_i : A_i \hookrightarrow \mathbb{N}$. Sea p_i el i-ésimo número primo. Definimos $g : \bigcup_{i\in\mathbb{N}} A_i \to \mathbb{N}$ donde $g(x) = p_i^{f_i(x)+1}$ con $i = \text{mín}\{j \in \mathbb{N} \,|\, x \in A_j\}$. Se puede apreciar que g es inyectiva, puesto que $\mathbb{Z}$ es un dominio de factorización única. Luego $\text{Card}(\bigcup_{i\in\mathbb{N}} A_i) \leq \text{Card}(\mathbb{N})$. Por lo tanto, $\bigcup_{i\in\mathbb{N}} A_i$ es numerable. □

Proposición 1.8. *Sean A, B conjuntos numerables, entonces $A \times B$ también es numerable.*

Demostración. Como A, B son numerables existen $f : A \hookrightarrow \mathbb{N}$, $g : B \hookrightarrow \mathbb{N}$ aplicaciones inyectivas. Definimos $h : A \times B \to \mathbb{N}^2$ tal que $h(a, b) = (f(a), g(b))$. Como h es inyectiva y $\mathbb{N}^2 = \bigcup_{i\in\mathbb{N}} \{(i, j) \,|\, j \in \mathbb{N}\}$ por la Proposición anterior se tiene que $A \times B$ es numerable. □

Cantor demostró que los números racionales son numerables, a continuación propondremos una prueba de este hecho.

Corolario 1.9. *El conjunto de los números racionales es numerable.*

Demostración. Como $\mathbb{Z}$ es numerable, por la proposición anterior, $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ es numerable. Podemos definir, $f : \mathbb{Q} \to \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ tal que para $x \in \mathbb{Q} \setminus \{0\}$ $f(a/b) = (a, b)$, siendo $a \in \mathbb{Z}$, $b \in \mathbb{Z}^+$, $\text{mcd}(a, b) = 1$ y si $x = 0$ entonces $f(0) = (0, 1)$. Se tiene que f es una inyección, luego $\mathbb{Q}$ es numerable. □

Proposición 1.10. *El anillo de polinomios $\mathbb{Q}[x]$ es numerable.*

Demostración. Como $\mathbb{Q}$ es numerable entonces existe $f : \mathbb{Q} \hookrightarrow \mathbb{N}$ aplicación inyectiva además podemos suponer sin pérdida de generalidad que $f(0) = 0$. Definamos la aplicación $g : \mathbb{Q}[x] \to \mathbb{N}$ tal que

$$f\left(\sum_{i=1}^{n} a_i x^i\right) = \prod_{i=1}^{n} p_i^{f(a_i)} \text{ donde } p_i \text{ es el i-ésimo número primo.}$$

Como hay un número finito de $a_i \neq 0$ y $f(0) = 0$, la aplicación g está bien definida, ya que el producto de finitas potencias de primos por finitos $p_i^{f(0)} = 1$ es finito y como la descomposición en factores primos es única entonces g es inyectiva. Por lo tanto $\mathbb{Q}[x]$ es numerable. □

Proposición 1.11. *El conjunto de los números reales no es numerable.*

Demostración. Supongamos que $\mathbb{R}$ es numerable, entonces como $(0,1) \subseteq \mathbb{R}$ se tiene que $\text{Card}((0,1)) \leq \text{Card}(\mathbb{N})$ y sea $f : \mathbb{N} \to (0,1)$ aplicación sobreyectiva, escribimos

$$f(i) = \sum_{j\in\mathbb{N}} a_{ij} \cdot 10^{-(j+1)} = 0, a_{i0}a_{i1}a_{i2}\dots \text{ con } a_{ij} \in \{0,\dots,9\}.$$

Elegimos $x = 0, b_0b_1b_2\dots$ con $b_i \neq a_{ii}$ y $b_i \neq 9$. Se puede apreciar que x es un número real distinto a $f(i)$ para cualquier $i \in \mathbb{N}$ y no aparece el periodo 9, entonces f no es sobreyectiva, por lo tanto $\text{Card}(\mathbb{N}) < \text{Card}((0,1))$ en consecuencia $\mathbb{R}$ no es numerable. □

Observación 1.12. El producto cartesiano no finito de conjuntos numerables no es, en general, numerable. Por ejemplo $\Delta := \{(a_0, a_1, \dots) \,|\, a_i \in \{0,1\}\} = (a_i)_{i\in\mathbb{N}}$. Veamos que $\text{Card}(\mathcal{P}(\mathbb{N})) = \text{Card}(\Delta)$, para ello definamos $f : \mathcal{P} \to \Delta$ tal que

$$f(A) = (a_i)_{i\in\mathbb{N}} \text{ con } \begin{cases} a_i = 1 \textit{ si } i \in A \\ \\ a_i = 0 \textit{ si } i \notin A. \end{cases}$$

Se aprecia que f está bien definida y es biyectiva, por lo tanto Δ no es numerable.

Proposición 1.13. *Los números complejos son equipotentes a los reales.*

Demostración. Como la inclusión es una aplicación inyectiva de $\mathbb{R} \to \mathbb{C}$ entonces $\text{Card}(\mathbb{R}) \leq \text{Card}(\mathbb{C})$. Definimos $f : \mathbb{C} \to \mathbb{R}$

$$f((\dots a_1a_0.a_{1,1}a_{1,2}\dots) + i(\dots b_1b_0.b_{1,1}b_{1,2}\dots)) = ..b_1a_1b_0a_0.b_{1,1}a_{1,1}b_{1,2}a_{1,2}\dots$$

aplicación inyectiva. Por lo tanto $\text{Card}(\mathbb{C}) = \text{Card}(\mathbb{R})$. □

1.2. Números trascendentes

Nuestro objetivo ahora será probar de manera no constructiva la existencia de números trascendentes haciendo uso de las nociones sobre cardinalidad recogidas en la sección anterior.

Definición 1.14 (Elemento algebraico). *Sea $K \hookrightarrow L$ una extensión de cuerpos. Se dice que $\alpha \in L$ es algebraico sobre K si existe $p(x) \in K[x]\backslash\{0\}$ tal que $p(\alpha) = 0$.*

Si un elemento no es algebraico se denomina trascendente. A un número complejo trascendente sobre $\mathbb{Q}$ se le denomina número trascendente.

Definición 1.15 (Clausura algebraica). *Sea K un cuerpo, existe un cuerpo $\overline{K}$ $\overline{K}$ es algebraico sobre K y algebraicamente cerrado.*

Observación 1.16. La clausura algebraica es única salvo isomorfismo de cuerpos.

Cantor demostró que existían infinitos números trascendentes probando primero que el cardinal del conjunto de los números algebraicos es numerable. Como el conjunto de los números complejos no lo es entonces el conjunto de los números trascendentes tampoco es numerable, lo que quiere decir que hay "más"números trascendentes que algebraicos.

Proposición 1.17. *El conjunto de los números trascendentes no es numerable.*

Demostración. Podemos ver $\mathbb{C}$ como $\overline{\mathbb{Q}} \bigcup T$, donde $\overline{\mathbb{Q}}$ es la clausura algebraica de $\mathbb{Q}$ y T el conjuntos de los elementos trascendentes sobre $\mathbb{Q}$. Sabemos también, por la Proposición 1.1.2 que $\text{Card}(\mathbb{N}) < \text{Card}(\mathbb{R}) = \text{Card}(\mathbb{C})$, luego $\mathbb{C}$ no es numerable. Veamos entonces que $\overline{\mathbb{Q}}$ es numerable. Para ello definimos

$$R_n := \{\alpha \in \mathbb{C} \,|\, \exists p(x) \in \mathbb{Q}[x], p(\alpha) = 0, \text{ con } \deg(p(x)) = n\}.$$

Resulta fácil ver que $\overline{\mathbb{Q}} = \bigcup_{n\in\mathbb{N}} R_n$, además si comprobamos que R_n es numerable para todo natural, por la Proposición 1.7, tendremos que $\overline{\mathbb{Q}}$ será numerable. Demostremos que los R_n son numerables.
Sabemos que $\mathbb{Q}_n[x]$, el conjunto de los polinomios de grado n con coeficientes racionales es numerable. Sea $p(x) \in \mathbb{Q}_n[x]$ mediante el Teorema fundamental del Álgebra tiene n raíces en $\mathbb{C}$, contando multiplicidades. Sea el conjunto $\{\alpha_1, \ldots, \alpha_n\}$ las raíces de $p(x)$ ordenadas tomando primero las de menor módulo y si hay dos con el mismo módulo pondremos primero la que tenga menor argumento principal, definimos ahora la aplicación $f : \mathbb{Q}_n[x] \times \{1, 2, \ldots, n\} \to R_n$ donde $f(p(x), i) = \alpha_i$. Se aprecia que f es sobreyectiva por construcción, por lo tanto $\text{Card}(R_n) \leq \text{Card}(\mathbb{Q}_n[x] \times \{1, 2, \ldots, n\}) = \text{Card}(\mathbb{N})$. Hemos obtenido que R_n es numerable y como la unión numerable de numerables es numerable (1.7) entonces $\overline{\mathbb{Q}}$ es numerable y por lo tanto $\text{Card}(\overline{\mathbb{Q}}) < \text{Card}(\mathbb{C})$ lo cual prueba que T no es numerable. □

Dado que los números algebraicos son un conjunto numerable dentro de $\mathbb{C}$, buscar números trascendentes debería ser tarea fácil, como "buscar una paja en un pajar". No obstante, decidir sobre la trascendencia de un elemento explícito es, a priori, un problema más complicado. Probaremos ahora que el número e es trascendente. Hemos de recalcar que el primer número trascendente descubierto fue la Constante de Liouville $\mathscr{L} = \sum_{i=1}^{\infty} 10^{-k!}$ en 1850 y que Lindemann demostró que π es trascendente en 1873 solucionando así el problema de la cuadratura del círculo que permanecía irresoluto desde la antigüedad.

Teorema 1.18. *El número e es trascendente.*

La prueba original es de Hermite (1873) pero nosotros expondremos una de Hilbert. [2, Teorema 20]

Demostración. Sea $k \in \mathbb{Z}^+$, definimos $J_k := \int_0^\infty x^k e^{-x} dx$ que es convergente para todo k. Si integramos por partes obtenemos que

$$J_k = \lim_{\lambda \to \infty} \left[-x^k e^{-x} \right]_0^\lambda + k \int_0^\infty x^{k-1} e^{-x} dx = k \cdot J_{k-1}.$$

Por lo tanto

$$J_k = k \cdot J_{k-1} = k(k-1) \cdot J_{k-2} = \ldots = k! \cdot J_0 = k! \tag{1.1}$$

Como consecuencia, si $p(x) \in \mathbb{Z}[x]$ y $m \geq 0$, se tiene que

$$\int_0^\infty x^m p(x) e^{-x} dx \equiv p(0) m! \qquad \text{mód } (m+1)! \tag{1.2}$$

Supongamos ahora que e es algebraico. Entonces existe un polinomio en $\mathbb{Z}[x]$ cumpliendo que:

$$a_0 + a_1 e + \ldots + a_n e^n = 0. \tag{1.3}$$

Sea $r \in \mathbb{Z}^+$ definimos:

$$I_b^c = \int_b^c x^r \left[(x-1) \ldots (x-n) \right]^{r+1} e^{-x} dx$$

con $0 \leq b \leq c \leq \infty$. Es fácil ver que la integral I_0^∞ converge pues si tomamos $f(x) := x^r \left[(x-1) \ldots (x-n) \right]^{r+1} e^{-x}$ nos basta con elegir $g(x) := x^{(n(r+1)+r)+1} e^{-x}$ que mayora a $f(x)$ y como hemos visto anteriormente (1.1) $\int_0^\infty g(x) dx$ converge y por lo tanto I_0^∞. Definamos ahora P_1 y P_2 a partir de (1.3):

$$\begin{cases} P_1 = a_0 I_0^\infty + a_1 e I_1^\infty + \ldots + a_n e^n I_n^\infty \\ \\ P_2 = a_1 e I_0^1 + \ldots + a_n e^n I_0^n. \end{cases}$$

Además podemos apreciar que $P_1 + P_2 = 0$ pues en este caso $I_0^\infty = I_0^n + I_n^\infty$. Veamos que es contradictorio, para ello vamos a probar que existe un $r \in \mathbb{Z}^+$ tal que $\dfrac{P_1}{r!}$ es un entero distinto de cero y que $\dfrac{|P_2|}{r!} < 1$. Comprobemos en primer lugar que $P_1 \neq 0$. Para ello integramos haciendo el cambio de variable $y = x - k$.

$$
\begin{aligned}
a_k e^k I_k^\infty &= a_k \int_k^\infty x^r \left[(x-1)\dots(x-n)\right]^{r+1} e^{-(x-k)} dx = \\
&= a_k \int_k^\infty (y+k)^r \left[(y+k-1)\dots(y+k-n)\right]^{r+1} e^{-y} dy = \\
&= \begin{cases} a_0 \int_0^\infty y^r p_0(y) e^{-y} & si \quad k=0 \\ \\ a_k \int_k^\infty y^{r+1} p_k(y) e^{-y} \; si \; 0 < k \leq n, \end{cases} \\
&\text{donde } p_i(y) \in \mathbb{Z}[y], 0 \leq i \leq n.
\end{aligned}
$$

Hemos demostrado que todos lo términos de P_1 son enteros, además las integrales que resultan son de la forma (1.2) donde todos los términos menos el primero son múltiplos de $(m+1)!$. Por consiguiente:

$$
\begin{aligned}
&P_1 \equiv a_0 p_0(0) r! \equiv a_0 (-1)^{n(r+1)} (n!)^{r+1} r! \qquad \text{mód } (r+1)! \quad \Rightarrow \\
&\Rightarrow P_1 = a_0 (-1)^{n(r+1)} (n!)^{r+1} r! + \lambda (r+1)!, \qquad \lambda \in \mathbb{Z}.
\end{aligned}
$$

Luego P_1 es múltiplo de $r!$ y si $P_1 = 0$ tenemos que

$$a_0 (-1)^{n(r+1)} (n!)^{r+1} + \lambda (r+1) = 0.$$

Pero esto no puede ser cierto si $r+1$ contiene un factor primo no común con $a_0 n!$. Luego si tomamos un r suficientemente grande que cumpla lo anteriormente citado para $r+1$ entonces $P_1 \neq 0$.
Busquemos ahora una cota superior de $|P_2|$. Para ello definimos:

$$M = \max_{0 \leq x \leq n} \left|x(x-1)\dots(x-n)\right|, \quad N = \max_{0 \leq x \leq n} \left|(x-1)\dots(x-n)e^{-x}\right|.$$

Sea $k \in [1,n]$ gracias a M y N podemos mayorar

$$
\begin{aligned}
\left|a_k I_0^k\right| &= |a_k| \left| \int_0^k x^r \left[(x-1)\dots(x-n)\right]^{r+1} e^{-x} dx \right| \\
&\leq |a_k| \int_0^k M^r N dx = k \left|a_k\right| M^r N.
\end{aligned}
$$

Luego obtenemos que

$$|P_2| = \left|a_1 e I_0^1 + \dots + a_n e^n I_0^n\right| \leq \left(|a_1| e + \dots + n \left|a_n\right| e^n\right) M^r N.$$

Como M es una constante

$$\lim_{r \to \infty} \frac{M^r}{r!} = 0 \quad \text{por lo tanto, si elegimos } r \text{ suficientemente grande} \quad |P_2| < r!.$$

Tomamos r suficientemente grande que además satisfaga que $r+1$ contenga un factor primo no común con $a_0 n!$. Entonces terminamos la demostración pues hemos llegado a un absurdo. □

Veamos a continuación dos resultados que nos permitirán probar, de forma rápida, la trascendencia de nuevos números a partir de otros ya conocidos.

Proposición 1.19. *Sean α, β dos números trascendentes y $\gamma \in \mathbb{C}$. Se tiene que:*

i) $\alpha + \gamma$ *o* $\alpha - \gamma$ *es trascendente.*
ii) $\beta + \alpha$ *o* $\beta\alpha$ *es trascendente.*

Demostración. Sabemos que α, β son trascendentes.

i) Supongamos que tanto $\alpha + \gamma$ como $\alpha - \gamma$ son algebraicos, entonces ambos pertenecen a $\overline{\mathbb{Q}}$. Como $\overline{\mathbb{Q}}$ es un cuerpo entonces $(\alpha + \gamma) + (\alpha - \gamma) = 2\alpha \in \overline{\mathbb{Q}}$. Luego, 2α es algebraico, lo que es contradictorio.
ii) Consideramos el polinomio $(x-\alpha)(x-\beta) = x^2-(\beta+\alpha)x+\beta\alpha$ que tiene tanto a α como a β como raíz y apreciamos que o $\alpha\beta$ o $\beta+\alpha$ son trascendentes, porque si ambos fueran algebraicos β y α lo serían, esto se debe a que la extensión $\mathbb{Q}(\alpha\beta, \alpha + \beta) \hookrightarrow \mathbb{Q}(\alpha, \beta)$ sería algebraica.

□

Observación 1.20. Utilizando a la proposición anterior y el Teorema 1.18 se tiene que o $e+\pi$ o $e-\pi$ es trascendente y o $\pi+e$ o πe es trascendente. Hemos de añadir que se desconoce si $\pi + e, \pi - e, \pi e$ o π^e son racionales o irracionales.

Entre los 23 problemas que Hilbert propuso en el Congreso Internacional de Matemáticas de 1900, el número siete trata sobre la trascendencia de algunos números. El Teorema de Gelfond-Schneider (1934) es la solución al séptimo problema.

Teorema 1.21 (Teorema Gelfond-Schneider). *Sean α, β algebraicos sobre $\mathbb{Q}$, con $\alpha \notin \{0, 1\}$ y $\beta \notin \mathbb{Q}$, entonces α^β es un número trascendente.*

Gracias a este resultado podemos saber que $2^{\sqrt{5}}, \sqrt{2}^{\sqrt{3}}$ son trascendentes. Sorprendentemente, también se prueba que e^π es trascendente pues $i^{-i} = e^{-i \cdot \mathrm{Log(i)}} = e^\pi$.

2

Elementos algebraicos

Tras haber probado la existencia de elementos trascendentes nos centraremos en los números algebraicos. No es difícil demostrar que si $K \hookrightarrow L$ es una extensión de cuerpos entonces el conjunto $\{\alpha \in L \,|\, \alpha \text{ algebraico sobre } K\}$ es un cuerpo intermedio, recordaremos una prueba en la primera sección de este capítulo. Como consecuencia de este resultado, si $\alpha, \beta \in L$ son elementos algebraicos sobre K, entonces tanto $\alpha + \beta$ como $\alpha\beta$ también lo son. No obstante, conocidos polinomios en $K[x]$ que se anulen en α y en β (como, por ejemplo, sus polinomios mínimos sobre K), no es tan fácil determinar un polinomio que se anule en $\alpha + \beta$ y en $\alpha\beta$. En este capítulo abordaremos una solución para este problema utilizando como herramienta la resultante. Hemos empleado [7], [8], [9] como bibliografía de apoyo en la elaboración de este capítulo.

2.1. Extensiones algebraicas y separables

En esta sección abordaremos algunas definiciones y resultados que nos serán útiles más adelante. Además aportaremos una variante a la demostración usual del Teorema del elemento primitivo, que nos dará nuevas formas de encontrar el elemento primitivo de una extensión finita y separable.

Definición 2.1 (Extensión algebraica). *Una extensión de cuerpos $K \hookrightarrow L$ es algebraica si todos los elementos de L son algebraicos sobre K.*

Definición 2.2 (Extensión finita). *Una extensión de cuerpos $K \hookrightarrow L$ es finita si L es un K-espacio vectorial de dimensión finita. Se llama grado de la extensión $[L : K]$ a la dimensión de L como K-espacio vectorial.*

Teorema 2.3. *Sea $K \hookrightarrow L$ una extensión de cuerpos. Entonces $K \hookrightarrow L$ es finita si y solo si $K \hookrightarrow L$ es algebraica y finitamente generada*

Proposición 2.4. *Dada la extensión de cuerpos $K \hookrightarrow L$. El conjunto de los elementos de L que son algebraicos sobre K es un cuerpo intermedio.*

Demostración. Sea $M = \{\alpha \in L \,|\, \alpha \text{ algebraico sobre } K\}$. Es evidente que $K \subseteq M \subseteq L$. Para probar que es cuerpo tomamos $x, y \in M$ y veamos que tanto $x - y$ como xy^{-1} con $y \neq 0$ pertenecen a M. Tenemos la siguiente torre de cuerpos

$$K \hookrightarrow K(x, y) \hookrightarrow L.$$

Como x, y son algebraicos sobre K la extensión $K \hookrightarrow K(x, y)$ es algebraica y finita, por lo tanto $x - y, xy^{-1} \in K(x, y)$ son algebraicos y pertenecen a M. □

Esta prueba no es constructiva, pues no nos indica cómo calcular los polinomios que se anulan $x-y, xy^{-1}$. El los objetivo principal de este capítulo es obtener una prueba constructiva de este resultado; es decir, una prueba que describa cómo obtener un polinomio que se anule en $x - y$ y otro en xy^{-1}.

Definición 2.5 (Separabilidad). *Sea K un cuerpo:*

i) Un polinomio en $K[x]$ es separable si todas sus raíces son simples (de multiplicidad uno). El siguiente enunciado sirve como caracterización:

$$f \text{ es separable si y solo si } \operatorname{mcd}(f, f') = 1.$$

ii) Sea $\alpha \in \overline{K}$, α es separable sobre K si lo es su polinomio mínimo.

iii) Una extensión $K \hookrightarrow L$ diremos que es separable si es algebraica y todo elemento de L es separable sobre K.

Observación 2.6. Si K es un cuerpo de característica 0, toda extensión algebraica de K es separable.

Reproducimos a continuación la prueba del Teorema del elemento primitivo de [7, Teorema 5.4.1].

Teorema 2.7 (Teorema del elemento primitivo). *Toda extensión finita y separable es simple.*

Demostración. Sea $K \hookrightarrow L$ una extensión finita y separable. Distinguiremos entre cuerpos finitos e infinitos.
Si K es finito se tiene que L debe ser finito entonces, $(L^*, \cdot)$ es un grupo cíclico que estará generado por un elemento α. Por lo tanto $L = K(\alpha)$.
Si K es infinito la extensión será algebraica y estará finitamente generada. Supongamos que $L = K(\beta, \gamma)$ puesto que si estuviera generada por un solo elemento el resultado sería evidente y por inducción basta solo verlo para dos. Consideramos los polinomios mínimos de β y γ con raíces $\{\beta_1, \ldots, \beta_n\}$,$\{\gamma_1, \ldots, \gamma_m\}$ respectivamente, siento $\beta = \beta_r$ y $\gamma = \gamma_s$ para ciertos r, s. Tomamos un $a \in K$ no nulo tal que

$$a \neq \frac{\beta_i - \beta_j}{\gamma_k - \gamma_l} \text{ con } i \neq j, k \neq l. \tag{2.1}$$

Como $K(\beta + a\gamma) \subseteq K(\beta, \gamma)$ solo faltaría demostrar el otro contenido. Probemos que $\gamma \in K(\beta + a\gamma)$. Sean $f(x) := m_{\beta,K}(x), g(x) := m_{\gamma,K}(x)$ y tomamos $h(x) := f(\beta + a\gamma - ax)$ y $q(x) := \text{mcd}(g, h) \in K(\beta + a\gamma)[x]$. Se puede apreciar que γ es raíz de $q(x)$ pues hace cero tanto a g como a h y que no tienen más raíces comunes ya que si δ fuera una raíz común

$$\begin{cases} g(\delta) = 0 \\ \\ h(\delta) = f(\beta + a\gamma - a\delta) \end{cases} \Rightarrow \begin{cases} \exists j \text{ tal que } \gamma_j = \delta \\ \\ \exists i \text{ tal que } \beta_i = \beta + a\gamma - a\delta \end{cases} \Rightarrow a = \frac{\beta_i - \beta}{\gamma - \gamma_j}.$$

Lo que lleva a contradicción (2.1). En conclusión, como q tiene una raíz única y γ es separable $q(x)$ tiene una raíz única entonces $q(x) = x - \gamma$, luego $\gamma \in K(\beta + a\gamma)$. Solo faltaría ver que $\beta \in K(\beta + a\gamma)$, esto es fácil de ver pues $\beta = \beta + a\gamma - a\gamma \in K(\beta + a\gamma)$. □

En esta demostración se describe cómo obtener el elemento primitivo. En la siguiente observación encontramos, basándonos en la misma idea de la prueba anterior, otros elementos primitivos.

Observación 2.8. Sea la extensión $K \hookrightarrow K(\beta, \gamma)$ donde K es un cuerpo de característica 0. Sea $a \in K$, ¿cuándo es el elemento $\beta(\gamma + a)$ primitivo?
Basta con tomar a, de forma análoga a (2.1),

$$a \neq \frac{\delta_i - \delta_j}{\gamma_k - \gamma_l} \text{ con } i \neq j, k \neq l.$$

donde los δ_i, γ_k son las raíces de $m_{\beta\gamma,K}(x)$ y $m_{\gamma,K}(x)$ respectivamente. Es fácil ver que los siguientes cuerpos son iguales.

$$K(\beta, \gamma) = K(\beta, \beta\gamma) = K(a\beta + \beta\gamma) = K(\beta(\gamma + a)).$$

2.2. Resultante de dos polinomios

Estudiaremos ahora la resultante de dos polinomios. La utilizaremos como herramienta para, dados un polinomio que se anula en α y otro que se anula en β, obtener polinomios que se anulen en $\alpha + \beta$ y $\alpha\beta$.

Lema 2.9. *Sean $f, g \in K[x]$ con $\deg(f) = n$ y $\deg(g) = m$ positivos. Entonces, f y g tienen un divisor común no unidad si y solo si existen dos polinomios $A, B \in K[x] \setminus \{0\}$ cumpliendo que $\deg(A) < m, \deg(B) < n$ y $Af + Bg = 0$*

Demostración. Supongamos sin pérdida de generalidad que $n \leq m$. Como f y g tienen un factor común no unidad existe un $h \in K[x]$ con $0 < \deg(h) \leq n$ cumpliendo que $f = h \cdot f_1$ y $g = h \cdot g_1$ donde $\deg(f_1) < n$ y $\deg(f_2) < m$. Como $g_1 \cdot f - f_1 \cdot g = g_1 \cdot h \cdot f_1 - f_1 \cdot h \cdot g_1 = 0$. Tomamos $A = g_1$ y $B = -f_1$. Recíprocamente, supongamos por reducción al absurdo que f y g no tienen un factor común, entonces $\mathrm{mcd}(f, g) = 1$, luego existen $C, D \in K[x]$ tal que $Cf + Dg = 1$ entonces

$$B = BCf + DBg = BCf - DAf = f(BC - DA).$$

Luego f divide a B con B no nulo, luego $\deg(B) \geq m$, lo que no es posible, entonces f y g tienen un factor común. □

Definición 2.10 (Matriz de Sylvester). *Sean* $f(x) = \sum_{i=0}^{n} f_i x^i$, $g(x) = \sum_{j=0}^{m} g_j x^j$ *polinomios, de grado* n *y* m *respectivamente, en* $K[x]$. *Se denomina matriz de Sylvester de* f *y* g *respecto a* x *a la matriz cuadrada de orden* $n + m$

$$\mathrm{Syl}_x(f,g) := \begin{pmatrix} f_0 & 0 & \cdots & 0 & g_0 & 0 & \cdots & 0 \\ f_1 & f_0 & \cdots & 0 & g_1 & g_0 & \cdots & 0 \\ f_2 & f_1 & \ddots & 0 & g_2 & g_1 & \ddots & 0 \\ \vdots & \ddots & \ddots & \vdots & \vdots & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \vdots & g_m & g_{m-1} & \ddots & \vdots \\ f_n & f_{n-1} & \ddots & \vdots & 0 & g_m & \ddots & \vdots \\ 0 & f_n & \ddots & \vdots & 0 & 0 & \ddots & \vdots \\ 0 & 0 & \ddots & \vdots & 0 & 0 & \ddots & \vdots \\ 0 & 0 & \cdots & f_n & 0 & 0 & \cdots & g_m \end{pmatrix} \tag{2.2}$$

Definición 2.11 (Resultante). *La resultante de dos polinomios* f *y* g *respecto a una variable* x *es el determinante de la matriz de Sylvester de* f *y* g *respecto a* x. *Es decir,*

$$\mathrm{Res}_x(f,g) := \det(\mathrm{Syl}_x(f,g)).$$

Proposición 2.12. *Sean dos polinomios* $f, g \in K[x]$ *con* $\deg(f), \deg(g) > 0$. *Entonces,* $\mathrm{mcd}(f, g) = 1$ *si y solo si* $\mathrm{Res}_x(f, g) \neq 0$.

Demostración. Sean $f = \sum_{i=1}^{n} f_i x^i, g = \sum_{i=1}^{m} g_i x^i \in K[x]$. Sabemos que tienen un factor común en $K[x]$ si y solo si existen $A, B \in K[x] \setminus \{0\}$ tal que $Af + Bg = 0$ con $\deg(A) < m, \deg(B) < n$, por el Lema 2.9.

$$Af + Bg = \sum_{i=0}^{n+m} \left(\sum_{j=0}^{i} (a_j f_{i-j} + b_j g_{i-j}) \right) x^i,$$

donde se entiende que a_i, b_j, f_k, g_l vale 0 cuando el subíndice sea negativo o mayor que el grado de A, B, f, g respectivamente. Si escribimos matricialmente esta igualdad, se tiene:

$$\mathrm{Syl}_x(f,g) \begin{pmatrix} a_0 \\ \vdots \\ a_{m-1} \\ b_0 \\ \vdots \\ b_{n-1} \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ \vdots \\ \vdots \\ 0 \end{pmatrix}$$

Tenemos que $\mathrm{Res}_x(f,g) = \det(\mathrm{Syl}_x(f,g)) = 0$ si y solo si el sistema planteado es compatible indeterminado, lo que es equivalente a que existan A, B en las condiciones del Lema 2.9, por lo tanto, f, g tienen un factor común no unidad. □

Veremos ahora que la resultante se puede escribir en función de las raíces de los polinomios. Para ello utilizaremos una proposición y un lema técnico.

Lema 2.13. *Sea D un dominio de factorización única. Sean $f(x) \in D[x]$ y $d \in D$. Entonces, $f(d) = 0$ si y solo si $(x-d)$ divide a f. En particular, si $g \in K[x_1, \ldots, x_n]$ con K un cuerpo, se tiene que $g(x_1, \ldots, x_i, \ldots, x_{j-1}, x_i, x_{j+1}, \ldots, x_n) = 0$ si y solo si $(x_i - x_j)$ divide a g.*

Demostración. Sea $d \in D$, definimos $\varphi : D[x] \to D[x]$ el único homomorfismo de anillos tal que

$$\begin{cases} \varphi(a) = a,\ a \in D \\ \\ \varphi(x) = d. \end{cases}$$

Veamos que $\ker(\varphi) = (x - d)$. Como $x - d \in \ker(\varphi)$ entonces $(x - d) \subseteq \ker(\varphi)$. Sea $p(x) \in \ker(\varphi)$ entonces

$$\begin{aligned} p(x) = \sum_{i=1}^{n} a_i x^i = \sum_{i=1}^{n} a_i ((x-d)+d)^i = (x-d)q(x) + \sum_{i=1}^{n} a_i d^i = \\ = (x-d)q(x) + \varphi(p(x)) = (x-d)q(x). \end{aligned}$$

Hemos obtenido que $(x - d)$ divide a $p(x)$. Para terminar la prueba basta con tomar $D[x_j] = K[x_1, \ldots, x_n]$ y $d = x_i$. □

En el siguiente resultado vamos a considerar la resultante de dos polinomios f y g genéricos como polinomio en los coeficientes de f y g y como polinomio en las raíces de f y g y vamos a calcular su grado en cada caso. Recordamos que un polinomio es homogéneo si todos sus términos tienen el mismo grado.

Proposición 2.14. *Sean* $f(x) = \sum_{i=0}^{n} f_i x^i$, $g(x) = \sum_{j=0}^{m} g_j x^j$ *polinomios en* $K[x]$ *con raíces* $\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_m$ *respectivamente. Entonces:*

i) $\mathrm{Res}_x(f,g) \in \mathbb{Z}[f_0, \ldots, f_n, g_0, \ldots, g_m]$ *de grado* $n+m$.
ii) $\mathrm{Res}_x(f,g) \in \mathbb{Z}[\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_m]$ *homogéneo de grado* $n \cdot m$.

Demostración. Probaremos por orden.

i) A partir de la fórmula general del determinante para una matriz A cuadrada de orden k.

$$\det(A) = \sum_{\sigma \in S_k} \mathrm{sgn}(\sigma) a_{\sigma(1)1} \ldots a_{\sigma(k)k}. \tag{2.3}$$

Como $\mathrm{Res}_x(f,g) = \det(\mathrm{Syl}_x(f,g))$, la matriz de Sylvester es de orden $n+m$ y las entradas de la matriz son o bien 0 o bien f_i o g_j, entonces, la resultante considerada como polinomio en las variables $f_0, \ldots, f_n, g_0, \ldots, g_m$, tendrá grado menor o igual que $n+m$. Al ser la identidad la única permutación con la que se obtiene la diagonal principal en (2.3) se tiene que $f_0^m g_m^n$ solo aparece una vez en el sumatorio (2.3) y con coeficiente 1. Por lo tanto, el grado de la resultante es $n+m$.

ii) Sea s_{ij} el elemento (i,j) de $\mathrm{Syl}_x(f,g)$, con $1 \leq i,j \leq n+m$. Si $j \leq m$ entonces $s_{ij} = f_{i-j}$ si $0 \leq i-j \leq n$, mientras que $s_{ij} = 0$ en cualquier otro caso. Además, como $f = \sum_{j=0}^{n} f_j x^j = f_n \prod_{i=1}^{n} (x - \alpha_i)$ se tiene que

$$f_k = f_n \sum_{\substack{\mathrm{Card\}(A)=n-k \\ A \subseteq \{1,\ldots,n\}}} (-1)^{n-k} \left(\prod_{a_k \in A} a_k \right)$$

es un polinomio homogéneo en $\alpha_1, \ldots, \alpha_n$ de grado $n-k$. Por lo tanto, s_{ij} es 0 o un polinomio homogéneo de grado $n-i+j$, para todo $j \leq m$. Ahora, cuando $m \leq j \leq n+m$ entonces $s_{ij} =_{i-j+m}$ si $m \leq i-j \leq n+m$, mientras que en cualquier otro caso $s_{ij} = 0$. Procediendo como antes obtenemos que s_{ij} es 0 o un polinomio homogéneo de grado $m-i+j-m = j-i$, para todo $m \leq j \leq m+n$. Sea $\sigma \in S_{n+m}$, entonces $s_{\sigma(1)1} \ldots s_{\sigma(n+m)n+m}$ es 0 o un polinomio homogéneo de grado $\sum_{j=1}^{n+m} \deg(s_{\sigma(i)i}) = \sum_{j=1}^{m} \deg(s_{\sigma(j)j}) + \sum_{j=m+1}^{m+n} \deg(s_{\sigma(j)j}) = \sum_{j=1}^{m} n - \sigma(j) + j +$

$\sum_{j=1}^{m} j - \sigma(j) = n \cdot m - \sum_{j=1}^{n+m} \sigma(j) + \sum_{j=1}^{n+m} j = n \cdot m$. En conclusión, $\mathrm{Res}_x(f, g)$ es una suma de polinomio homogéneos de grado $n \cdot m$ y por lo tanto, es un polinomios homogéneo de grado $n \cdot m$.

□

Proposición 2.15. *Sean* $f(x) = f_n \prod_{i=1}^{n}(x - \alpha_i)$ *y* $g(x) = g_m \prod_{j=1}^{m}(x - \beta_j)$ *con* $f, g \in K[x]$*, entonces*

$$\mathrm{Res}_x(f, g) = (-1)^{nm} f_n^m g_m^n \prod_{i=1}^{n}\prod_{j=1}^{m}(\alpha_i - \beta_j) = (-1)^{nm} f_n^m \prod_{i=1}^{n} g(\alpha_i) = g_m^n \prod_{j=1}^{m} f(\beta_j).$$

Demostración. Probaremos primero los dos primeros miembros de la igualdad. Hemos demostrado en la Proposición 2.14 que la resultante es un polinomio homogéneo de grado $n \cdot m$ en las raíces. Si existen i, j tal que $\alpha_i = \beta_j$ se tiene que f y g tienen una raíz común, entonces $\mathrm{Res}_x(f, g) = 0$. Aplicando el Lema 2.13 tenemos que $(\alpha_i - \beta_j)$ divide a $\mathrm{Res}_x(f, g)$, luego $\prod_{i}^{n}\prod_{j}^{m}(\alpha_i - \beta_j)$ divide a $\mathrm{Res}_x(f, g)$. Es fácil ver que $\prod_{i}^{n}\prod_{j}^{m}(\alpha_i - \beta_j)$ es homogéneo de grado nm puesto que $(\alpha_i - \beta_j)$ es un polinomio homogéneo y el producto de homogéneos también lo es. Además, por la Proposición 2.14 la resultante es homogénea en las raíces. Como el producto de las raíces divide a la resultante y ambos del mismo grado, entonces se diferencian en una unidad, es decir

$$\mathrm{Res}_x(f, g) = c \prod_{i=1}^{n}\prod_{j=1}^{m}(\alpha_i - \beta_j).$$

Evaluamos en los polinomios $f(x) = f_n(x - 1)^n$ y $g(x) = g_m x^m$ cuyas raíces son 1 y 0 respectivamente y obtenemos que la diferencia del producto de las raíces es 1 y que la matriz Sylvester es triangular, luego el determinante es el producto de la diagonal principal, es decir

$$\mathrm{Res}_x(f,g) = \begin{vmatrix} (-1)^n f_n & 0 & \cdots & 0 & 0 & 0 & \cdots & 0 \\ k_1 & (-1)^n f_n & \cdots & 0 & 0 & 0 & \cdots & 0 \\ k_2 & k_1 & \ddots & 0 & 0 & 0 & \ddots & 0 \\ \vdots & \ddots & \ddots & \vdots & \vdots & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \vdots & g_m & 0 & \ddots & \vdots \\ f_n & k_{n-1} & \ddots & \vdots & 0 & g_m & \ddots & \vdots \\ 0 & f_n & \ddots & \vdots & 0 & 0 & \ddots & \vdots \\ 0 & 0 & \ddots & \vdots & 0 & 0 & \ddots & \vdots \\ 0 & 0 & \cdots & f_n & 0 & 0 & \cdots & g_m \end{vmatrix} = (-1)^{nm} f_n^m g_m^n,$$

de esta forma hemos demostrado la igualdad. Para comprobar los otros de miembros veamos que

$$\prod_{i=1}^{n}(\alpha_i - \beta_j) = g(\alpha_i) \Rightarrow (-1)^{nm} f_n^m g_m^n \prod_{i=1}^{n}\prod_{j=1}^{m}(\alpha_i - \beta_j) = (-1)^{nm} f_n^m \prod_{i=1}^{n} g(\alpha_i)$$

$$\prod_{j=1}^{m}(\alpha_i - \beta_j) = (-1)^{nm} f(\beta_j) \Rightarrow (-1)^{nm} f_n^m g_m^n \prod_{i=1}^{n}\prod_{j=1}^{m}(\alpha_i - \beta_j) = g_m^n \prod_{i=1}^{n} f(\beta_j).$$

□

La resultante no solo es útil para conocer si dos polinomios tienen una raíz común, sino que se puede utilizar, por ejemplo, para determinar cuando un polinomio tiene raíces dobles, como veremos en la Sección 2.4. Nosotros la emplearemos en la próxima sección para obtener el polinomio mínimo de la suma y el producto de dos elementos conociendo previamente el polinomio mínimo de estos.

2.3. El polinomio mínimo de la suma y el producto de elementos algebraicos.

Definición 2.16 (Polinomio mínimo). *Sea $K \hookrightarrow L$ una extensión de cuerpos y sea $\alpha \in L$ algebraicos sobre K. Sea $\varphi : K[x] \to K(\alpha)$, donde $\varphi(p(x)) = p(\alpha)$. Se denomina polinomio mínimo de α sobre K al generador mónico del* $\ker\varphi$.

Como $K[x]$ es un dominio de ideales principales, el polinomio mínimo está bien definido.. El polinomio mínimo se denota por $m_{\alpha,K}(x)$ y es el polinomio de grado más pequeño mónico e irreducible en $K[x]$ del que α es una raíz.

Proposición 2.17. *Sean f, g dos polinomios en $K[x]$ de grados n y m con raíces α y β respectivamente. Entonces:*

i) *Tanto* $\mathrm{Res}_y(f(x-y), g(y)) \in K[x]$ *como* $\mathrm{Res}_y(y^n f(x/y), g(y)) \in K[x]$ *tienen grado* nm.
ii) $\mathrm{Res}_y(f(x-y), g(y))$ *es un polinomio en* $K[x]$ *que se anula en* $\alpha+\beta$.
iii) $\mathrm{Res}_y(y^n f(x/y), g(y))$ *es un polinomio en* $K[x]$ *que se anula en* $\alpha\beta$.

Demostración. Sean $\{\alpha_1, \ldots, \alpha_n\}$ y $\{\beta_1, \ldots, \beta_m\}$ las raíces de f y g respectivamente. Se deduce inmediatamente que las resultantes de (ii) y (iii) están en $K[x]$ puesto que las filas correspondientes a f en la matriz de Sylvester se forman con monomios pertenecientes a $K[x]$, mientras que las filas correspondientes a g tiene elementos de K y su determinante será un polinomio en $K[x]$.

i) Determinaremos el grado de $\mathrm{Res}_y(f(x-y), g(y)) \in K[x]$. Vemos que los coeficientes de $g(y)$ no dependen de x, por lo tanto serán constantes en K. Se tiene que

$$f(x-y) = \sum_{i=1}^{n} a_i (x-y)^i = \sum_{i=1}^{n} a_i \left[\sum_{k=0}^{i} (-1)^k \binom{n}{k} x^{i-k} y^k \right] = \sum_{j=1}^{n} f_j y^j,$$

donde

$$f_j = \sum_{i=j}^{n} (-1)^i a_i \binom{n}{j} x^{i-j}.$$

Se aprecia que $\deg_x(f_j) \leq n-j$ y que $\deg_x(f_0) = n$, es decir, el f_0 es el monomio con mayor grado. Al introducir los coeficientes a la matriz de Sylvester y calcular el determinante, se puede comprobar que el mayor grado lo obtendremos al multiplicar los monomios que están en la diagonal principal (2.2) y que este es exactamente $g_m^n f_0^n$, polinomio en $K[x]$ de grado exactamente $n \cdot m$. Nos quedaría garantizar que no obtenemos otro coeficiente de grado $n \cdot m$ que anule al anterior. Esto se debe a que el término de grado $n \cdot m$ se consigue al multiplicar f_0 m veces y esto solo ocurre al multiplicar la diagonal principal, pues la única permutación que multiplica todos los elementos de la diagonal principal es la identidad. Procedemos de la misma forma con $\mathrm{Res}_y(y^n f(x/y), g(y))$. Hemos de mencionar si $f(x) = \sum_{i=0}^{n} a_i x^i$, entonces $y^n f(x/y) = \sum_{i=0}^{n} a_i x^i y^{n-i} \in K[x,y]$.

ii) Ya demostramos (Proposición 2.15) que

$$\mathrm{Res}_y(f(x-y), g(y)) = (-1)^{nm} f_n^m g_m^n \prod_{i=1}^{n} \prod_{j=1}^{m} (a_i(x) - \beta_j)$$

Donde $a_i(x) = x - \alpha_i$ son las raíces de $f(x-y)$. Haciendo $x = \alpha+\beta$ se tiene que $a_i(x) - \beta_j = 0$ para ciertos i, j. Luego $\mathrm{Res}_y(f(x-y), g(y))$ se anula en $\alpha+\beta$.

iii) Aplicando el mismo procedimiento que hemos utilizado para demostrar (ii) pero considerando $a_i(x) = x/\alpha_i$ llegamos a que $\alpha\beta$ anula a $\mathrm{Res}_y(y^n f(x/y), g(y))$.

□

Utilizando las resultantes expuestas en la proposición anterior enunciaremos dos resultados que nos permitirán obtener múltiplos del polinomio mínimo de la suma y el producto de dos algebraicos conociendo previamente sus polinomios mínimos.

Corolario 2.18. *Sean α y β algebraicos sobre K tales que $f(x) = m_{\alpha,K}(x)$ y $g(x) = m_{\beta,K}(x)$. Entonces,* $\mathrm{Res}_y(f(x-y), g(y))$ *se anula en $\alpha+\beta$. En particular, $m_{\alpha+\beta,K}(x)$ divide a* $\mathrm{Res}_y(f(x-y), g(y))$.

Demostración. Gracias a la Proposición 2.17 $\mathrm{Res}_y(f(x-y), g(y))$ es un polinomio en $K[x]$ que se anula en $\alpha+\beta$. Luego, por la definición de polinomio mínimo $m_{(\alpha+\beta),K}(x)$ divide a $\mathrm{Res}_y(f(x-y), g(y))$. □

Veamos a continuación dos ejemplos de cálculo del polinomio mínimo de la suma. Primero uno donde el polinomio buscado coincide con la resultante. En segundo lugar veremos cómo la resultante obtenida no es irreducible y, por tanto, el polinomio mínimo es uno de sus factores irreducibles.

Ejemplo 2.19. Veamos cómo calcular el polinomio mínimo de $\alpha := \sqrt{2}+\sqrt{3}$ en $\mathbb{Q}[x]$. Sean $f(x) := m_{\sqrt{2},\mathbb{Q}}(x)$, $g(x) := m_{\sqrt{3},\mathbb{Q}}(x)$. Se tiene que

$$f(x-y) = y^2 - 2xy - x^2 - 2 \qquad g(y) = -3 + y^2$$

$$\mathrm{Res}_y(f(x-y), g(y)) = \begin{vmatrix} x^2-2 & 0 & -3 & 0 \\ -2x & x^2-2 & 0 & -3 \\ 1 & -2x & 1 & 0 \\ 0 & 1 & 0 & 1 \end{vmatrix} = x^4 - 10x^2 + 1 \in \mathbb{Q}[x].$$

Se puede apreciar que el polinomio obtenido es mónico y se anula en α. Aplicando el Teorema del elemento primitivo (Teorema 4.17) a la extensión $\mathbb{Q} \hookrightarrow \mathbb{Q}(\sqrt{2},\sqrt{3})$ de grado 4 se obtiene que $\mathbb{Q}(\sqrt{2},\sqrt{3}) = \mathbb{Q}(\alpha)$. Al ser el polinomio de grado 4 será el mínimo.

Ejemplo 2.20. Veamos un ejemplo de cómo el método propuesto no siempre nos da el polinomio mínimo de $\alpha+\beta$. Para ello tomamos $\alpha := \sqrt{2}+\sqrt{3}$ y $\beta := -\sqrt{3}$. Tenemos que $f(x) := m_{\sqrt{2}+\sqrt{3},\mathbb{Q}}(x)$, $g(x) := m_{-\sqrt{3},\mathbb{Q}}(x)$. Calculando la resultante

$$\begin{aligned} \mathrm{Res}_y(f(x-y), g(y)) &= x^8 - 32x^6 + 216x^4 - 512x^2 + 400 \\ &= (x^2-2)^2(x^4 - 28x^2 + 100). \end{aligned}$$

El polinomio obtenido es múltiplo del polinomio mínimo de $\alpha+\beta = \sqrt{2}$.

Corolario 2.21. *Dados α y β algebraicos sobre K. Si $f(x) = m_{\alpha,K}(x)$ y $g(x) = m_{\beta,K}(x)$. Entonces, $\alpha\beta$ es raíz de $\mathrm{Res}_y(y^{\deg(f)}f(x/y), g(y))$. En particular, $m_{\alpha\beta,K}(x)$ divide a $\mathrm{Res}_y(y^{\deg(f)}f(x/y), g(y))$.*

Demostración. Sabemos por la Proposición (2.15) que $\mathrm{Res}_y(y^{\deg(f)}f(x/y), g(y))$ es un polinomio en $K[x]$ que se anula en $\alpha\beta$. Luego, por la definición de polinomio mínimo $m_{(\alpha\beta),K}(x)$ divide a $\mathrm{Res}_y(y^{\deg(f)}f(x/y), g(y))$. □

Presentamos ahora dos ejemplos de cálculo del polinomio mínimo del producto.

Ejemplo 2.22. El polinomio mínimo de $\sqrt{2}\cdot\omega$ en $\mathbb{Q}[x]$, donde ω es una raíz primitiva tercera de la unidad. Sean $f(x) = x^2 - 2$, $g(x) = x^2 + x + 1$ los polinomios mínimos de $\sqrt{2}$ y ω respectivamente. Mediante el Corolario 2.21 se obtiene:

$$y^3 f(x/y) = x^2 - 2y^2 \qquad g(y) = 1 + y + y^2$$

$$\mathrm{Res}_y(y^2 f(x/y), g(y)) = \begin{vmatrix} x^2 & 0 & 1 & 0 \\ 0 & x^2 & 1 & 1 \\ -2 & 0 & 1 & 1 \\ 0 & -2 & 0 & 1 \end{vmatrix} = x^4 + 2x^2 + 4$$

No es difícil comprobar que este polinomio es irreducible y, por tanto, el polinomio mínimo de $\sqrt{2}\cdot\omega$.

Ejemplo 2.23. El polinomio mínimo de $\alpha\beta$ en $\mathbb{Q}[x]$. Donde $\alpha := \sqrt[3]{3}$ y $\beta := \sqrt[3]{2}\omega$ con ω es una raíz primitiva tercera de la unidad. Sean $f(x) := m_{\alpha,\mathbb{Q}}(x), g(x) := m_{\beta,\mathbb{Q}}(x)$. Tenemos que

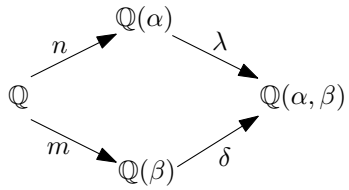
$$\mathrm{Res}_y(y^3 f(x/y), g(y)) = x^9 - 18x^6 + 108x^3 - 216 = (x^3 - 6)^3$$

El polinomio obtenido es múltiplo del polinomio mínimo, que es $x^3 - 6$.

Tras un proceso de experimentación observamos que en la mayoría de casos los polinomios obtenido en los Corolarios 2.18 y 2.21 son el polinomio mínimo de la suma y el producto respectivamente. A continuación daremos una condición suficiente para que el polinomio obtenido sea el polinomio mínimo de la suma y/o el producto.

Proposición 2.24. *Sean α, β elementos algebraicos sobre K cuyos polinomios mínimos $f(x), g(x)$ tienen grados n, m respectivamente. Si $\mathrm{mcd}(n, m) = 1$, entonces el polinomio mínimo de $\alpha + a\beta$ es $a^{nm}\mathrm{Res}_y(f(x - y), g(y/a))$ y el polinomio mínimo de $\alpha(\beta + a)$ es $\mathrm{Res}_y(y^n f(x/y), g(y - a))$ salvo para un número finito de valores de a, que no exceden a $\binom{n}{2}\binom{m}{2}$.*

Demostración. Tenemos que $[\mathbb{Q}(\alpha):\mathbb{Q}] = n$ y $[\mathbb{Q}(\beta):\mathbb{Q}] = m$, podemos construir las siguientes torres de cuerpos.



Se tiene que $\lambda \leq m$ y $\delta \leq n$, además, $n \cdot \lambda = m \cdot \delta$, entonces n divide a $m \cdot \delta$ y como tenemos que $\delta \leq n$ y $\mathrm{mcd}(n,m) = 1$ por lo tanto $\delta = n$ lo que no lleva a que $m = \lambda$ con lo que demostramos que $[\mathbb{Q}(\alpha,\beta):\mathbb{Q}] = n \cdot m$. Falta ahora por determinar si bajo nuestras hipótesis, $\mathbb{Q}(\alpha,\beta) = \mathbb{Q}(\alpha+\beta)$. Para ello recurrimos a la demostración del Teorema del elemento primitivo. Se tiene que $\mathbb{Q}(\alpha,\beta) = \mathbb{Q}(\alpha + a\beta)$ con $a \neq \dfrac{\alpha_i - \alpha_j}{\beta_r - \beta_s}$. Es fácil comprobar, aplicando la Proposición 2.15 y el Corolario 2.18, que el polinomio mínimo de $\alpha + a\beta$ es $a^{nm}\mathrm{Res}_y(f(x-y), g(y/a))$ salvo cuando no la igualdad de cuerpos no sea cierta para ese a, cosa que ocurre como máximo para $\binom{n}{2}\binom{m}{2}$ elementos. Procedemos análogamente para $\alpha(\beta + a)$. □

2.4. El discriminante de un polinomio

Veremos ahora una segunda aplicación de la resultante, el cálculo del discriminante, el cual emplearemos en el Capítulo 4 para determinar cómo son las raíces y el grupo de Galois de algunos polinomios.

Definición 2.25 (Discriminante). *Dado un polinomio* $f(x) = \sum_{i=0}^{n} f_i x$ *con coeficientes en un cuerpo, el discriminante es*

$$\Delta(f) = \frac{(-1)^{\frac{n(n-1)}{2}}}{f_n}\mathrm{Res}_x(f, f')$$

Veremos a continuación otra forma de definir el discriminante y probaremos que son equivalentes utilizando la Proposición 2.15.

Proposición 2.26. *Sea* $f(x) = f_n \prod_{i=1}^{n}(x-\alpha_i) \in K[x]$ *se tiene la siguiente igualdad:*

$$\Delta(f) = f_n^{2n-2}\left(\prod_{i<j}(\alpha_i - \alpha_j)\right)^2.$$

Demostración. Sabemos que $f'(x) = f_n \sum_{i=1}^{n} \prod_{j\neq i}(x-\alpha_j)$, por lo tanto $f'(\alpha_i) = f_n \prod_{j\neq i}(\alpha_i - \alpha_j)$. Obtenemos de la Proposición 2.15:

$$\begin{aligned}\mathrm{Res}_x(f,f') &= (-1)^{n(n-1)} f_n^{n-1} \prod_{k=1}^{n} f'(\alpha_k) = (-1)^{n(n-1)} f_n^{n-1} \prod_{k=1}^{n} \left[\left(\prod_{i\neq k} (\alpha_k - \alpha_i) \right) f_n \right] \\ &= (-1)^{\binom{n}{2}} f_n^{2n-1} \left(\prod_{i<k} (\alpha_k - \alpha_i) \right)^2 .\end{aligned}$$

Ajustando las constante tenemos que

$$\Delta(f) = f_n^{2n-2} \left(\prod_{i<k} (\alpha_i - \alpha_k) \right)^2 .$$

□

Una de las utilidades del discriminante es la de proporcionar un método para saber si un polinomio es separable, como indica el siguiente Corolario.

Corolario 2.27. *Sea f un polinomio en $K[x]$. Entonces, $\Delta(f) = 0$ si y solo si f tiene una raíz múltiple.*

Demostración. Por la Proposición 2.12 se tiene que $\Delta(f) = \mathrm{Res}_x(f,f') = 0$ si y solo si f y f' tienen un factor en común, luego no son coprimos, por lo tanto f tiene una raíz múltiple. □

Ejemplo 2.28. En la tabla a continuación, describimos explícitamente el discriminante de varias familias de polinomios de grado ≤ 5 en función de sus coeficientes.

Polinomio	Discriminante (Δ)
$x^3 + ax^2 + bx + c$	$a^2b^2 - 4b^3 - 4a^3c + 18abc - 27c^2$
$x^3 + bx + c$	$-4b^3 - 27c^2$
$x^4 + ax^2 + bx + c$	$16a^4c - 4a^3b^2 - 128a^2c^2 + 144ab^2c - 21b^2 + 256c^3$
$x^4 + ax^2 + c$	$14c(4c - a^2)^2$
$x^4 + bx + c$	$256c^3 - 27b^4$
$x^5 + ax + b$	$256a^5 + 3125b^4$

3

Resolución de ecuaciones utilizando transformaciones de Tschirnhaus

Ehrenfried Walther von Tschirnhaus publicó en 1683 un método para reducir polinomios, las trasformaciones de Tschirnhaus. Utilizando este método se pueden resolver ecuaciones de tercer y cuarto grado. Tschirnhaus creyó que sirviéndose de estas transformaciones podría convertir cualquier polinomio de quinto grado en $y^5 + a$, eligiendo la transformación $y = x^4 + A_3x^3 + A_2x^2 + A_1x + A_0$ adecuada. No obstante, Leibniz probó que encontrar los A_i precisos con los que convertir cualquier quíntica en la forma anteriormente mencionada requería, como paso intermedio, obtener una solución explícita de una ecuación de quinto grado general, y como bien sabemos eso no es siempre posible, por el Teorema de Abel-Ruffini. Sin embargo, Bring y más tarde Jerrard probaron usando las ideas de Tschirnhaus que cualquier quíntica se puede reducir a la forma $x^5 + ax + b$. Además, por el Teorema 5.9 (que veremos en el capítulo 5) sabemos cuándo estas serán resolubles.

En este capítulo veremos cómo resolver las ecuaciones de tercer y cuarto grado utilizando transformaciones Tschirnhaus. Esto supone una alternativa a los métodos clásicos de Cardano y Ferrari y esbozaremos cómo demostrar los resultados de Bring y Jerrard usando las mismas ideas (no incluimos la demostración entera puesto que requiere de muchos cálculos intermedios).

La idea principal del método de Tschirnhaus es que para calcular las raíces de un polinomio $p(x) \in \mathbb{Q}[x]$, vamos a hacer transformaciones del tipo $y = h(x)$ para cierto polinomio $h(x)$. Además elegiremos $h(x)$ de tal forma que el polinomio $p(x)$ transformado sea mucho más simple. Por ejemplo, en caso de que $p(x)$ tenga grado 3, conseguiremos que el polinomio transformado sea $x^3 + c$. De esta forma, si $\beta_1, \ldots, \beta_r$ son las raíces del polinomio $p(x)$ transformado, entonces las raíces de $p(x)$ se obtienen resolviendo $\beta_i = h(x)$ para todo $i \in \{1, \ldots, r\}$. Para hacer las citadas transformaciones nos serviremos de la resultante introducida en el capítulo anterior. Para elaborar este capítulo nos hemos basado en [1] y [11].

3.1. Ecuación cúbica

El objetivo de esta sección es mostrar el método alternativo de Tchirnhaus para resolver la cúbica. Para ello partimos de una cúbica (mónica) general $p(x) = x^3 + px^2 + qx + r \in \mathbb{Q}[x]$. Realizando una transofrmación lineal del tipo $x \to x - \frac{p}{3}$, podemos suponer que el polinomio es de la forma $f(x) = x^3 + ax + b$. Si $a = 0$, entonces la resolución de la cública $f(x)$ es directa y las raíces son $\sqrt[3]{-b} \cdot \omega^i, i \in \{0, 1, 2\}$ siendo $\omega = e^{2i\pi/3}$. Supondremos a partir de ahora que $a \neq 0$. Utilizaremos la transformación $y = x^2 + mx + n$ con n, m bien elegidas tales que el polinomio resultante $y^3 + A_2y^2 + A_1y + A_0$ tenga coeficientes $A_2 = A_1 = 0$. Es decir, obtendermos un polinomio $q(y) = y^3 + A_0$, del que podremos conocer fácilmente sus raíces. Para realizar este cambio de variable utilizaremos la resultante y la Proposición 2.15; veamos cómo.

Sea $f(x) \in \mathbb{Q}[x]$ un polinomio de tercer grado con raíces $\alpha_1, \alpha_2, \alpha_3$ se tiene que

$$\begin{aligned} \mathrm{Res}_x(f(x), y - (x^2 + mx + n)) &= \prod_{i=1}^{3} (y - \alpha_i^2 - \alpha_i m - n) \\ &= y^3 + A_2y^2 + A_1y + A_0 = q(y), \end{aligned} \tag{3.1}$$

donde los $A_i \in \mathbb{Q}[\alpha_1, \alpha_2, \alpha_3, m, n]$.

Por lo tanto, si conocemos las raíces β_i de $q(y)$ podremos conocer las raíces de f que se obtendrán al resolver la ecuación $\beta_i = \alpha_i^2 + \alpha_i m + n$. No obstante, para cada β_i obtendremos dos posibles α_i, es decir, seis posibles raíces. Debemos comprobar cuáles son las verdaderas raíces de f.

Veamos entonces cómo encontrar el polinomio $q(y)$ adecuado. Para ello calculamos la resultante (3.1) y obtenemos los coeficientes

$$A_2 = 2a - 3n \qquad A_1 = a^2 + am^2 - 4an + 3bm + 3n^2.$$

Haciendo $A_1 = A_2 = 0$ y sustituyendo n en la segunda ecuación obtenemos una ecuación de segundo grado en m. Tras haber obtenido n, m adecuados

$$n = \frac{2a}{3} \qquad m = \frac{-3b \pm \sqrt{9b^2 + \frac{4a^3}{3}}}{2a}$$

ya podemos obterner las raíces de $q(y)$ fácilmente. Vale la pena comentar que no siempre m será racional; no obstante, siempre será raíz de un polinomio de grado 2 con coeficientes en $\mathbb{Q}$ (y, por tanto, expresable por radicales).

Ejemplo 3.1. Consideramos el polinomio $f(x) = x^3 - x - 1$. Se tiene que los coeficientes adecuados para la transformación son $n = -\frac{2}{3}$ y $m = \frac{-9+\sqrt{69}}{6}$o $m = \frac{-9-\sqrt{69}}{6}$. Al elegir el primer m obtenemos

$$q(y) = y^3 + \frac{1}{216}(2116 - 276\sqrt{69}).$$

Calculamos las raíces de q. A partir de las raíces de q, calculamos las de f resolviendo $\beta_i = x^2 + \frac{-9+\sqrt{69}}{6}x - \frac{2}{3}$ para $i \in \{1, 2, 3\}$. Y obtenemos, para β_1, las raíces α_1 y α_1'. Se puede comprobar que α_1 no es raíz de f mientras que α_1' sí lo es. Procedemos de forma análoga para β_2 y β_3 y se obtiene lo siguiente (hemos puesto en color verde las raíces de f y en rojo las que no lo son).

$$\beta_1 = \frac{1}{3}\sqrt[3]{\frac{69\sqrt{69}}{2} - \frac{529}{2}} \quad \begin{cases} \alpha_1 \approx -1.2092 \\ \alpha_1' \approx 1.3247 \end{cases}$$

$$\beta_2 = -\frac{1}{3}\sqrt[3]{-\frac{23}{2}(3\sqrt{69} - 23)} \quad \begin{cases} \alpha_2 \approx -0.66236 + 0.56228i \\ \alpha_2' \approx 0.77792 - 0.56228i \end{cases}$$

$$\beta_3 = (-1)^{2/3}\frac{1}{3}\sqrt[3]{\frac{23}{2}(3\sqrt{69} - 23)} \quad \begin{cases} \alpha_3 \approx -0.66236 - 0.56228i \\ \alpha_3' \approx 0.77792 + 0.56228i \end{cases}$$

3.2. Ecuación cuártica

Hay varias formas de resolver una cuártica por medio de transformaciones de Tschirnhaus, nosotros proponemos aquí la siguiente astucia: mediante una transformación cuadrática bien elegida, trasnformaremos una cuártica en una cuártica bicuadrada, que es fácil de resolver. Cabe destacar que para elegir los coeficientes de la trasformación cuadráctica que nos conviene, hemos de resolver una ecuación cúbica. Así que, en resumen, podemos resolver una ecuación de grado cuatro resolviendo una cúbica y una ecuación de grado 4 bicuadrática. Sea $f(x) = x^4 + ax^2 + bx + c \in \mathbb{Q}[x]$, como en el caso anterior comenzaremos aplicando la transformación cuadrática $y = x^2 + mx + n$ al polinomio f, es decir,

$$\mathrm{Res}_x(f(x), y - (x^2 + mx + n)) = y^4 + A_3y^3 + A_2y^2 + A_1y + A_0.$$

Nos interesará ahora elegir la transformación adecuada para que $A_1 = A_3 = 0$, donde:

$$A_3 = 2a - 4n$$
$$A_1 = bm^3 + (4c - 2an)m^2 + (ab - 6bn)m - 2a^2n + 2ac + 6an^2 - b^2 - 4cn - 4n^3.$$

Observamos que para obtener $A_3 = 0$, basta con tomar $n = a/2$. Luego, al sustituir este valor de n en la expresión de A_1 tenemos un polinomio de grado a lo sumo 3 en la variable m, que podemos resolver (mediante Cardano o resolviendo la cúbica con el método de Tschirnhaus propuesto anteriormente). Al igual que antes, se observa que tanto m como n se pueden calcular explícitamente y son expresables por radicales. Tras elegir estos valores de m y n obtendremos el polinomio bicuadrado $q(y) = y^4 + A_2y^2 + A_0$. Si obtenemos las cuatro raíces β_i podremos despejar resolver la ecuación $\beta_i = \alpha_i^2 + m\alpha_i + n$ para cada i, obteniendo así ocho candidatos a raíz de f. Finalmente, debemos elegir los α_i que, efecctivamente, sean raíces de f.

3.3. Ecuación de quinto grado

Si siguiendo las ideas de las secciones anteriores, pudiéramos llegar a un polinomio de la forma $y^5 + A_0$ entonces, toda quíntica sería resoluble por radicales. Dado que no es este el caso, nos conformaremos con transformar toda quíntica a la forma de Bring-Jerrard.

Definición 3.2 (Forma de Bring-Jerrard). *Decimos que un polinomio de grado 5 está en forma de Bring-Jerrard si es de la forma* $x^5 + ax + b$.

Teorema 3.3 (Teorema de Bring-Jerrard). *La equación* $x^5 + c_4x^4 + c_3x^3 + c_2x^2 + c_1x + c_0 = 0$ *es equivalente a una ecuación* $x^5 + ax + b = 0$*, donde* a, b *son expresiones radicales en* $\mathbb{Q}[c_0, \ldots, c_4]$.

No probaremos este Teorema por falta de espacio, pero la demostración está en [11]. La forma de Bring-Jerrard de un polinomio $f(x)$ de grado 5 se puede obtener mediante una trasnformación $y = h(x)$ donde $h(x)$ es un polinomio conveniente de grado 4. Para la elección de los coeficientes de $h(x)$, buscamos que $\mathrm{Res}_x(f(x), y - h(x)) = y^5 + ay + b$; es decir, que los coeficientes de y^2, y^3 e y^4 sean cero. Las demostraciones de que se puede elegir un $h(x)$ con la propiedad anterior que se encuentran en la bibliografía son largas, no son tan directas como en los casos de la cúbica y la cuártica y suelen hacer uso de las fórmulas de Newton. En el Capítulo 5 veremos cuando una quíntica en forma Bring-Jerrard es resoluble por radicales.

4

El grupo de Galois de cúbicas y cuárticas

El objetivo de este capítulo es proporcionar resultados que caractericen el grupo de Galois de polinomios cúbicos y cuárticos en $\mathbb{Q}[x]$ a partir de sus coeficientes. Los principales resultados obtenidos en este sentido son el Teorema 4.24, para polinomios de tercer grado y el Teorema 4.32, que servirá como clasificación de los grupos de Galois para polinomios de cuarto grado. Finalmente comentaremos brevemente la relación de los resultados de este capítulo con el problema inverso de Galois, pues las clasificaciones obtenidas en estos teoremas nos permiten encontrar todos los subgrupos de S_3 y de S_4 como grupos de Galois de polinomios de grado a lo sumo 4. Hemos seguido como bibliografía de referencia para este capítulo [5], [6] y [7].

4.1. El grupo de Galois

En esta primera sección recordaremos algunas definiciones y teoremas a los que nos referiremos más adelante. Además demostraremos algunos resultados técnicos que nos serán de utilidad para determinar los grupos de Galois en las siguientes secciones de este capítulo.

Definición 4.1 (Grupo de Galois). *Sea $K \hookrightarrow L$ una extensión de cuerpos, el grupo de Galois de L sobre K es el conjunto de los automorfismos de L que restringidos a K son la inclusión, es decir,*

$$\mathrm{Gal}(L : K) = \{\sigma \in \mathrm{Aut}(L) \,|\, \sigma_{|K} = i\}.$$

La operación de este grupo es la composición de aplicaciones.

Definición 4.2 (Cuerpo de descomposición). *Sea $f(x) \in K[x]$, el cuerpo de descomposición de f sobre K es el menor cuerpo que contiene a K y a todas las raíces de f.*

Definición 4.3 (Extensión normal). *Una extensión $K \hookrightarrow L$ algebraica, es normal si todo polinomio irreducible $f(x) \in K[x]$ con una raíz en L tiene todas sus raíces en L.*

Teorema 4.4 (Caracterización de extensiones normales finitas). *Sea $K \hookrightarrow L$ una extensión finita. Entonces, es normal si y solo si existe un polinomio en $f(x) \in K[x]$ tal que L es su cuerpo de descomposición de f sobre K.*

Definición 4.5 (K-inmersión). *Sea $K \hookrightarrow L$ una extensión algebraica. Se denomina K-inmersión de L a cualquier monomorfismo $\phi : L \to \overline{K}$ tal que $\phi_{|K} = i$ (es decir, ϕ restringida a K es la inclusión).*

El siguiente resultado describe las K-inmersiones de una extensión algebraica simple.

Proposición 4.6. *Sea α algebraico sobre K y sea $m_{\alpha,K}(x)$ su polinomio mínimo. Entonces la siguiente aplicación es biyectiva.*

$$\begin{aligned}\{\beta \,|\, \beta \text{ es raiz de } m_{\alpha,K}(x)\} &\longrightarrow \{\phi : K(\alpha) \longrightarrow \overline{K} \,|\, \phi \text{ es una } K-\text{inmersion}\} \\ \beta &\mapsto \phi_\beta : K(\alpha) \longrightarrow \overline{K} \text{ con } \phi_\beta(\alpha) = \beta\end{aligned}$$

En consecuencia hay tantas K-inmersiones de $K(\alpha)$ como raíces tenga $m_{\alpha,K}(x)$.

También nos será útil la proposición siguiente, que afirma que toda K-inmersión de un cuerpo intermedio se puede extender

Proposición 4.7. *Sea $K \hookrightarrow L$ una extensión algebraica y M un cuerpo intermedio. Si $\gamma : M \to \overline{K}$ es una K-inmersión, entonces existe una K-inmersión $\sigma : L \to \overline{K}$ que extiende a γ, es decir, $\sigma_{|M} = \gamma$.*

Veamos que se puede caracterizar la normalidad de una extensión por medio de las K-inmersiones.

Teorema 4.8. *Sea $K \hookrightarrow L$ una extensión algebraica. Entonces, $K \hookrightarrow L$ es normal si y solo si las imágenes de todas las K-inmersiones de L están contenidas en L*

Definición 4.9 (Extensión de Galois). *Una extensión se dice de Galois si es finita normal y separable.*

Proposición 4.10. *Sea $K \hookrightarrow L$ una extensión finita, entonces $|\mathrm{Gal}(L : K)| \leq [L : K]$. Además, si $K \hookrightarrow L$ es de Galois se tiene que $|\mathrm{Gal}(L : K)| = [L : K]$.*

Si $f(x) \in K[x]$ es un polinomio con raíces $\{\alpha_1, \ldots, \alpha_n\}$ y L su cuerpo de descomposición sobre K, se tiene que todo elemento del grupo de Galois se corresponde con una permutación de las raíces de f. Como consecuencia, podemos definir un monomorfismo de grupos entre $\mathrm{Gal}(L : K) \to S_n$, de forma que $\sigma(\alpha_i) = \alpha_{\tau(i)}$, donde $\sigma \in \mathrm{Gal}(L : K)$ y $\tau \in S_n$.

Proposición 4.11. *Sea $f(x) \in K[x]$ un polinomio de grado n y L el cuerpo de descomposición de f sobre K. Entonces*

$$\mathrm{Gal}(L : K) \cong H \leq S_n$$

Como consecuencia de las Proposiciones 4.6, 4.7 y del Teorema 4.8 se tiene el siguiente resultado.

Proposición 4.12. *Sea $K \hookrightarrow L$ una extensión de Galois y sea $x \in L$. Entonces $x \in K$ si y solo si para todo $\sigma \in \mathrm{Gal}(L : K)$ se cumple que $\sigma(x) = x$.*

Definición 4.13 (Extensión radical y resoluble). *Una extensión $K \hookrightarrow L$ es radical si existen los cuerpos*

$$K = K_0 \subset K_1 \subset \ldots \subset K_n = L$$

donde dado un $\gamma_i \in K_i$ se tiene que $K_i = K_{i-1}(\gamma_i)$ con $\gamma_i^{m_i} \in K_{i-1}, m_i > 0, \forall i$. Una extensión $K \hookrightarrow L$ es resoluble si existe otra extensión $L \hookrightarrow M$ tal que $K \hookrightarrow M$ es radical.

Definición 4.14 (Polinomio resoluble por radicales). *Sea $f(x) \in K[x]$ y L su cuerpo de descomposición sobre K. Diremos que f es resoluble por radicales si $K \hookrightarrow L$ es resoluble.*

Que un polinomio sea resoluble por radicales es equivalente a que las raíces se puedan expresar en términos de los coeficientes usando sumas, restas, productos, divisiones, potencias y raíces. Ahora ya podemos presentar el Gran Teorema de Galois, que reduce el problema de decidir si un polinomio (separable) es resoluble por radicales a un problema de teoría de Grupos.

Teorema 4.15 (Gran Teorema de Galois). *Sea $K \hookrightarrow L$ una extensión de Galois, son equivalentes:*

i) $K \hookrightarrow L$ *es una extensión resoluble.*
ii) $\mathrm{Gal}(L : K)$ *es un grupo resoluble.*

Nuestro siguiente objetivo es el de demostrar el Teorema 4.17 que caracteriza los polinomios (separables) irreducibles de grado n como aquellos cuyo grupo de Galois es un subgrupo transitivo de S_n.

Definición 4.16. *Sea H un subgrupo de S_n, decimos que es transitivo si para todo par de elementos $i, j \in \{1, \ldots, n\}$ existe $\tau \in H$ tal que $\tau(i) = j$.*

Teorema 4.17. *Sea $f(x) \in K[x]$ separable de grado n y L su cuerpo de descomposición. Entonces, f es irreducible si y solo si $\mathrm{Gal}(L : K)$ es un subgrupo transitivo de S_n*

Demostración. Sea $\Omega = \{\alpha_1, \ldots, \alpha_n\}$ el conjunto de las raíces de f. Sabemos que $L = K(\alpha_1, \ldots, \alpha_n)$. Dado un $\alpha \in \Omega$ arbitrario, podemos plantear la siguiente torre de cuerpos.

$$K \hookrightarrow K(\alpha) \hookrightarrow L \hookrightarrow \overline{K}$$

Definimos, $\tau_1 : K(\alpha) \to \overline{K}$ la K-inmersión tal que $\tau_1(\alpha) = \beta \in \Omega$. Extendemos τ_1 para cada β, es decir, gracias a la Proposición 4.6 podemos definir $\tau : L \to \overline{K}$ monomorfismo de cuerpos tal que τ restringido a K es la inclusión. Además como la extensión es normal, mediente el Teorema 4.8 se tiene que $\mathrm{Im}(\tau) \subseteq L$ luego existe $\sigma : L \to L$ en las mismas condiciones de τ, con $\sigma \in \mathrm{Gal}(L : K)$. Luego $\sigma(\alpha_i) = \alpha_j$, para todo i, j. Por lo tanto el grupo de Galois es transitivo. Recíprocamente, sea h un factor irreducible de f con $\deg(h) \leq n$. Entonces existe al menos una raíz α_i de f común a h. Sea α_j otra raíz de f, como $\mathrm{Gal}(L : K)$ es transitivo existirá $\sigma \in \mathrm{Gal}(L : K)$ tal que $\sigma(\alpha_i) = \alpha_j$, como σ es K-inmersión, entonces α_j también debe ser raíz de h. Se tiene entonces que h tiene al menos n raíces, por lo tanto $\deg(h) \geq n$, de lo que concluimos que $h = a \cdot f$, con $a \in K \setminus \{0\}$. Por lo tanto, que f es irreducible. □

Nuestro siguiente objetivo es presentar un criterio para decidir cuándo el grupo de Galois de un polinomio separable $f \in \mathbb{Q}[x]$ de grado n es un subgrupo del grupo alternado A_n. Para ayudarnos primero probaremos este Lema técnico.

Lema 4.18. *Sea $\sigma = (ab) \in S_n$ una trasposición con $1 \leq a < b \leq n$ entonces, el siguiente conjunto tiene número impar de elementos.*

$$\{(a, b) \,|\, 1 \leq i < j \leq n, \sigma(i) > \sigma(j)\}.$$

Demostración. Es fácil ver que si $i < j$, entonces $\sigma(i) > \sigma(j)$ si y solo si $i = a \leq j \leq b$ o $a \leq i < j = b$ y esto ocurre $2(b - a) - 1$ veces. □

Proposición 4.19. *Sean $f(x) \in \mathbb{Q}[x]$ un polinomio separable de grado n, su discriminante Δ y sea L su cuerpo de descomposición sobre $\mathbb{Q}$. Entonces,* $\mathrm{Gal}(L : \mathbb{Q}) \leq A_n$ *si y solo si* $\sqrt{\Delta} \in \mathbb{Q}$.

Demostración. Supongamos sin pérdida de generalidad que $f(x)$ es un polinomio mónico. Sea $\delta = \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)$, por la Proposición 2.26 se tiene que $\delta \in K$ y $\delta^2 = \Delta \in \mathbb{Q}$. Tomamos $\sigma \in \mathrm{Gal}(L : \mathbb{Q}) \leq S_n$, como pertenece al grupo de Galois permuta las raíces de f, luego tenemos, por el lema anterior, y gracias al hecho de que todo ciclo se puede descomponer en trasposiciones que

$$\sigma(\delta) = \prod_{1 \leq i < j \leq n} (\sigma(\alpha_i) - \sigma(\alpha_j)) \Rightarrow \sigma(\delta) = \mathrm{sgn}(\sigma)\delta.$$

Que aparezca la signatura en la expresión anterior se debe a que, como consecuencia del Lema 4.18, cada trasposición produce un número impar de cambios de signo. Por lo tanto, $\sigma(\delta) = \pm\delta$ y como f es separable, entonces $\delta \neq 0$ y se tiene que $\sigma \in A_n$ si y solo si $\operatorname{sgn}(\delta) = 1$. Es decir, el grupo de Galois $\operatorname{Gal}(L : \mathbb{Q})$ es un subgrupo de A_n si y solo si $\sigma(\delta) = \delta)$ para todo $\delta \in Gal(L : \mathbb{Q})$ y, por la Proposición 4.12,esto es equivalente a que $\delta = \sqrt{\Delta} \in \mathbb{Q}$. □

En las siguientes secciones, para clasificar el grupo de Galois, necesitaremos ser capaces de detectar las raíces racionales y saber el número de raíces reales de un polinomio. Para ello usaremos los siguientes resultados.

Proposición 4.20. *Sea* $f(x) = \sum_{i=1}^{n} a_i x^i \in \mathbb{Z}[x]$. *Si* $\alpha = \frac{\beta}{\gamma} \in \mathbb{Q}$ *con* $\operatorname{mcd}(\beta, \gamma) = 1$, *es raíz de* f, *entonces* β *divide a* a_0 *y* γ *divide a* a_n.

Teorema 4.21 (Teorema de Sturm). *Sea* $f(x) \in \mathbb{Q}[x]$, *definimos la siguiente cadena*

$$f_0 = f(x), \quad f_1 = f'(x), \quad \text{y si } f_{k-1} \notin K \text{ entonces } f_k = -\operatorname{Resto}(f_{k-2}, f_{k-1}).$$

Si $f_r \in K$ *obtenemos las sucesiones de signos.* $S_+ = (f_0^+, \ldots, f_r^+)$ *y* $S_- = (f_0^-, \ldots, f_r^-)$, *donde* g^+ *es el signo* $(+$ *o* $-)$ *del coeficiente líder de* $g(x)$ *y* g^- *es el signo del coeficiente líder de* $g(-x)$. *Si denotamos por* σ_+ *(respect.* σ_-*) el número de cambios de signo en* S_+ *(respect.* S_-*), entonces el número de raíces reales de* f *es* $|\sigma_- - \sigma_+|$.

Una prueba del teorema de Sturm puede encontrarse en [3, Teorema 2.55].

4.2. Grupo de Galois de una ecuación cúbica

Para determinar el grupo de Galois un polinomio $f(x) = x^3 + ax^2 + bx + c$ de la expresión del discriminante dada en el Ejemplo 2.28.

Proposición 4.22. *Sea* $f(x) \in \mathbb{Q}[x]$ *un polinomio de grado 3. Sea* α *una raíz cualquiera de* f *y sea* Δ *su discriminante. Entonces el cuerpo de descomposición de* f *sobre* $\mathbb{Q}$ *es* $\mathbb{Q}(\alpha, \sqrt{\Delta})$. *Como consecuencia, si* f *tuviera una raíz racional el cuerpo de descomposición el cuerpo de descomposición de* f *sobre* $\mathbb{Q}$ *es* $\mathbb{Q}(\sqrt{\Delta})$.

Demostración. Supongamos que $f(x)$ mónico con raíces $\{\alpha, \alpha_2, \alpha_3\}$. Sea $L = \mathbb{Q}(\alpha, \alpha_2, \alpha_3)$ el cuerpo de descomposición de f sobre $\mathbb{Q}$. Podemos expresar $f(x) = (x-\alpha)g(x)$, con $g(x) = (x-\alpha_2)(x-\alpha_3)$ y $g(\alpha) \neq 0$. Mediante la fórmula cuadrática para $g(x)$ en $\mathbb{Q}(\alpha)$ se tiene que $L = \mathbb{Q}(\alpha)(\alpha_2, \alpha_3) = \mathbb{Q}(\alpha)(\sqrt{\Delta(g)})$. Al ser $\Delta = \Delta(f) = (\alpha_1 - \alpha_2)^2(\alpha_1 - \alpha_3)^2(\alpha_2 - \alpha_3)^2 = g(\alpha)^2\Delta(g)$ hemos probado que $L = \mathbb{Q}(\alpha, \sqrt{\Delta})$. Si f es reducible tiene al menos una raíz racional. Si tomamos α como esa raíz en el razonamiento anterior, tenemos que $\mathbb{Q}(\alpha, \sqrt{\Delta}) = \mathbb{Q}(\sqrt{\Delta})$. □

Determinemos el grupo de Galois de un polinomio cúbico, para ello tomemos un $f(x) \in \mathbb{Q}[x]$ mónico, con raíces $\{\alpha_1, \alpha_2, \alpha_3\}$. Distingamos 4 casos.

(1) Si todas las raíces son racionales, el cuerpo de descomposición será $\mathbb{Q}$, luego $\mathrm{Gal}(\mathbb{Q} : \mathbb{Q}) = \{1\}$.
(2) Si $f(x)$ tiene una sola raíz α_1 racional y dos que no lo son, el polinomio será reducible con un factor de grado dos $g(x)$ irreducible. Además una raíz se puede expresar en función de la otra, $\alpha_2 = \lambda\alpha_3^{-1}$ con $\lambda \in \mathbb{Q}$. Por lo tanto, el cuerpo de descomposición del polinomio sobre $\mathbb{Q}$ es $\mathbb{Q}(\alpha_2)$ y como α_2 es raíz de un polinomio mónico e irreducible $[\mathbb{Q}(\alpha_2) : \mathbb{Q}] = 2$, luego $\mathrm{Gal}(\mathbb{Q}(\alpha_2) : \mathbb{Q}) \cong \mathbb{Z}_2$.
(3) Si posee una raíz real no racional α_1 y dos complejas no reales α_2, α_3. el polinomio es irreducible. Como $[L : \mathbb{Q}] \leq 3!$ con L el cuerpo de descomposición de f sobre $\mathbb{Q}$, tenemos la siguiente torre de cuerpos y los siguiente grados.

$$\mathbb{Q} \overset{3}{\hookrightarrow} \mathbb{Q}(\alpha_1) \overset{2}{\hookrightarrow} \mathbb{Q}(\alpha_1, \alpha_2) \overset{1}{\hookrightarrow} \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3)$$

Luego el cuerpo de descomposición sera $\mathbb{Q}(\alpha_1, \alpha_2)$ y como la extensión es de grado 6 el grupo de Galois es isomorfo a S_3.
(4) Si todas las raíces son reales no racionales el polinomio es irreducible, luego su grupo de Galois debe ser transitivo, por el Teorema 4.17, y los únicos subgrupos transitivos de S_3 son el propio S_3 y A_3. Distinguimos dos casos:
  (4.1) Si $\sqrt{\Delta} \in \mathbb{Q}$ por la Proposición 4.19 tenemos que el grupo de Galois es subgrupo de A_3, entonces $\mathrm{Gal}(L : \mathbb{Q}) \cong A_3$.
  (4.2) Si $\sqrt{\Delta} \notin \mathbb{Q}$ nuevamente por la Proposición 4.19 tenemos que no es subgrupo de A_3, entonces $\mathrm{Gal}(L : \mathbb{Q}) \cong S_3$.

Para distinguir entre los casos estudiaremos cómo son las raíces en función de los coeficientes del polinomio. Si queremos determinar las raíces racionales utilizamos la Proposición 4.20 y así distinguimos cuándo estamos ante el caso (1) o (2).

En caso de que $f(x)$ sea irreducible, para diferenciar entre A_3 y S_3 haremos uso de la siguiente proposición.

Proposición 4.23. *Sea $f(x) \in \mathbb{Q}[x]$ un polinomio mónico e irreducible de tercer grado. Si $\sqrt{\Delta} \in \mathbb{Q}$ entonces f tiene tres raíces reales no racionales.*

Demostración. Sean $\alpha_1, \alpha_2, \alpha_3$ las raíces de f. Supongamos por reducción al absurdo que $\alpha_2, \alpha_3 \in \mathbb{C} \setminus \mathbb{R}$. Como $\sqrt{\Delta} = (\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)(\alpha_2 - \alpha_3) \in \mathbb{Q}$. Al ser α_2 el conjugado de α_3, entonces $\sqrt{\Delta} = \lambda \cdot 2i \cdot \mathrm{Im}(\alpha_2) \notin \mathbb{Q}$, para cierto $\lambda \in \mathbb{R}$. Esto supone una contradicción. □

Teorema 4.24 (Clasificación del grupo de Galois de una cúbica). *Sean $f(x) = x^3 + ax^2 + bx + c \in \mathbb{Q}$, Δ el discriminante de f y L el cuerpo de descomposición de f sobre $\mathbb{Q}$, se tiene que:*

i) Si f se descompone en $\mathbb{Q}$ entonces $\mathrm{Gal}(L:\mathbb{Q}) \cong \{1\}$.
ii) Si f tiene una sola raíz racional entonces $\mathrm{Gal}(L:\mathbb{Q}) \cong \mathbb{Z}_2$.
iii) Si f es irreducible con $\sqrt{\Delta} \in \mathbb{Q}$, entonces $\mathrm{Gal}(L:\mathbb{Q}) \cong A_3$.
iv) En cualquier otro caso, se tiene que $\mathrm{Gal}(L:\mathbb{Q}) \cong S_3$.

Veamos a continuación ejemplos de polinomios de grado 3 y sus grupos de Galois.

Ejemplo 4.25. Daremos un ejemplo para cada uno de los 4 casos que describimos antes.

$f(x)$	Irreducible	Δ	a^2-3b	Raíces	$\mathrm{Gal}(L:\mathbb{Q})$
$x^3-6x^2+11x-6$	No			3 en $\mathbb{Q}$	$\{1\}$
x^3-x^2-2x+2	No			1 en $\mathbb{Q}$, 2 en $\mathbb{R}\setminus\mathbb{Q}$	$\mathbb{Z}_2$
x^3-x-1	Sí	-23	3	1 en $\mathbb{R}\setminus\mathbb{Q}$, 2 en $\mathbb{C}\setminus\mathbb{R}$	S_3
x^3+2x^2-5x+1	Sí	19^2	19	3 en $\mathbb{R}\setminus\mathbb{Q}$	A_3
$x^3+6x^2-27x+3$	Sí	93393	117	3 en $\mathbb{R}\setminus\mathbb{Q}$	S_3

Según el Teorema 4.24 no hace falta calcular ni Δ ni a^2-3b para determinar el grupo de Galois de los polinomios cúbicos reducibles.

4.3. Grupo de Galois de un polinomio de cuarto grado

Estudiamos ahora las raíces y el grupo de Galois de una cuártica, que es subgrupo de S_4, luego podrá ser isomorfo a $\{1\}, \mathbb{Z}_2, \mathbb{Z}_3, \mathbb{Z}_4, \mathbb{Z}_2\times\mathbb{Z}_2, S_3, D_4, A_4, S_4$. Gracias al Teorema 4.17 sabemos que si f es irreducible en $\mathbb{Q}$ su grupo de Galois será transitivo. Los subgrupos transitivos de S_4 son $\mathbb{Z}_4, V, D_4, A_4$ y S_4.

Observación 4.26. S_4 tiene tanto subgrupos isomorfos a $\mathbb{Z}_2\times\mathbb{Z}_2$ transitivos como no transitivos. Por ejemplo, el subgrupo $\{1, (12)(34), (13)(24), (14)(23)\}$ es transitivo e isomorfo a $\mathbb{Z}_2\times\mathbb{Z}_2$, pero $\{1, (12), (34), (12)(34)\}$ es también isomorfo pero no es transitivo. Denotaremos por V al subgrupo transitivo de S_4 isomorfo a $\mathbb{Z}_2\times\mathbb{Z}_2$.

Para determinar el grupo de Galois, distinguiremos si el polinomio es reducible o irreducible.

4.3.1. Caso reducible

Si $f(x) \in \mathbb{Q}$ es un polinomio de grado 4 reducible con al menos una raíz racional podemos descomponerlo como $f = gh$, donde el grado de g es 3. Además el grupo de Galois de f y g coinciden y, aplicando el Teorema 4.24 a g se obtiene el grupo de Galois de f. Sin embargo, si f es reducible pero no tiene raíces racionales se descompone como producto de dos polinomios de grado dos irreducibles, es decir, $f(x) = g(x)h(x)$. Veamos qué grupo de Galois tiene mediante la siguiente proposición.

Proposición 4.27. *Sea $f(x) \in \mathbb{Q}[x]$ un polinomio reducible de grado 4 tal que $f(x) = g(x)h(x)$ donde g y h son irreducibles. Sea L su cuerpo de descomposición sobre $\mathbb{Q}$. Entonces* $\mathrm{Gal}(L : \mathbb{Q}) \cong \mathbb{Z}_2$ *si y solo si* $\sqrt{\dfrac{\Delta(g)}{\Delta(h)}} \in \mathbb{Q}$. *En caso contrario* $\mathrm{Gal}(L : \mathbb{Q}) = \mathbb{Z}_2 \times \mathbb{Z}_2$.

Demostración. Sea $f = gh$, como g, h son irreducibles no tiene raíces en $\mathbb{Q}$. Sean α, β raíces cualesquiera de g y h respectivamente. Entonces ambas son raíces de f y por lo tanto el cuerpo de descomposición de f es $L = \mathbb{Q}(\alpha, \beta)$. Gracias a la fórmula cuadrática se tiene que $L = \mathbb{Q}(\sqrt{\Delta(g)}, \sqrt{\Delta(h)})$. Entonces, $\sqrt{\dfrac{\Delta(g)}{\Delta(h)}} \in \mathbb{Q}$ si y solo si existe $\lambda \in \mathbb{Q}$ tal que $\sqrt{\Delta(g)} = \lambda\sqrt{\Delta(h)}$ y afirmamos que esto es equivalente a que $\sqrt{\Delta(h)} \in \mathbb{Q}(\sqrt{\Delta(g)})$. Como una implicación es evidente, solo vamos a justificar la otra. Si $\sqrt{\Delta(h)} \in \mathbb{Q}(\sqrt{\Delta(g)})$ entonces existen $A, B \in \mathbb{Q}$ tales que $\Delta(h) = A^2 + B^2\Delta(g) + 2AB\sqrt{\Delta(g)}$. Como g es irreducible $\{1, \sqrt{\Delta(g)}\}$ es $\mathbb{Q}$-linealmente independiente, además $\Delta(h) \in \mathbb{Q}$. Entonces, se tiene que $\Delta(h) = A^2 + B^2\Delta(g)$ y $2AB\sqrt{\Delta(g)} = 0$, como g es separable su discriminante no puede ser 0 y $B \neq 0$ pues $\Delta(h)$ sería cuadrado perfecto y eso es contradictorio al ser un polinomio de grado dos irreducible. Por lo tanto, $A = 0$, entonces $\sqrt{\Delta(g)} = B^2\sqrt{\Delta(h)}$. Se tiene ahora que $\sqrt{\Delta(h)} \in \mathbb{Q}(\sqrt{\Delta(g)})$ equivale a que $L = \mathbb{Q}(\sqrt{\Delta(g)})$ y como $\left[\mathbb{Q}(\sqrt{\Delta(g)}) : \mathbb{Q}\right] = 2$ se tiene que $\mathrm{Gal}(L : \mathbb{Q}) \cong \mathbb{Z}_2$. Si $\sqrt{\Delta(h)} \notin \mathbb{Q}(\sqrt{\Delta(g)})$ el grupo de Galois no podría ser $\mathbb{Z}_2$ pues $[L : \mathbb{Q}] \neq 2$. Si $\sqrt{\dfrac{\Delta(g)}{\Delta(h)}} \notin \mathbb{Q}$ entonces $[L : \mathbb{Q}] = 4$ y al ser f reducible, por el Teorema 4.17 tenemos que su grupo de Galois no puede ser transitivo, entonces no puede tener 4-ciclos por lo que debe ser isomorfo a $\mathbb{Z}_2 \times \mathbb{Z}_2$. □

4.3.2. Caso irreducible

Sea $f(y) = y^4 + \lambda_3 y^3 + \lambda_2 y^2 + \lambda_1 y + \lambda_0 \in \mathbb{Q}[y]$ un polinomio mónico de cuarto grado irreducible. Mediante la transformación de Tschirnhaus $y = x - \frac{\lambda_3}{4}$ obtenemos el polinomio $f(x) = x^4 + ax^2 + bx + c$, para ciertos $a, b, c \in \mathbb{Q}$, que sabemos que es irreducible si y solo si $f(y)$ lo es. Además las raíces de $f(x)$ serán una traslación de las de $f(y)$ por un racional, por lo que ni el grupo de Galois ni el discriminante (por la Proposición 2.15) variará. Para saber cómo serán sus raíces utilizaremos el Teorema de Sturm sobre el polinomio sin coeficiente de grado 3 y la expresión del discriminante dada en el Ejemplo 2.28. Distinguiremos dos casos:

1. Si $a \neq 0$ y $-2a^3 + 8ac - 9b^2 \neq 0$ obtenemos los coeficientes

$$f_2 = -\frac{ax^2}{2} - \frac{3bx}{4} - c \qquad f_3 = \frac{(-2a^3 + 8ac - 9b^2)x}{a^2} - \frac{ba^2 + 12bc}{a^2}$$
$$f_4 = \frac{a^2\Delta}{4(-2a^3 + 8ac - 9b^2)^2}$$

Estudiando los cambios de signo obtenemos donde están las raíces según las condiciones siguientes:

Número de raíces reales	Condición
2	$\Delta < 0$
4	$a < 0$, $-2a^3 + 8ac - 9b^2 > 0$ y $\Delta > 0$
Ninguna	En cualquier otro caso

2. Si $a \neq 0$ y $-2a^3 + 8ac - 9b^2 = 0$ se tiene que

$$f_3 = -\frac{ba^2 + 12bc}{a^2}.$$

Al estudiar los cambios de signos se observa que f no tendrá ninguna raíz real.

3. Si $a = 0$ y $b \neq 0$ se tiene que $\Delta = 256c^3 - 27b^4$ y que los coeficientes dados por Sturm son

$$f_2 = -\frac{3bx}{4} - c \qquad f_3 = \frac{\Delta}{27b^3}$$

Si $\Delta > 0$ las raíces del polinomio serán complejas, mientras que si $\Delta < 0$ tendrá solamente dos raíces reales. Observamos del estudio de los signos que el polinomio reducido con coeficiente $a = 0$ no puede tener 4 raíces reales.

4. Si $a = 0$ y $b = 0$ tendremos que $f_2 = -c$. Si $c < 0$ entonces f tiene dos raíces reales, mientras que si $c > 0$ f no tendrá ninguna raíz real.

Procedamos a determinar el grupo de Galois, para ello introducimos el resolvente cúbico de un polinomio de grado 4. Debemos mencionar que en general los siguientes resultados son ciertos para cuerpos con característica distinta a 2.

Definición 4.28 (Resolvente cúbico). *Sea $f(x) \in \mathbb{Q}[x]$ un polinomio mónico de grado 4 con raíces $\alpha_1, \alpha_2, \alpha_3, \alpha_4$. Se llama resolvente cúbico de f al polinomio*

$$R_3(x) = (x - (\alpha_1\alpha_2 + \alpha_3\alpha_4))((x - (\alpha_1\alpha_3 + \alpha_2\alpha_4))(x - (\alpha_1\alpha_4 + \alpha_2\alpha_3)) \tag{4.1}$$

Si $f(x) = x^4 + \lambda x^3 + ax^2 + bx + c$, el resolvente es

$$R_3(x) = x^3 - ax^2 + (\lambda b - 4c)x - (\lambda^2 c + b^2 - 4ac)$$

Veamos esto con detenimiento. Desarrollando el polinomio (4.1) se tiene que

$$-(\alpha_1\alpha_2 + \alpha_3\alpha_4 + \alpha_1\alpha_3 + \alpha_2\alpha_4 + \alpha_1\alpha_4 + \alpha_2\alpha_3) = -a$$

$$\alpha_1^2\alpha_2\alpha_3 + \alpha_1\alpha_2^2\alpha_4 + \alpha_1\alpha_3^2\alpha_4 + \ldots + \alpha_1\alpha_2\alpha_4^2 + \alpha_2^2\alpha_3\alpha_4 = (\lambda b - 4c)$$
$$-(\alpha_1\alpha_2 + \alpha_3\alpha_4)(\alpha_1\alpha_3 + \alpha_2\alpha_4)(\alpha_1\alpha_4 + \alpha_2\alpha_3) = -(\lambda^2 c + b^2 - 4ac)$$

La resolvente podrá ser reducible o irreducible. Además, realizando el cambio de variable $x = x - \frac{\lambda}{4}$, podemos suponer sin pérdida de generalidad que el coeficiente de grado 3 de $f(x)$ es 0 y $f(x) = x^4 + ax^2 + bx + c$. Así, la resolvente queda

$$R_3(x) = x^3 - ax^2 - 4cx - (b^2 - 4ac) \tag{4.2}$$

Lema 4.29. *Sea $f(x)$ un polinomio mónico de grado 4, y $R_3(x)$ su resolvente. Entonces ambos tienen el mismo discriminante. Por lo tanto, $f(x)$ es separable si y solo si $R_3(x)$ también lo es.*

Demostración. De (4.1) sabemos cómo son las raíces de $R_3(x)$, luego se tiene que

$$(\alpha_1\alpha_2 + \alpha_3\alpha_4) - (\alpha_1\alpha_3 + \alpha_2\alpha_4) = (\alpha_1 - \alpha_4)(\alpha_2 - \alpha_3)$$
$$(\alpha_1\alpha_3 + \alpha_2\alpha_4) - (\alpha_1\alpha_4 + \alpha_2\alpha_3) = (\alpha_1 - \alpha_2)(\alpha_3 - \alpha_4)$$
$$(\alpha_1\alpha_2 + \alpha_3\alpha_4) - (\alpha_1\alpha_4 + \alpha_2\alpha_3) = (\alpha_1 - \alpha_3)(\alpha_2 - \alpha_4)$$

Mediante la Proposición 2.26, multiplicando las igualdades y elevando al cuadrado obtenemos que los discriminantes son iguales. Además, f es separable si su discriminante es distinto de 0 y al haber probado que son iguales, $R_3(x)$ tendrá discriminante no nulo si f lo tiene. Por lo tanto, f es separable si y solo si $R_3(x)$ es separable. □

Veamos unos lemas técnicos que nos ayudaran a probar el Teorema de clasificación del grupo de Galois de una cuártica.

Lema 4.30. *S_3 y $\mathbb{Z}_3$ no son subgrupos transitivos de S_4. Además los únicos subgrupos transitivos de S_4 con un 3-ciclo son el propio S_4 y A_4.*

Demostración. Para probar que S_3 no es un subgrupo transitivo de S_4 supondremos que lo es y demostraremos que si $f(123) = (123)$, entonces no existe $\sigma \in \mathrm{Im}(f)$ tal que $\sigma(4) \neq 4$, donde $f : S_3 \to S_4$ es un monomorfismo. Como f es monomorfismo quede bien definido el orden de la imagen de los generadores de S_3 debe ser el mismo que el de estos. Como $f(123) = (123)$ ya conocemos la imágen de todos los tres ciclos. Si S_3 fuese transitivo existiría una trasposición (ab) tal que $f(ab) \in S_4$ y mueve al 4. Vamos a suponer que $(ab) = (12)$, si no la prueba es análoga. Separemos dos casos puesto que la imagen del (12) puede ser un 2-ciclo o el producto de dos trasposiciones. Supongamos los siguientes casos, si no la prueba es análoga.

1. Si $f(12) = (14)$, entonces $(123)(12) = (23)$ mientras que $f((123)(12)) = (1234)$, luego f no es inyectivo.

2. Si $f(12) = (14)(23)$, entonces $(123)(12) = (23)$ mientras que $f((123)(14)(23)) = (134)$, luego tampoco f no es inyectivo.

Se puede fácilmente que $\mathbb{Z}_3$ no es transitivo. Además como los subgrupos que contienen 3-ciclos son $\mathbb{Z}_3, S_3, A_4, S_4$ y S_3 y $\mathbb{Z}_3$ no son transitivos, entonces los únicos subgrupos transitivos de S_4 con un 3-ciclo son el propio S_4 y A_4. No obstante, A_4 es transitivo pues $(12)(34), (13)(24), (14)(34) \in A_4$. □

Lema 4.31. *Sean $f(x) \in \mathbb{Q}[x]$ un polinomio de grado 4 irreducible, $R_3(x)$ su resolvente cúbico y sea L su cuerpo de descomposición sobre $\mathbb{Q}$. Si $R_3(x)$ tiene una raíz racional entonces el grupo de Galois de f no contiene ningún 3-ciclo.*

Demostración. Sean $\alpha_1, \ldots, \alpha_4$ las raíces de $f(x)$, $r_1 = \alpha_1\alpha_2 + \alpha_3\alpha_4, r_2 = \alpha_1\alpha_4 + \alpha_2\alpha_3$ y $r_3 = \alpha_1\alpha_3 + \alpha_2\alpha_4$ las raíces de $R_3(x)$ y supongamos que $r_1 \in \mathbb{Q}$. Supongamos que el grupo de Galois tiene un 3-ciclo, que supondremos sin pérdida de generalidad que es (123). Entonces existe $\tau \in Gal(L : \mathbb{Q})$ tal que $\tau(\alpha_1) = \alpha_2, \tau(\alpha_2) = \alpha_3, \tau(\alpha_3) = \alpha_1$ y $\tau(\alpha_4) = \alpha_4$. Aplicando τ a r_1 tenemos que $\tau(r_1) = r_2, \tau(r_2) = r_3$ y $\tau(r_3) = r_1$. Luego, como $r_1 \in \mathbb{Q}$ tenemos que $\tau(r_1) = r_2 = \tau(\tau(r_1)) = r_3$, es decir, $R_3(x)$ no es separable, entonces $\Delta(R_3) = 0$ por lo tanto, $\Delta(f) = 0$ lo que implica que $f(x)$ no es separable. Pero f es irreducible en $\mathbb{Q}[x]$ por lo tanto es separable. □

Teorema 4.32 (Clasificación del grupo de Galois de una cuártica). *Sean $f(x) \in \mathbb{Q}[x]$ un polinomio de grado 4 irreducible, Δ su discriminante, L el cuerpo de descomposición de f sobre $\mathbb{Q}$ y $R_3(x)$ su resolvente cúbico. Se tienen los siguientes casos:*

i) Si $R_3(x)$ es irreducible en $\mathbb{Q}[x]$ y $\sqrt{\Delta} \notin \mathbb{Q}$, entonces $\mathrm{Gal}(L : \mathbb{Q}) \cong S_4$.
ii) Si $R_3(x)$ es irreducible en $\mathbb{Q}[x]$ y $\sqrt{\Delta} \in \mathbb{Q}$, entonces $\mathrm{Gal}(L : \mathbb{Q}) \cong A_4$.
iii) Si $R_3(x)$ tiene una raíz en $\mathbb{Q}$, entonces o $\mathrm{Gal}(L : \mathbb{Q}) \cong D_4$ *o* $\mathrm{Gal}(L : \mathbb{Q}) \cong \mathbb{Z}_4$.
iv) Si $R_3(x)$ se descompone completamente en $\mathbb{Q}$, entonces $\mathrm{Gal}(L : \mathbb{Q}) \cong V$.

Para hacer más visual este resultado lo ilustraremos en la siguiente tabla.

$\sqrt{\Delta} \in \mathbb{Q}$	$R_3(x)$	$\mathrm{Gal}(L : \mathbb{Q})$
No	Irreducible	S_4
Sí	Irreducible	A_4
	Una raíz racional	D_4 o $\mathbb{Z}_4$
	Se descompone en $\mathbb{Q}$	V

Demostración. Probaremos por orden el teorema anterior.

i) Como $R_3(x)$ es irreducible en $\mathbb{Q}[x]$, entonces todas sus raíces estarán en L. Sea r raíz de $R_3(x)$, como $r \notin \mathbb{Q}$, entonces $[\mathbb{Q}(r) : \mathbb{Q}] = 3$. Luego 3 divide a $[L : \mathbb{Q}] = |\mathrm{Gal}(L : \mathbb{Q})|$, por lo tanto existe un 3-ciclo en el grupo de Galois y

sabemos, Lema 4.30, que los únicos subgrupos transitivos con un elemento de orden 3 son S_4 y A_4, pero como $\sqrt{\Delta} \notin \mathbb{Q}$ por la Proposición 4.19 tenemos que $\mathrm{Gal}(L:\mathbb{Q}) \cong S_4$.

ii) En este caso, como en el anterior, podemos razonar que en el grupo de Galois habrá un 3-ciclo, pero como $\sqrt{\Delta} \in \mathbb{Q}$ se tiene que $\mathrm{Gal}(L:\mathbb{Q}) \cong A_4$.

iii) Como $R_3(x)$ tiene una raíz racional, por la Proposición 4.22 tenemos que su cuerpo de descomposición sobre $\mathbb{Q}$ es $\mathbb{Q}(\sqrt{\Delta(R_3)})$. Por lo tanto, como f y $R_3(x)$ tienen el mismo discriminante tenemos que $\sqrt{\Delta} \notin \mathbb{Q}$ lo que por la Proposición 4.19 implica que $\mathrm{Gal}(L:\mathbb{Q}) \not\leq A_4$, entonces solo podrá ser isomorfo a S_4, D_4, o $\mathbb{Z}_4$. La diferencia entre estos 3 grupos es que en S_4 hay 3-ciclos, pero como $R_3(x)$ tiene una raíz racional, aplicando el Lema 4.31, el grupo de Galois de f no posee ningún 3-ciclo. Por lo tanto $\mathrm{Gal}(L:\mathbb{Q}) \cong D_4$ o $\mathrm{Gal}(L:\mathbb{Q}) \cong \mathbb{Z}_4$.

iv) Al descomponerse $R_3(x)$ completamente en $\mathbb{Q}$ se tiene que su discriminante y por lo tanto el de f es un cuadrado perfecto en $\mathbb{Q}$, entonces $\mathrm{Gal}(L:\mathbb{Q}) \leq A_4$ y por lo tanto, $\mathrm{Gal}(L:\mathbb{Q}) \cong A_4$ o $\mathrm{Gal}(L:\mathbb{Q}) \cong V$. Siguiendo el mismo razonamiento que en el caso (iii) y dado que en A_4 hay 3-ciclos, llegamos nuevamente a una contradicción, por lo tanto $\mathrm{Gal}(L:\mathbb{Q}) \cong V$.

□

Ejemplo 4.33. Grupos de Galois de polinomios de grado 4 irreducibles.

$f(x)$	Δ	$R_3(x)$	$\mathrm{Gal}(L:\mathbb{Q})$
x^4-2x^2-x-1	-731	x^3+2x^2+4x+7	S_4
$x^4+8x+12$	576^2	$x^3-48x+64$	A_4
x^4-2x^2-2	-4608	$(x+2)(x^2+8)$	D_4 o $\mathbb{Z}_4$
x^4+5x+5	15125	$(x-5)(x^2+5x+5)$	D_4 o $\mathbb{Z}_4$
x^4+5x^2+2	9248	$(x-5)(x^2-8)$	D_4 o $\mathbb{Z}_4$
x^4-5x^2+5	2000	$(x+5)(x^2-20)$	D_4 o $\mathbb{Z}_4$
x^4-2x^2+9	384^2	$(x+2)(x-6)(x+6)$	V

Para completar con éxito nuestro propósito debemos de poder diferenciar cuándo el grupo de Galois será $\mathbb{Z}_4$ o D_4. Teorema 4.35 hace esta distinción, aunque por falta de espacio en esta memoria no incluimos la demostración que puede encontrarse en [5]. No obstante, lo que sí incluimos es el siguiente resultado que aporta condiciones suficientes para que el grupo de Galois sea $\mathbb{Z}_4$ o D_4.

Proposición 4.34. *Bajo las mismas hipótesis que en el Teorema 4.32 si $R_3(x)$ es reducible en $\mathbb{Q}[x]$ y $\sqrt{\Delta} \notin \mathbb{Q}$.*

i) Si $\mathrm{Gal}(L:\mathbb{Q}) \cong \mathbb{Z}_4$ entonces $\Delta > 0$.

ii) Si f tiene dos raíces en $\mathbb{R} \setminus \mathbb{Q}$ y otras dos complejas conjugadas, entonces $\mathrm{Gal}(L:\mathbb{Q}) \cong D_4$.

Demostración. Probaremos por orden.

i) Como el grupo de Galois tiene orden 4 entonces $[L:\mathbb{Q}]=4$. Distinguimos dos casos.

a) Si f tiene una raíz real α, entonces tiene todas sus raíces reales, ya que podemos plantear la siguiente torre de cuerpos

$$\mathbb{Q} \overset{4}{\hookrightarrow} \mathbb{Q}(\alpha) \overset{1}{\hookrightarrow} L$$

y como $\mathbb{Q}(\alpha) \subset \mathbb{R}$ y $\mathbb{Q}(\alpha) = L$, todas las raíces son reales. Luego, $\delta = \prod_{1\leq i<j\leq n} (\alpha_i - \alpha_j) \in \mathbb{R}$ por lo tanto, $\delta^2 = \Delta > 0$.

b) Si f tiene dos pares de raíces complejas conjugadas $\alpha, \overline{\alpha}, \beta, \overline{\beta}$. Entonces, $\mathbb{Q}(\alpha) \subset \mathbb{C}$, luego todas las raíces son complejas. Por lo tanto tenemos

$$\delta = (\alpha-\overline{\alpha})(\alpha-\beta)(\alpha-\overline{\beta})(\overline{\alpha}-\beta)(\overline{\alpha}-\overline{\beta})(\beta-\overline{\beta}) = |\alpha-\beta|^2 \left|\alpha-\overline{\beta}\right|^2 (\alpha-\overline{\alpha})(\beta-\overline{\beta}),$$

con $(\overline{\alpha}-\overline{\alpha}), (\beta-\overline{\beta})$ imaginarios puros, por lo tanto $\delta \in \mathbb{R}$ y $\delta^2 = \Delta > 0$.

ii) Sabemos que el orden del grupo de Galois es 4 u 8. Sean las raíces reales de f, α, β y $\gamma, \overline{\gamma}$ las complejas conjugadas, como $\alpha \in \mathbb{R}$ se tiene que $\mathbb{Q}(\alpha) \subset \mathbb{R}$ y $[\mathbb{Q}(\alpha):\mathbb{Q}] = 4$. Además, $\gamma \notin \mathbb{Q}(\alpha)$ pues no es real y $[L:\mathbb{Q}] = 8$, con L el cuerpo de descomposición de f sobre $\mathbb{Q}$. Planteamos la siguiente torre de cuerpos

$$\mathbb{Q} \overset{4}{\hookrightarrow} \mathbb{Q}(\alpha) \overset{2}{\hookrightarrow} \mathbb{Q}(\alpha,\gamma) \overset{1}{\hookrightarrow} L$$

y concluimos que $\mathbb{Q}(\alpha,\gamma) = L$, por lo tanto $|\mathrm{Gal}(L:\mathbb{Q})| = 8$, entonces $\mathrm{Gal}(L:\mathbb{Q}) \cong D_4$.

□

Teorema 4.35. *Sean $f(x) = x^4 + ax^2 + bx + c \in \mathbb{Q}[x]$, L su cuerpo de descomposición y Δ su discriminante. Supongamos que $\sqrt{\Delta} \notin \mathbb{Q}$ y que $R_3(x)$ es irreducible con una única raíz $r \in \mathbb{Q}$. Si $-(a-r)\Delta$ y $(r^2-4c)\Delta$ son cuadrados perfectos en $\mathbb{Q}$, entonces* $\mathrm{Gal}(L:\mathbb{Q}) \cong \mathbb{Z}_4$. *En caso contrario,* $\mathrm{Gal}(L:\mathbb{Q}) \cong D_4$.

Gracias a los Teoremas 4.32 y 4.35 podemos al fin distinguir cual es el grupo de Galois de un polinomio de grado 4 irreducible. Resumiremos toda la información en la siguiente tabla.

$\sqrt{\Delta} \in \mathbb{Q}$	$R_3(x)$	$\sqrt{-(a-r)\Delta} \in \mathbb{Q}$ y $\sqrt{(r^2-4c)\Delta} \in \mathbb{Q}$	$\mathrm{Gal}(L:\mathbb{Q})$
No	Irreducible	Irrelevante	S_4
Si	Irreducible	Irrelevante	A_4
No	Una raíz $r \in \mathbb{Q}$	Sí	$\mathbb{Z}_4$
No	Una raíz $r \in \mathbb{Q}$	No	D_4
Si	Se descompone en $\mathbb{Q}$	Irrelevante	V

Ejemplo 4.36. Distinción entre los grupos D_4 y $\mathbb{Z}_4$ de el Ejemplo 4.33.

$f(x)$	Δ	$R_3(x)$	$-(a-r)\Delta$	$(r^2-4c)\Delta$	$\mathrm{Gal}(L:\mathbb{Q})$
x^4-2x^2-2	-4608	$(x+2)(x^2+8)$	0	-55296	D_4
x^4+5x+5	15125	$(x-5)(x^2+5x+5)$	275^2	4275^2	$\mathbb{Z}_4$
x^4+5x^2+2	9248	$(x-5)(x^2-8)$	0	157216	D_4
x^4-5x^2+5	2000	$(x+5)(x^2-20)$	0	100^2	$\mathbb{Z}_4$

Hemos de añadir que existe un software matemático llamado Magma [4] que calcula el grupo de Galois de un polinomio. Para ello se puede utilizar la función `GaloisGroup(F)`, que recibe un polinomio y devuelve su grupo de Galois.

4.4. El problema inverso de Galois

Una de las principales preguntas abiertas desde el siglo XIX en Teoría de Galois y sobre la que aún se investiga intensamente a día de hoy, es la siguiente:

Todo grupo finito G es grupo de Galois de una extensión finita $\mathbb{Q} \hookrightarrow K$.

Esto es lo que se conoce como *problema inverso de Galois* sobre $\mathbb{Q}$. El grupo más pequeño G del que del que no se ha encontrado ninguna extensión finita $\mathbb{Q} \hookrightarrow K$ tal que $\mathrm{Gal}(K:\mathbb{Q}) \cong G$ es el grupo de Mathieu M_{23}, cuyo orden es 10.200.960. En otras palabras, no se ha encontrado un polinomio en $\mathbb{Q}[x]$ cuyo grupo de Galois sea M_{23} (ver [14, Sección 5.2.8])

Si cambiamos $\mathbb{Q}$ por otro cuerpo K, el análogo problema inverso de Galois sobre K puede tener respuesta afirmativa o negativa. Así por ejemplo, para cuerpos finitos solo los grupos cíclicos aparecen como grupos de Galois (ver [13]). Por otra parte, desde el siglo XIX se sabe que para $K = \mathbb{C}(x)$, el cuerpo de funciones racionales sobre $\mathbb{C}$, la respuesta al problema inverso de Galois es afirmativa. También este es el caso de $K = \mathbb{Q}(x)$; la demostración, nada fácil, de este hecho se la debemos a Hilbert (1892). Lo que sí es fácil de demostrar es que para todo grupo finito G, existe una extensión de Galois $K \hookrightarrow L$ tal que $Gal(L:K) \cong G$ (ver, por ejemplo, [7, Teorema 7.4.5]).

Volviendo al problema inverso de Galois sobre $\mathbb{Q}$. En esta memoria, con la clasificación de los grupos de Galois de la cúbica y la cuártica de este capítulo, aportamos una prueba elemental para del problema inverso de Galois sobre $\mathbb{Q}$ para los subgrupos de S_3 y S_4.

5

Resolubilidad de la quíntica

En este capítulo estudiaremos cómo determinar si un polinomio de quinto grado es resoluble por radicales, en este sentido el Corolario 5.8 nos permitirá decidir sobre la resolubilidad de las quínticas. Sabemos que como S_5 no es resoluble y hay polinomios irreducibles de grado 5 con grupo de Galois S_5, entonces no todos lo polinomios de quinto grado irreducibles serán resolubles por radicales. Como consecuencia del Gran Teorema de Galois (Teorema 4.15) y del Teorema 4.17, los polinomios irreducibles de grado 5 que son resolubles son exactamente aquellos cuyo grupo de Galois es un subgrupo transitivo resoluble de S_5. En el Teorema 5.9 se presenta un criterio que determina cuándo los polinomios racionales en forma Bring-Jerrard son resolubles por radicales, encontrando como consecuencia una familia resoluble de quínticas. Además, gracias a los resultados vistos en el Capítulo 3, como todo polinomio se puede reducir a esta forma podremos determinar cuándo serán resolubles por radicales. Como bibliografía de referencia hemos utilizado [7].

5.1. Subgrupos transitivos de S_5

El grupo de Galois de un polinomio de quinto grado irreducible será isomorfo a un subgrupo transitivo de S_5 por el Teorema 4.17. Veamos cuales son.

Lema 5.1. *Sea H un subgrupo de S_5. Las siguientes condiciones son equivalentes*

i) H es transitivo.
ii) $|H|$ es divisible por 5.
iii) H contiene un 5-ciclo.

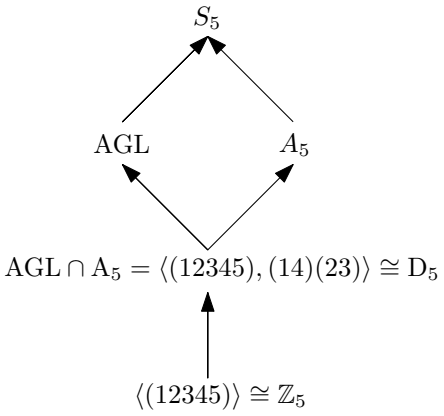
Demostración. $(i) \Rightarrow (ii)$. Sea $H \leq S_5$ un subgrupo transitivo, entonces existe $\tau \in H$ tal que $\tau(i) = j$, para todo $i, j \in \{1, \ldots, 5\}$. Definimos $H_i := \{\sigma \in H \,|\, \sigma(1) = i\}$. Es fácil ver que $H = \bigsqcup_{i=1}^{5} H_i$, y por lo tanto $|H| = \sum_{i=1}^{5} |H_i|$. Veamos que $|H_i| = |H_j|$, para to $i, j \in \{1, \ldots, 5\}$. Para ello definimos la aplicación $H_i \to H_j$

tal que $\sigma \to \tau \circ \sigma$. Es fácil probar que están bien definida y que es inyectiva. Además, como $\tau^{-1} \in H$ la aplicación es sobre. Por lo tanto, $|H_i| = |H_j|$, luego $|H| = \sum_{i=1}^{5} |H_i| = 5 \cdot |H_5|$.
$(ii) \Rightarrow (iii)$. Consecuencia directa del Teorema de Cauchy para grupos y del hecho de que los únicos elementos en S_5 de orden 5 son los 5-ciclos.
$(iii) \Rightarrow (i)$. Es evidente. □

Aplicando el Lema anterior a la lista de subgrupos de S_5 (ver [10]) obtenemos que los subgrupos transitivos de S_5 son el propio S_5 además de todos los grupos isomorfos a $\mathbb{Z}_5$, D_5 y el grupo General Afín de orden 20, al que denotaremos por $\mathrm{AGL} = \{\sigma \in S_5 \,|\, \sigma_{a,b}(i) \equiv ai + b \mod 5, a \neq 0\}$. Veamos que es subgrupo de S_5 y algunas propiedades que posee en el siguiente lema.

Lema 5.2. *El grupo* AGL *es un subgrupo de orden 20 de* S_5 *resoluble y generado por* $\langle(12345)(1243)\rangle$. *Además, cualquier subgrupo de orden 20 de* S_5 *es conjugado a* AGL.

Demostración. Es evidente que la identidad está en AGL, pues coincide con $\sigma_{1,0}$. Si tomamos dos elementos cualesquiera $\sigma_{a,b}, \sigma_{c,d}$ se tiene que $\sigma_{a,b} \circ \sigma_{c,d} = \sigma_{ac,ad+b} \in$ AGL. Finalmente, como $\sigma_{a,b} = \sigma_{1,b} \circ \sigma_{a,0}$ tendríamos que el inverso $\sigma_{a,b}^{-1} = \sigma_{a^{-1},0} \circ \sigma_{1,-b} = \sigma_{a^{-1},-a^{-1}b} \in$ AGL. Por lo tanto, AGL $\leq S_5$. Además, como tenemos cuatro posibilidades para a y cinco para b se tiene que $|\mathrm{AGL}| \leq 20$. Por otro lado, tenemos que $\langle(12345), (1243)\rangle \leq$ AGL, pues $\sigma_{1,1} = (12345)$ y $\sigma_{2,0} = (1243)$. Como AGL posee un 5-ciclo y un 4-ciclo, 5 y 4 dividen al orden del grupo, entonces 20 divide al orden, por lo tanto $|\mathrm{AGL}| = 20$. También, debemos mencionar que AGL es resoluble [7, Teorema 8.1.8 (De Burnside)]. Por último, es conocido que S_5 tiene exactamente 6 subgrupos de orden 20 y todos ellos son conjugados a AGL (ver, por ejemplo `groupprops.subwiki.org/wiki/Subgroup_structure_of_symmetric_group:S5`). □



(5.1)

El diagrama anterior nos muestra que subgrupos transitivos de S_5 contienen a otros. Hemos de mencionar que AGL $\not\subset A_5$ pues en A_5 hay 3-ciclos y en AGL no. Las siguiente proposición es consecuencia directa del diagrama y de este hecho.

Proposición 5.3. *Sea H un subgrupo de S_5 transitivo. Entonces*

i) $H \leq$ AGL *o* $A_5 \leq H$.
ii) H *es resoluble si y solo si* $H \leq$ AGL.

5.2. El resolvente séxtico

Para estudiar la resolubilidad de un polinomio de quinto grado necesitaremos definir el resolvente séxtico. Sea $f(x) = x^5 - c_4x^4 + c_3x^3 - c_2x^2 + c_1x - c_0 \in \mathbb{Q}[x]$ un polinomio irreducible. Consideramos $h \in \mathbb{Q}[x_1, \ldots, x_5]$ tal que $h = u^2$, donde

$$u = x_1x_2 + x_2x_3 + x_3x_4 + x_4x_5 + x_5x_1 - x_1x_3 - x_3x_5 - x_5x_2 - x_2x_4 - x_4x_1. \quad (5.2)$$

Si ahora a cada elemento $\sigma \in S_5$ lo hacemos corresponder con un f_σ que envía $x_i \to x_{\sigma(i)}$ observamos que $f_{(12345)}(u) = u$, mientras que $f_{(1243)}(u) = -u$. Se aprecia que h queda fijo por estas dos permutaciones, luego h permanece invariante mediante todas las permutaciones de $\langle(12345), (1243)\rangle$, es decir, tenemos el siguiente contenido entre lo grupos, AGL $\subseteq \{\sigma \in S_5 \,|\, \sigma(h) = h\}$. Veamos que se cumple también el otro contenido.

Lema 5.4. *Sea $h = u^2$, donde u se define como en (5.2). Entonces se tiene que* AGL $= \{\sigma \in S_5 \,|\, f_\sigma(h) = h\}$.

Demostración. Llamemos $H := \{\sigma \in S_5 \,|\, f_\sigma(h) = h\}$. Ya vimos que AGL $\leq H \leq S_5$. Como el orden de AGL es 20 se tiene que 20 divide a $|H|$ y que $|H|$ divide a 120, luego tenemos que el orden de H puede ser 20, 40, 60 o 120. Si el orden de H fuese 60 o 120, entonces H sería A_5 o S_5 respectivamente. Sin embargo, tomando $(15) \in A_5 \subset S_5$, se tiene que $f_\sigma(h) \neq h$. Por tanto $H \neq A_5$, $H \neq S_5$. Por otro lado, el orden no puede ser 40 pues S_5 no posee subgrupos de ese orden [10]. Luego la única posibilidad es que el orden de H sea 20 y como AGL $\subseteq H$, se debe tener la igualdad. □

Para calcular la órbita de h en S_5, $\{\sigma(h) \,|\, \sigma \in S_5\}$, nos será de utilidad calcular los representantes de las clases de equivalencia a la izquierda en el cociente S_5/AGL:

$$Id, (123), (234), (345), (145), (125). \quad (5.3)$$

Como h queda fijo por $(12345), (1243)$ tenemos que la órbita de h en S_5 es

$$\{h_1 = h, h_2 = f_{(123)}(h), h_3 = f_{(234)}(h), h_4 = f_{(345)}(h), h_5 = f_{(145)}(h), h_6 = f_{(125)}(h)\}.$$

Definición 5.5 (Resolvente séxtico). *Sea* $f(x) = x^5 - c_4x^4 + c_3x^3 - c_2x^2 + c_1x - c_0 \in \mathbb{Q}[x]$ *irreducible y sean* $\alpha_1, \ldots, \alpha_5$ *sus raíces.. Se denomina resolvente séxtico de* f *al polinomio*

$$R_6(x) = \prod_{i=1}^{6}(x - \beta_i),$$

donde $\beta_i = h_i(\alpha_1, \ldots, \alpha_5)$.

Proposición 5.6. *Sea* $f(x) = x^5 - c_4x^4 + c_3x^3 - c_2x^2 + c_1x - c_0 \in \mathbb{Q}[x]$ *irreducible y* Δ *su discriminante. Entonces el resolvente séxtico es*

$$R_6(x) = (x^3 + b_2x^2 + b_4x + b_6)^2 - 2^{10}\Delta.$$

No demostraremos esta proposición por ser la prueba demasiado larga, pero esta puede encontrarse en [7, Teorema 13.2.5]. En ella podemos ver también quienes son los b_i en función de los coeficientes del polinomio.

$$b_2 = 8c_1c_3 - 3c_2^2 - 20c_4, \tag{5.4}$$

$$\begin{aligned} b_4 =& 3c_2^4 - 16c_1c_2^2c_3 + 16c_1^2c_3^2 + 16c_2c_3^2 + 1c_1^2c_2c_4 - 8c_2^2c_4 - 112c_1c_3c_4 \\ &+ 240c_4^2 - 64c_1^3c_5 + 240c_1c_2c_5 - 400c_3c_5, \end{aligned}$$

$$\begin{aligned} b_6 =& 8c_1c_2^4c_3 - c_2^6 - 16c_1^2c_2^2c_3^2 - 16c_2^3c_3^2 + 64c_1c_2c_3^3 - 64c_3^4 - 16c_1^2c_2^3c_4 + 28c_2^4c_4 \\ &+ 64c_1^3c_2c_3c_4 - 112c_1c_2^2c_3c_4 - 128c_1^2c_3^2c_4 + 224c_2c_3^2c_4 - 64c_1^4c_4^2 + 224c_1^2c_2c_4^2 \\ &- 176c_2^2c_4^2 - 64c_1c_3c_4^4 + 320c_4^3 + 48c_1c_2^3c_5 - 192c_1^2c_2c_3c_5 - 80c_2^2c_3c_5 + 640c_1c_3^2c_5 \\ &+ 384c_1^3c_4c_5 - 640c_1c_2c_4c_5 - 1600c_3c_4c_5 - 1600c_1^2c_5^2 + 4000c_2c_5^2. \end{aligned}$$

Demostraremos como consecuencia del siguiente teorema que un polinomio de quinto grado irreducible con coeficientes racionales es resoluble por radicales si y solo si $R_6(x)$ tiene una raíz en $\mathbb{Q}$. Recordemos que que por la Proposición 4.19 el grupo de Galois de la quíntica será subgrupo de A_5 si y solo si $\sqrt{\Delta} \in \mathbb{Q}$.

Teorema 5.7. *Sean* $f \in \mathbb{Q}[x]$ *un polinomio mónico irreducible de quinto grado y* L *su cuerpo de descomposición. Entonces,* $\mathrm{Gal}(L : \mathbb{Q})$ *es conjugado a un subgrupo de* AGL *si y solo si* $R_6(x)$ *tiene una raíz en* $\mathbb{Q}$.

Demostración. Como $\mathrm{Gal}(L : \mathbb{Q})$ es subgrupo transitivo de S_5, por tanto puede ser isomorfo a AGL, a D_5 o a $\mathbb{Z}_5$. Si es isomorfo a AGL vimos que es conjugado de AGL, si es isomorfo a D_5, entonces se sabe que es conjugado a $\langle (12345), (14)(23) \rangle$ que es subgrupo de AGL y si es $\mathbb{Z}_5$, es fácil ver que es conjugado a $\langle (12345) \rangle$ (que es subgrupo de S_5). Podemos suponer que $\mathrm{Gal}(L : \mathbb{Q}) \leq \mathrm{AGL}$. Sea $\sigma \in \mathrm{Gal}(L : \mathbb{Q})$ entonces

$$\sigma(\beta_1) = \sigma(h(\alpha_1, \ldots, \alpha_5)) = h(\sigma(\alpha_1), \ldots, \sigma(\alpha_5)).$$

Como σ pertenece al grupo de Galois y este es un subgrupo de AGL aplicando el Lema 5.4 se tiene que

$$h(\sigma(\alpha_1), \ldots, \sigma(\alpha_5)) = (f_\sigma \circ h(\alpha_1, \ldots, \alpha_5)) = h(\alpha_1, \ldots, \alpha_5) = \beta_1.$$

Al ser la extensión $\mathbb{Q} \hookrightarrow L$ de Galois se tiene que $\beta_1 \in \mathbb{Q}$, ya que β_1 queda fijo por todos los elementos del grupo de Galois (ver Proposición 4.12), de lo que se deduce que $R_6(x)$ tiene una raíz en $\mathbb{Q}$. Recíprocamente, si $R_6(x)$ tiene una raíz $\beta_1 \in \mathbb{Q}$. Supongamos por reducción al absurdo que $\mathrm{Gal}(L : \mathbb{Q})$ no es conjugado a un subgrupo de AGL. Como el grupo de Galois es transitivo, por la Proposición 5.3 y el diagrama 5.1, deberá contener a A_5. Sean τ_i un 3-ciclo en (5.3) con $f_{\tau_i} \cdot h = h_i$ y $\sigma_i \in \mathrm{Gal}(L : \mathbb{Q})$. Entonces, procediendo como anteriormente, se tiene que $\sigma_i(\beta_1) = \beta_i$, para todo i. Como β_1 es racional y $\sigma_i \in \mathrm{Gal}(L : \mathbb{Q})$ llegamos a que $\beta_1 = \ldots = \beta_6$, es decir $R_6(x) = (x - \beta_1)^6$. De la Proposición 5.6 tenemos que

$$R_6(x) = (x - \beta_1)^6 = (x^3 + b_2x^2 + b_4x + b_6)^2 - 2^{10}\Delta,$$

donde Δ es el discriminante de f. Comparando los coeficientes en la igualdad anterior obtenemos que $b_2 = -3\beta_1, b_4 = 3\beta_1^2, b_6 = -\beta_1^3$. Tras sustituir y simplificar se tiene que

$$(x - \beta_1)^6 = (x - \beta_1)^6 - 2^{10}\Delta,$$

es decir, $\Delta = 0$, lo que es contradictorio ya que $f \in \mathbb{Q}[x]$ es irreducible y por lo tanto es separable. □

Corolario 5.8. *Sea $f(x) \in \mathbb{Q}[x]$ un polinomio de grado 5 mónico e irreducible. f es resoluble por radicales si y solo si $R_6(y)$ tiene al menos una raíz en $\mathbb{Q}$.*

Demostración. Por la Proposición 5.3 se tiene que un subgrupo de S_5 es resoluble si es subgrupo de AGL lo que es equivalente a ser conjugado a un subgrupo de AGL. Por el Teorema 5.7, el grupo de Galois será resoluble si $R_6(x)$ tiene una raíz en $\mathbb{Q}$. □

5.3. Resolubilidad de la quíntica en forma de Bring-Jerrard

En esta sección demostraremos cuándo los polinomios en forma Bring-Jerrard son resolubles por radicales. Recordamos que un polinomio de grado 5 está en forma de Bring Jerrard si es de la forma $x^5 + ax + b$. Además, como vimos en el Capítulo 3, a toda quíntica se le puede asociar otra en forma de Bring-Jerrard de forma que la primera es resoluble si y solo si lo es la segunda.

Teorema 5.9. *Sea $f(x) = x^5 + ax + b \in \mathbb{Q}[x]$. Supongamos que f es irreducible en $\mathbb{Q}[x]$. Entonces, $f(x)$ es resoluble por radicales si y solo si existe $\lambda \in \mathbb{Q} \setminus \{1\}$ cumpliendo que*

$$a^5 = \frac{3125\lambda b^4}{(\lambda - 1)^4(\lambda^2 - 6\lambda + 25)} \tag{5.5}$$

Demostración. Si $a = 0$, entonces f es evidentemente resoluble y tomando $\lambda = 0$ se tiene el resultado. Supongamos a partir de ahora que $a \neq 0$. Sabemos que f será resoluble si y solo si $R_6(x)$ tiene al menos una raíz en $\mathbb{Q}$. Mediante (5.4) y usando la fórmula del discriminante del Ejemplo 2.28 obtenemos que

$$R_6(x) = (x^3 - 20ax^2 + 240a^2x + 320a^3)^2 - 2^{10}(256a^5 + 3215b^4)x.$$

Supongamos que $\alpha \in \mathbb{Q}$ es raíz de $R_6(x)$. Sean $\lambda = \dfrac{\alpha}{a}$, $\mu = \dfrac{b}{a} \in \mathbb{Q}$. Como α es raíz de $R_6(x)$ tenemos que

$$\begin{aligned} R_6(\alpha) = 0 &= ((a\lambda)^3 - 20a(a\lambda)^2 + 240a^2(a\lambda) + 320a^3)^2 - 2^{10}(256a^5 + 3215(a\mu)^4)(a\lambda) \\ &= 2^{12}a^5((\lambda^6 - 10\lambda^5 + 55\lambda^4 - 140\lambda^3 + 175\lambda^2 - 106\lambda + 25)a - 3125\lambda\mu^4) \\ &= 2^{12}a^5(((\lambda - 1)^4(\lambda^2 - 6\lambda + 25))a - 3125\lambda\mu^4). \end{aligned}$$

Al ser $a \neq 0$ y $b = a\mu$ obtenemos que

$$a = \frac{3125\lambda\mu^4}{(\lambda - 1)^4(\lambda^2 - 6\lambda + 25)} \Rightarrow a^5 = \frac{3125\lambda b^4}{(\lambda - 1)^4(\lambda^2 - 6\lambda + 25)}$$

□

Ejemplo 5.10. El polinomio $x^5 - 5x - 12$ es resoluble por radicales ya que se cumple la igualdad (5.5) si tomamos $\lambda = -5$. Además, utilizando Magma [4] obtenemos que el grupo de Galois de este polinomio es isomorfo a D_5.

Bibliografía

[1] Adamchik, V. S. Jeffrey, D. J.. Polynomial transformations of Tschirnhaus, Bring and Jerrard. *ACM SIGSAM Bull*, 2003, vol 37, Nº 3, pp. 90–93

[2] Balanzario, E. P. "Números algebraicos y trascendentes", UNAM-Morelia, Mexico, 2003 [en línea]. Disponible en: http://matmor.unam.mx/~euba/irra.pdf.

[3] Basu, S. Pollack, R. Roy, M-F. *Algorithms in Real Algebraic Geometry.* Springer, New York, 2004.

[4] Bosma, W. Cannon, J. Playoust, C. The Magma algebra system. I. The user language.*Journal of Symbolic Computation*, 1997, vol. 24, Nº 3-4, pp. 235–265.

[5] Conrad, K. "Galois groups of cubics and quartics (not in characteristic 2)", Math Dept. UConn [en línea]. Disponible en: https://kconrad.math.uconn.edu/blurbs/galoistheory/cubicquartic.pdf.

[6] Conrad, K. "Galois groups as permutation groups", Math Dept. UConn [en línea]. Disponible en: https://kconrad.math.uconn.edu/blurbs/galoistheory/galoisaspermgp.pdf.

[7] Cox, D. A. *Galois theory.* John Wiley & Sons, Inc. New Jersey, 2004.

[8] Cox, D. A. Little, J. O'Shea, D. *Ideals, varieties, and algorithms. An introduction to computational algebraic geometry and commutative algebra.* (Fourth edition). Springer, New York, 2015.

[9] Rowen, L. H. *Graduate algebra: commutative view.* Providence: American Mathematical Society, Rhode Island, 2006.

[10] Samaila, D. Counting the Subgroups of the One-Headed Group S5 up to Automorphism. *IOSR Journal of Mathematics*, 2013, vol. 8, Nº 3, pp. 87–93.

[11] Stillwell, J.Eisenstein's Footnote. *The Mathematical Intelligencer*, 1995, vol. 17, Nº 2, pp. 58–62.

[12] Suppes, P. *Axiomatic set theory.* Van Nostrand Company, Canada, 1960.

[13] Vila, N. On the inverse problem of Galois theory.*Publicacions matematiques*, 1992, vol. 36, Nº 2.2, pp. 1053–1073.

[14] Wilson, R. A. *The finite simple groups*. Springer, New York, 2009.

Algebraic elements and small degree polynomial equations

Sección de Matemáticas
Universidad de La Laguna

Alejandro Jiménez Pérez
Facultad de Ciencias · Sección de Matemáticas
Universidad de La Laguna
alu0101024530@ull.edu.es

Abstract

The goal of this memory is to delve into of some concepts in Galois Theory. Firstly, we use the resultant to prove constructively that the addition and product of algebraic elements is algebraic. We also see an alternative method to solve the third and fourth-degree equations by means of the Tschirnhaus transformations. Finally, we classify the Galois groups of cubic and quartics and characterize when a quintic is solvable.

1. The main tool: the resultant

The Resultant of two monic polynomials $f, g \in K[x]$ of degrees n and m is

$$\mathrm{Res}_x(f,g) = (-1)^{nm} \prod_{i=1}^{n} \prod_{j=1}^{m} (\alpha_i - \beta_j)$$

where $\alpha_i, \beta_j \in \overline{K}$ are the roots of f, g respectively.

Proposition. *If $f, g \in K[x]$, then $\mathrm{Res}_x(f,g) \in K$.*
Moreover, $\mathrm{Res}_x(f,g)$ can be computed by means of the coefficients of f and g.

2. Minimal polynomial

A complex problem in Galois theory is to find the minimal polynomial of the addition and product of algebraic elements knowing, their minimal polynomials.

Proposition. *If f, g are the minimal polynomials of α and β, respectively. Then,*

$$\alpha+\beta \text{ is a root of } \mathrm{Res}_y(f(x-y), g(y)) \in K[x]$$

$$\alpha\cdot\beta \text{ is a root of } \mathrm{Res}_y(y^n f(x/y), g(y)) \in K[x]$$

As the following result shows, sometimes these polynomials are the actual minimal polynomials.

Theorem. *If α, β are algebraic elements over K, with minimal polynomials $f(x), g(x)$ of coprime degree. Then, the minimal polinomial of $\alpha+a\beta$ is $a^{nm}\mathrm{Res}_y(f(x-y), g(y/a))$ and the minimal polinomial of $\alpha(\beta+a)$ is $\mathrm{Res}_y(y^n f(x/y), g(y-a))$, except for a finite number of values of $a \in K$.*

3. Solving cubic equations with Tschirnhaus transformations

Let $f(x) \in \mathbb{Q}$ be a monic cubic polynomial, by performing a linear transformation we can asume that $f(x) = x^3 - ax + b$. We can obtain the roots of f in the following way:

1. Perform a Tschirnhaus transformation $y = x^2 + mx + n$ with

$$n = \frac{2a}{3} \qquad m = \frac{-3b \pm \sqrt{9b^2 + \frac{4a^3}{3}}}{2a}$$

That is

$$q(y) = \mathrm{Res}_x(f(x), y - (x^2 + mx + n))$$

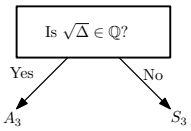
The above choice of m, n implies that $q(y) = y^3 - A_0$.

2. Compute the roots of $q(y)$, these are $\beta_k = \sqrt[3]{-A_0} \cdot e^{2ik\pi/3}$, for $k = 0, 1, 2$.
3. Compute $\alpha_{k,j}$ the solutions of $\beta_k = x^2 + xm + n$.
4. Verify which of the six $\alpha_{k,j}$ are roots of f.

A similar method can be applied to solve quartic equations.

4. Galois group of irreducible cubics

Given an irreducible cubic $f(x) = x^3 + ax^2 + bx + c \in \mathbb{Q}[x]$ we can determine its Galois group with the following diagram.



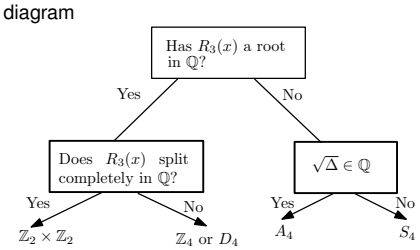
In this diagram, $\Delta = a^2b^2 - 4b^3 - 4a^3c + 18abc - 27c^2$ denotes the discriminant of f.

5. Galois group of irreducible quartic

Given an irreducible quartic $f(x) = x^4 + ax^2 + bx + c \in \mathbb{Q}[x]$, we can determine its Galois group using its cubic resolvent

$$R_3(x) = x^3 - ax^2 - 4cx - (b^2 - 4ac)$$

and this diagram



In this diagram, $\Delta = 16a^4c - 4a^3b^2 - 128a^2c^2 + 144ab^2c - 21b^2 + 256c^3$ denotes the discriminant of f.

6. Solvable quintics

Qintics are not solvable by radicals in general, as Abel proved.

Theorem (Abel-Ruffini)**.** *If $n \geq 5$, then the universal polynomial $f \in K[x]$ of degree n is not solvable by radicals over K.*

To determine when a given quintic is solvable, we associate to it a degree six polynomial, called the sextic resolvent and have the following:

Theorem. *If $f \in \mathbb{Q}[x]$ is a monic and irreducible quintic. Then, f is solvable if and only if its sextic resolvent has a root in $\mathbb{Q}$.*

References

[1] Cox, D. A. *Galois theory*. John Wiley & Sons, Inc. New Jersey, 2004.

TRABAJO FIN DE GRADO, Convocatoria de Junio, 2020