Universidad de Cantabria

Facultad
de
Ciencias

PROBLEMA INVERSO DE GALOIS
(Inverse Galois Problem)

Trabajo de Fin de Grado
para acceder al

GRADO EN MATEMÁTICAS

Autor: David Pérez Caballero

Director: Daniel Sadornil Renedo

Junio - 2025

«Un libro que no encierra su contralibro
es considerado incompleto»

-Jorge Luis Borges.

«Después de esto habrá, espero,
gentes que encontrarán provechoso
descifrar todo este lío»

-Évariste Galois.

Agradecimientos

... a mi director y amigo Dani, gracias por mostrar las Matemáticas de la forma en la que lo haces, siempre con una sonrisa en la cara, eres un referente para mí. Quién iba a decir cuando nos conocimos hace más de diez años que este momento llegaría, me alegra saber que este último escalón lo he superado junto a ti.

... a mis padres, Jaime y Placi, gracias por creer en mí siempre, por celebrar conmigo cada victoria y por apoyarme incondicionalmente en cada derrota. Gracias por forjar con vuestro cariño y paciencia al estudiante y persona que soy.

... a mis abuelos Juana, Pili, Lolo y Antonio; por vuestro amor, por vuestro ejemplo y por estar, incluso cuando algunos ya no estabais. En cada logro añoro vuestra presencia, en cada paso que doy queda marcada vuestra huella.

... a mis amigos, los de siempre y los que me ha dado la universidad, por todas esas mañanas tomándonos un café hablando de la vida. Soñábamos con terminar este viaje, y sólo ahora que lo hemos hecho nos damos cuenta de lo felices que fuimos recorriéndole.

... a Sofía, porque en mis momentos de incertidumbre me hiciste creer de nuevo en mis capacidades, por darme la fuerza que necesitaba en cada instante, la valentía que yo mismo no encontraba; por seguir ahí incluso mostrándote mi peor cara.

... al joven David, por tenerlo tan claro siempre, por no rendirte nunca, tu pasión ha llegado más lejos de lo que nunca imaginaste, estarías orgulloso de lo que hemos conseguido.

Resumen

En la perspectiva habitual de la teoría de Galois se parte de polinomios para describir sus grupos de automorfismos. El Problema Inverso de Galois trata de revertir este enfoque, dado un grupo se estudia si existe algún polinomio sobre el cuerpo de los racionales que lo tenga como grupo de Galois. En este trabajo fin de grado se demuestra que todo grupo abeliano finito se puede realizar como grupo de Galois dentro de una extensión ciclotómica, siguiendo los pasos que culminaron en el Teorema de Kronecker-Weber. A continuación, se elaboran polinomios cuyo grupo de Galois es el grupo simétrico utilizando la transitividad del grupo y la aparición de determinados ciclos, con el respaldo siempre del Teorema de Dedekind. La realización de los grupos alternados se logra forzando discriminantes cuadrados y empleando el Teorema de Irreducibilidad de Hilbert. Además, se exhibe la realización del grupo de los cuaterniones siguiendo una construcción clásica mediante extensiones cuadráticas en torre, aprovechando la estructura del grupo. Por último, se demuestra que los grupos diédricos son también realizables y se hace una mención a los grupos simples finitos.

Palabras clave: teoría de Galois, grupos finitos, polinomios ciclotómicos, permutaciones, discriminante, grupo de los cuaterniones.

Abstract

In the usual perspective of Galois theory, one starts from polynomials to describe their groups of automorphisms. The Inverse Galois Problem seeks to reverse this approach: given a group, one studies whether there exists a polynomial over the field of rational numbers whose Galois group is precisely that group. In this final degree project it is shown that every finite abelian group can be realized as a Galois group within a cyclotomic extension, following the steps that culminated in the Kronecker–Weber theorem. Next, polynomials are constructed whose Galois group is the symmetric group, using the group's transitivity and the presence of certain cycles, always backed by Dedekind's theorem. The realization of alternating groups is achieved by forcing square discriminants and applying Hilbert's Irreducibility Theorem. Also, the realization of the quaternion group is exhibited following a classical construction using a tower of quadratic extensions, exploiting the group's internal structure. Finally, it is shown that the dihedral groups are realizable as well and the finite simple groups are mentioned.

Key words: Galois theory, finite groups, cyclotomic polynomials, permutations, discriminant, quaternion group.

Índice general

Introducción.

En las antiguas tablillas babilónicas se describen procedimientos numéricos para resolver problemas que hoy interpretamos como ecuaciones cuadráticas, utilizando tablas de cuadrados y recíprocos, sin sospechar que aquellas soluciones obedecían a patrones de simetría entre sus raíces. Con la aparición de las fórmulas de *Cardano, Tartaglia y Ferrari* en el Renacimiento, la resolución de las cúbicas y cuárticas comenzó a revelar una estructura oculta: permutar raíces sin alterar la ecuación. El Teorema de *Abel–Ruffini* estableció la imposibilidad de soluciones generales por radicales a partir del quinto grado, y *Lagrange* exploró ya entonces el papel de las permutaciones en las fórmulas de *Cardano* y *Ferrari*. La aportación decisiva se atribuye a *Évariste Galois*, quien consolidó la teoría que hoy lleva su nombre: introdujo el grupo de Galois de un polinomio y estableció una profunda correspondencia entre subcuerpos y subgrupos, uniendo teoría de cuerpos y de grupos.

Invertir esta perspectiva dio lugar al *Problema Inverso de Galois*: para un grupo finito G dado, ¿existe un polinomio en $\mathbb{Q}[X]$ cuyo grupo de Galois sea isomorfo a G? En el caso abeliano, el legado de *Kronecker* y *Weber* muestra que toda extensión ciclotómica de $\mathbb{Q}$ realiza grupos cíclicos finitos, y combinando subextensiones se obtienen productos de cíclicos arbitrarios. Para los grupos simétricos y alternados, *Dedekind* y *Hilbert* aportaron herramientas decisivas: el Teorema de Dedekind permite controlar la aparición de transposiciones y ciclos largos en el grupo de Galois de un polinomio, mientras que el Teorema de Irreducibilidad de Hilbert garantiza que, al considerar polinomios en $\mathbb{Q}(t)$ con grupo de Galois G, existen infinitas especializaciones en $\mathbb{Q}$ que conservan el grupo. El propio *Hilbert* fue el que propuso este problema, aunque no lo incluyó en su célebre lista de problemas para las matemáticas del siglo XX. Sí que incluyo, sin embargo, una generalización del Teorema de Kronecker-Weber a otros cuerpos base que no sean los racionales, subrayando la profundidad de la conexión entre teoría de números, cuerpos y grupos. Además de estas familias clásicas, otros grupos finitos de singular interés, como el cuaterniónico Q_8 exigen técnicas adaptadas: extensiones en torre de grado 2 y análisis de discriminantes. Este trabajo ofrece, para cada familia de grupos, un procedimiento explícito de construcción de polinomios cuyo grupo de Galois coincide con el deseado. Ejemplos detallados ilustran cómo la teoría de Galois, tanto directa como inversa, permite mostrar de modo efectivo las simetrías internas de las ecuaciones polinómicas.

Capítulo 1

Preliminares.

En este capítulo, salvo que así se indique, se seguirán las referencias [9, 15]. Se trata de un capítulo introductorio en el que se exponen resultados previos necesarios para el resto del trabajo.

Primero se introducirá uno de los resultados clásicos sobre los que se sustenta la teoría de números, cuya primera demostración completa se puede encontrar en [8].

Teorema 1.1 (**Pequeño Teorema de Fermat**). *Sea p un número primo, entonces para cada $a \in \mathbb{N}$ tal que $mcd(a,p) = 1$ se cumple que $a^{p-1} \equiv 1 \mod p$.*

Demostración. El teorema es equivalente a enunciar que dado p primo, entonces para todo $a \in \mathbb{N}$ se cumple que $a^p - a \equiv 0 \mod p$.

Se demuestra por inducción sobre los números naturales:

- Sea $n = 1$. De manera trivial, $1^p - 1 \equiv 0 \mod p$ para cualquier número primo p.
- Se supone que el resultado es cierto para todos los números naturales hasta n.

  Se utiliza el binomio de Newton para desarrollar $(n+1)^p = \sum_{k=0}^{p} \binom{p}{k} n^{p-k}$.

  Si se reordena el sumatorio eficazmente, la identidad anterior es equivalente a

  $$(n+1)^p - (n+1) = (n^p - n) + \sum_{k=1}^{p-1} \binom{p}{k} n^{p-k}.$$

  Donde se observa en la parte derecha de la identidad que por hipótesis inductiva $(n^p - n)$ es divisible por p y que el sumatorio también es divisible por p puesto que lo es $\binom{p}{k}$ con $0 < k < p$. Luego $(n+1)^p - (n+1)$ también es divisible por p.

□

Para el desarrollo del trabajo serán fundamentales estos resultados de teoría de grupos:

Lema 1.2. *Sea G un grupo abeliano y sean $x_1, x_2, \ldots, x_m \in G$ tales que $o(x_i) = n_i$ y $mcd(n_i, n_j) = 1$ si $i \neq j$, entonces se tiene que $o(x_1 \cdots x_m) = n_1 \cdots n_m$.*

Demostración. Se tiene que $(x_1x_2)^{n_1n_2} = 1$ puesto que G es abeliano, y por tanto $d = o(x_1x_2) \leq n_1n_2$, en particular $d \mid n_1n_2$. Supóngase por reducción al absurdo que $d < n_1n_2$, entonces $(x_1x_2)^d = 1$ y como G es abeliano se distinguen dos casos:

$x_1^d = x_2^d = 1$. Imposible puesto que, en ese caso: n_1, $n_2 \mid d$ implica que $n_1n_2 \mid d$, luego $d \geq n_1n_2$, lo cual es una contradicción.

$x_1^d \neq 1$ y $x_2^d \neq 1$. También imposible ya que eso supondría que $(x_1^d)^{-1} = x_2^d$, lo que implica por una parte que $x_2^d \in \langle x_1^d \rangle$, luego $o(x_2^d) \mid o(x_1^d) \mid n_1$, y por otra que $o(x_2^d) \mid n_2$. Por tanto, como n_1 y n_2 son primos entre sí se tiene que $o(x_2^d) = 1$, lo que contradice la hipótesis $x_2^d \neq 1$. Luego $d = n_1n_2$. De forma sucesiva se prueba para los m elementos. □

Teorema 1.3 (**Estructura de los grupos abelianos finitos**). *Sea G un grupo abeliano finito. Entonces $G \cong \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_s\mathbb{Z}$ con $n_i | n_{i+1}$, $\forall i < s$.*

A continuación, se definen las raíces de la unidad junto a ciertos conceptos y proposiciones relacionadas que serán esenciales más adelante:

Definición 1.4. Sea $n \in \mathbb{N}$, se dice que α es una *raíz n-ésima de la unidad* si es raíz del polinomio $X^n - 1$. Además, diremos que es *primitiva* si $\alpha^k \neq 1$ para cualquier $k < n$. El conjunto de raíces n-ésimas es: $\{e^{2\pi ik/n} : k \in \mathbb{N}, k \leq n\}$. Se denota como ζ_n a la primera de todas, es decir, $\zeta_n = e^{2\pi i/n}$.

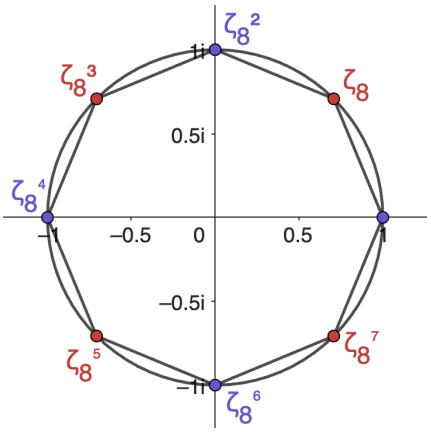


Figura 1.1: Raíces octavas (8-ésimas) de la unidad.

Proposición 1.5. *El conjunto de raíces n-ésimas de la unidad es un grupo cíclico donde ζ_n es un elemento generador del grupo y lo podemos expresar como:*

$$G = \langle \zeta_n \rangle = \{\zeta_n, \zeta_n^2, \ldots, \zeta_n^{n-1}, 1\}$$

Definición 1.6. Sea $n \in \mathbb{N}$, se define el *n-ésimo polinomio ciclotómico* sobre $\mathbb{Q}$ como el polinomio mónico cuyas raíces son exclusivamente las raíces n-ésimas primitivas de la unidad, es decir:

$$\phi_n(X) = \prod_{\substack{0 \leq i < n \\ (i,n)=1}} (X - \zeta_n^i)$$

Proposición 1.7. *Dado $n \in \mathbb{N}$, se tiene que $X^n - 1 = \prod_{d|n} \phi_d(X)$*

Ejemplo 1.8. Se calculan a continuación los primeros seis polinomios ciclotómicos:

$$\phi_1(X) = X - 1$$

$$\phi_2(X) = \frac{X^2-1}{\phi_1(X)} = \frac{X^2-1}{X-1} = X + 1$$

$$\phi_3(X) = \frac{X^3-1}{\phi_1(X)} = \frac{X^3-1}{X-1} = X^2 + X + 1$$

$$\phi_4(X) = \frac{X^4-1}{\phi_1(X)\phi_2(X)} = \frac{X^4-1}{X^2-1} = X^2 + 1$$

$$\phi_5(X) = \frac{X^5-1}{\phi_1(X)} = \frac{X^5-1}{X-1} = X^4 + X^3 + X^2 + X + 1$$

$$\phi_6(X) = \frac{X^6-1}{\phi_1(X)\phi_2(X)\phi_3(X)} = \frac{X^6-1}{(X^2-1)(X^2+X+1)} = X^2 - X + 1$$

Se incluye a continuación una proposición auxiliar relativa al comportamiento de las raíces múltiples en un polinomio, es una propiedad ampliamente conocida con numerosas referencias, concretamente se ha seguido [7]. Aunque su contenido no forma parte esencial del desarrollo de la teoría, su demostración resulta ilustrativa y la propiedad que establece será de utilidad más adelante en cierto razonamiento técnico.

Proposición 1.9. *Sea $f(X) \in K[X]$ un polinomio sobre un cuerpo K. Si $\alpha \in K$ es una raíz de multiplicidad $n > 1$ de $f(X)$, entonces α es raíz de multiplicidad al menos $n - 1$ de la derivada formal $f'(X)$.*

Demostración. Sea $\alpha \in K$ es una raíz de multiplicidad $n > 1$ de $f(X)$. Entonces, existe un polinomio $q(X) \in K[X]$ tal que $f(X) = (X - \alpha)^n q(X)$, con $q(\alpha) \neq 0$. Aplicando la regla del producto para derivadas formales, se obtiene:

$$f'(X) = \frac{d}{dX}[(X-\alpha)^n q(X)] = n(X-\alpha)^{n-1} q(X) + (X-\alpha)^n q'(X).$$

Entonces, se tiene que $f'(X) = (X-\alpha)^{n-1}[nq(X) + (X-\alpha)q'(X)]$. Evaluando en $X = \alpha$, el término $(X-\alpha)^{n-1}$ se anula, por lo tanto, $f'(\alpha) = 0$, y la multiplicidad de α como raíz de $f'(X)$ es al menos $n - 1$. □

Como cabría esperar en un documento que versa sobre el Problema Inverso de Galois, son necesarias ciertas definiciones y resultados básicos de la Teoría de Galois.

Las extensiones de cuerpos actúan como los ladrillos con los que se construye esta Teoría, cuya definición formal se expone a continuación:

Definición 1.10. Sea K un cuerpo, se dice que un cuerpo F es una *extensión de cuerpos* de K si K es un subcuerpo de F, se denota como F/K. De manera que $1_K = 1_F$ y F es un espacio vectorial sobre K.

La dimensión del K-espacio vectorial F se representa por $[F : K]$ y se llama *grado de la extensión* F/K. Una extensión F/K es *finita* cuando $[F : K]$ es finito, en caso contrario se dice que la extensión F/K es *infinita*.

Definición 1.11. Sea F/K una extensión de cuerpos y $\sigma : F \longrightarrow F$ un automorfismo. Se dice que σ *fija* K si para todo $a \in K$ se tiene que $\sigma(a) = a$. En ese caso se dice que σ es un K-automorfismo. El conjunto de K-automorfismos de la extensión F/K se denota como $Aut_K F$.

A partir de esta definición surge de manera natural la cuestión de si $(Aut_K F, \circ)$ tiene alguna estructura algebraica. La respuesta es afirmativa y se demuestra a continuación.

Proposición 1.12. *Sea F/K una extensión de cuerpos. Entonces el conjunto $Aut_K F$ tiene estructura de grupo con la composición de aplicaciones.*

Demostración. Para ver que $Aut_K F$ es un grupo bajo la composición de aplicaciones, se demostrará que se verifican los axiomas fundamentales de grupo.

La composición es una operación interna en $Aut_K F$, sean $\sigma, \tau \in Aut_K F$, entonces $\sigma \circ \tau$ también es un automorfismo de F y fija K, ya que para todo $x \in K$ se tiene

$$(\sigma \circ \tau)(x) = \sigma(\tau(x)) = \sigma(x) = x.$$

Existe un elemento neutro, se observa de manera trivial que la función identidad $Id : F \to F$ es un automorfismo que fija K. Además, para cualquier $\sigma \in Aut_K F$ se cumple que $\sigma \circ Id = \sigma = Id \circ \sigma$.

Cada elemento tiene un inverso, para todo $\sigma \in Aut_K F$, su inversa σ^{-1} también es un automorfismo de F y fija K, ya que si $\sigma(x) = x$ para todo $x \in K$, entonces

$$\sigma^{-1}(x) = \sigma^{-1}(\sigma(x)) = (\sigma^{-1} \circ \sigma)(x) = Id(x) = x.$$

La operación es asociativa, ya que la composición de funciones siempre lo satisface.

$$(\sigma \circ \tau) \circ \rho = \sigma \circ (\tau \circ \rho), \text{ para cualesquiera } \sigma, \tau, \rho \in Aut_K F \qquad \square$$

A partir de este hecho surge uno de los conceptos más elementales en la Teoría de Galois. El grupo de Galois de una extensión de cuerpos, el cual no es más que una redenominación del conjunto de automorfismos dotado de la estructura de grupo.

Definición 1.13. Sea F/K una extensión de cuerpos, entonces al grupo de automorfismos de F que fija K, $Aut_K F$, se le denomina *grupo de Galois* de la extensión F/K y se denota como $Gal(F/K)$.

Las siguientes dos definiciones no son exclusivas de la teoría de Galois. De hecho, son nociones centrales en diversas ramas del álgebra, donde aparecen de manera natural al estudiar soluciones de ecuaciones polinómicas.

Se define a continuación lo que es un elemento algebraico de una extensión, y el polinomio mínimo de un elemento algebraico.

Definición 1.14. Sea F/K una extensión de cuerpos. Se dice que $\alpha \in F$ es un elemento *algebraico* sobre K si α es raíz de algún polinomio no nulo en $K[X]$. En caso contrario, se dice que α es *trascendente* sobre K.

Dada una extensión F/K y un elemento $\alpha \in K$ algebraico, el conjunto de polinomios que se anulan en α es un ideal en el anillo $K[X]$. Como $K[X]$ es un dominio de ideales principales, este ideal está generado por un elemento. Además, se puede tomar un generador del conjunto de polinomios que se anulan en α que sea mónico, irreducible y el de menor grado que lo cumpla, como se indica en la siguiente definición:

Definición 1.15. Sea K un cuerpo, si $p(X) \in K[X]$ es mónico e irreducible tal que $p(\alpha) = 0$, entonces se dice que $p(X)$ es el *polinomio mínimo* de α sobre K.

Uno de los resultados esenciales en la Teoría de Galois es que, si una extensión contiene alguna raíz de un polinomio, entonces los automorfismos de dicha extensión que fijan el cuerpo base permutan estas raíces entre sí. De manera intuitiva puede pensarse que estos automorfismos *envían raíces a raíces* del mismo polinomio.

Teorema 1.16. *Sea F/K una extensión y $p(X) \in K[X]$ un polinomio. Se verifica:*

I) Si $\alpha \in F$ es raíz de $p(X)$ y $\sigma \in Gal(F/K)$, entonces $\sigma(\alpha)$ es raíz de $p(X)$.

II) Si $\alpha \in F$ es algebraico sobre K con polinomio mínimo $p(X)$ de grado n, se tiene que $|Gal(K(\alpha)/K)| = m$, el número de raíces distintas que tiene $p(X)$ en $K(\alpha)$.

El siguiente teorema es el último paso clave que cierra la preparación necesaria para abordar el Teorema Fundamental de la Teoría de Galois.

Teorema 1.17. *Sea F/K una extensión, L un cuerpo intermedio y H un subgrupo de $G = Gal(F/K)$. Entonces:*

I) $H' = \{\alpha \in F : \sigma(\alpha) = \alpha,\ \forall \sigma \in H\}$ *es un cuerpo intermedio de* F/K.

II) $L' = Gal(F/L) = \{\sigma \in G : \sigma(\alpha) = \alpha,\ \forall \alpha \in L\}$.

Definición 1.18. El cuerpo intermedio H' se denomina subcuerpo de F fijado por H.

Consecuencias directas del teorema anterior son las siguientes:

$$F' = Gal(F/F) = 1_G \qquad K' = Gal(F/K) = G \qquad 1'_G = F$$

Sin embargo, no es cierto en general que $G' = K$. Cuando esto sucede, la extensión recibe el nombre, quizás algo previsible, de *extensión de Galois*.

Definición 1.19. Se dice que F/K es una *extensión de Galois* cuando $G' = K$.

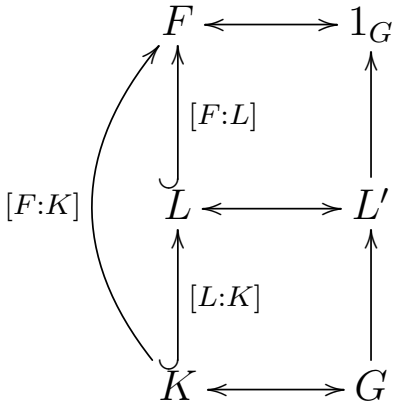
Con todas las herramientas desarrolladas hasta este punto, se está en posición de enunciar el resultado que da sentido y cohesión a toda la teoría:

Teorema 1.20 (**Fundamental de la Teoría de Galois**). *Sea F/K una extensión finita de Galois, entonces existe una biyección entre el conjunto de subcuerpos intermedios de F/K y el conjunto de subgrupos de $G = Aut_K F$.*
Dicha biyección viene dada por $L \mapsto L'$ y satisface:

I) Si $K \subseteq L \subseteq M \subseteq F$, entonces se tiene que: $[M : L] = |Aut_L F : Aut_M F|$.
En particular, $[F : K] = |Aut_K F : Aut_F F| = |Aut_K F|$.

II) Para todo L tal que $K \subseteq L \subseteq F$, F/L es de Galois, y se cumple L/K es de Galois si y solo si $Aut_L F$ es normal en G. En este caso, $Aut_K L \cong G/L'$.

El siguiente diagrama pretende proporcionar una representación visual del Teorema Fundamental de Galois. Se muestran tres niveles: el cuerpo de la extensión F, el cuerpo base K, y un cuerpo intermedio L entre ellos. Las flechas indican las inclusiones de cuerpos y subgrupos, mientras que las relaciones de biyección entre los subgrupos de $G = Gal(F/K)$ y los subcuerpos de F se visualizan mediante las conexiones horizontales entre los elementos correspondientes en el diagrama.



Una vez establecido el marco general de la teoría, es natural preguntarse cómo aplicar estos resultados a casos específicos, como el estudio de un polinomio concreto.

En ese contexto, surge de forma inmediata el concepto de cuerpo de escisión, proporcionando el mínimo cuerpo que contiene todas las raíces de un polinomio dado.

Definición 1.21. Sea F un cuerpo y $p(X) \in F[X]$ un polinomio de grado n. Se dice que $p(X)$ *escinde* en F cuando $p(X)$ puede ser expresado en $F[X]$ de la forma

$$p(X) = \alpha_0(X - \alpha_1) \cdots (X - \alpha_n) \text{ con } \alpha_i \in F \text{ para todo } i \in \{0, \ldots, n\}.$$

Definición 1.22. Sea F/K una extensión y $p(X) \in K[X]$ un polinomio. Se dice que F es un *cuerpo de escisión* de $p(X)$ sobre K cuando:

I) $p(X)$ se escinde en $F[X]$.

II) $F = K(\alpha_1, \ldots, \alpha_n)$ donde $\alpha_1, \ldots, \alpha_n$ son todas las raíces de $p(X)$ en F.

Ejemplo 1.23. El polinomio $p(X) = X^2 - 5$ no escinde en $\mathbb{Q}$ porque es irreducible al no tener raíces racionales. Sin embargo, escinde en $\mathbb{Q}(\sqrt{5})$ ya que se puede expresar en $\mathbb{Q}(\sqrt{5})[X]$ de la forma $p(X) = (X - \sqrt{5})(X + \sqrt{5})$.
De hecho, $\mathbb{Q}(\sqrt{5})$ es un cuerpo de escisión de $p(X)$ porque $\mathbb{Q}(\sqrt{5}, -\sqrt{5}) = \mathbb{Q}(\sqrt{5})$.

Estas definiciones presentan una reformulación clásica de la Teoría de Galois en términos de cuerpos de escisión y polinomios. A partir de este punto, se adoptará la notación clásica para el grupo de Galois de una extensión F/K, expresándolo como $Gal(p(X))$, donde F es el cuerpo de escisión del polinomio $p(X)$ sobre K. Esta notación será empleada de manera consistente a lo largo de todo el trabajo.

Definición 1.24. Sea $p(X) \in K[X]$ un polinomio y F un cuerpo de escisión de $p(X)$ sobre K. El *grupo de Galois del polinomio* $p(X)$ sobre K se define como el grupo de Galois de la extensión F/K.

A continuación se proporciona el cálculo del grupo de Galois de dos polinomios:

Ejemplo 1.25. Sea el polinomio $p(X) = X^2 - 5$, irreducible sobre $\mathbb{Q}$.

Sus raíces son $\pm\sqrt{5}$, luego como se vio en el Ejemplo 1.23 su cuerpo de escisión es $\mathbb{Q}(\sqrt{5}) = \{a + b\sqrt{5} : a, b \in \mathbb{Z}\}$.

Los automorfismos que fijan $\mathbb{Q}$ estarán unívocamente determinados por la imagen de sus raíces y son:

$$\begin{array}{rccc} \sigma_1 : & \mathbb{Q}(\sqrt{5}) & \longrightarrow & \mathbb{Q}(\sqrt{5}) \\ & \sqrt{5} & \longmapsto & \sqrt{5} \end{array} \qquad \begin{array}{rccc} \sigma_2 : & \mathbb{Q}(\sqrt{5}) & \longrightarrow & \mathbb{Q}(\sqrt{5}) \\ & \sqrt{5} & \longmapsto & -\sqrt{5} \end{array}$$

Esto indica que el grupo de Galois de $p(X)$ es un grupo de 2 elementos, luego es isomorfo al grupo cíclico de orden 2:

$$Gal(X^2 - 5) \cong \mathbb{Z}/2\mathbb{Z}$$

Ejemplo 1.26. Sea $q(X) = X^4 - 2 \in \mathbb{Q}[X]$, se calcula a continuación su grupo de Galois.

Una comprobación sencilla es suficiente para ver que las raíces de $q(X)$ son $\sqrt[4]{2}, \sqrt[4]{2}i, -\sqrt[4]{2}$ y $-\sqrt[4]{2}i$, luego su cuerpo de escisión es $\mathbb{Q}(\sqrt[4]{2}, i)$. El polinomio mínimo de $\sqrt[4]{2}$ es el propio $q(X)$, sin embargo el de i es $r(X) = X^2 + 1$ cuyas raíces son i e $-i$.

Conociendo esto es posible determinar los automorfismos que fijan $\mathbb{Q}$ en $\mathbb{Q}(\sqrt[4]{2}, i)$.

$$\begin{array}{rccc} \sigma_1: & \mathbb{Q}(\sqrt[4]{2},i) & \longrightarrow & \mathbb{Q}(\sqrt[4]{2},i) \\ & \sqrt[4]{2} & \longmapsto & \sqrt[4]{2} \\ & i & \longmapsto & i \end{array} \qquad \begin{array}{rccc} \sigma_2: & \mathbb{Q}(\sqrt[4]{2},i) & \longrightarrow & \mathbb{Q}(\sqrt[4]{2},i) \\ & \sqrt[4]{2} & \longmapsto & \sqrt[4]{2} \\ & i & \longmapsto & -i \end{array}$$

$$\begin{array}{rccc} \sigma_3: & \mathbb{Q}(\sqrt[4]{2},i) & \longrightarrow & \mathbb{Q}(\sqrt[4]{2},i) \\ & \sqrt[4]{2} & \longmapsto & -\sqrt[4]{2} \\ & i & \longmapsto & i \end{array} \qquad \begin{array}{rccc} \sigma_4: & \mathbb{Q}(\sqrt[4]{2},i) & \longrightarrow & \mathbb{Q}(\sqrt[4]{2},i) \\ & \sqrt[4]{2} & \longmapsto & -\sqrt[4]{2} \\ & i & \longmapsto & -i \end{array}$$

$$\begin{array}{rccc} \sigma_5: & \mathbb{Q}(\sqrt[4]{2},i) & \longrightarrow & \mathbb{Q}(\sqrt[4]{2},i) \\ & \sqrt[4]{2} & \longmapsto & \sqrt[4]{2}i \\ & i & \longmapsto & i \end{array} \qquad \begin{array}{rccc} \sigma_6: & \mathbb{Q}(\sqrt[4]{2},i) & \longrightarrow & \mathbb{Q}(\sqrt[4]{2},i) \\ & \sqrt[4]{2} & \longmapsto & \sqrt[4]{2}i \\ & i & \longmapsto & -i \end{array}$$

$$\begin{array}{rccc} \sigma_7: & \mathbb{Q}(\sqrt[4]{2},i) & \longrightarrow & \mathbb{Q}(\sqrt[4]{2},i) \\ & \sqrt[4]{2} & \longmapsto & -\sqrt[4]{2}i \\ & i & \longmapsto & i \end{array} \qquad \begin{array}{rccc} \sigma_8: & \mathbb{Q}(\sqrt[4]{2},i) & \longrightarrow & \mathbb{Q}(\sqrt[4]{2},i) \\ & \sqrt[4]{2} & \longmapsto & -\sqrt[4]{2}i \\ & i & \longmapsto & -i \end{array}$$

Se observa que

$$\sigma_2 \circ \sigma_2(a + b\sqrt[4]{2} + ci) = \sigma_2(\sigma_2(a + b\sqrt[4]{2} + ci)) = \sigma_2(a + b\sqrt[4]{2} - ci) = a + b\sqrt[4]{2} + ci.$$

$$\sigma_3 \circ \sigma_3(a + b\sqrt[4]{2} + ci) = \sigma_3(\sigma_3(a + b\sqrt[4]{2} + ci)) = \sigma_3(a - b\sqrt[4]{2} + ci) = a + b\sqrt[4]{2} + ci.$$

Luego el grupo de Galois de $q(X)$ tiene al menos dos elementos de orden 2 y además se tiene que

$$\sigma_2 \circ \sigma_5(a + b\sqrt[4]{2} + ci) = \sigma_2(\sigma_5(a + b\sqrt[4]{2} + ci)) = \sigma_2(a + b\sqrt[4]{2}i + ci) = a - b\sqrt[4]{2}i - ci$$

$$\sigma_5 \circ \sigma_2(a + b\sqrt[4]{2} + ci) = \sigma_5(\sigma_2(a + b\sqrt[4]{2} + ci)) = \sigma_5(a + b\sqrt[4]{2} - ci) = a + b\sqrt[4]{2}i - ci$$

Lo que indica que es un grupo no abeliano de orden 8. Sin embargo, el grupo de los cuaterniones Q_8 tiene únicamente un elemento de orden 2, resultando de manera directa en que debe ser isomorfo al grupo diédrico D_4.

$$Gal(X^4 - 2) \cong D_4.$$

Definición 1.27. Sea G un subgrupo del grupo simétrico S_n, se dice que G es *transitivo* si para cualesquiera $1 \leq i, j \leq n$ con $i \neq j$ existe $\sigma \in G$ tal que $\sigma(i) = j$.

En su formulación clásica, la teoría de Galois describe cada extensión de cuerpos mediante las permutaciones que los automorfismos efectúan sobre las propias raíces de un polinomio. Para un polinomio de grado n, su grupo de Galois se puede entender como un subgrupo de S_n, el grupo de permutaciones de esas n raíces.

Teorema 1.28. *Sea K un cuerpo y $f(X) \in K[X]$ irreducible, de grado n, sin raíces múltiples, con grupo de Galois G. Entonces G es isomorfo a un subgrupo transitivo de S_n.*

Demostración. Primero se ve que G es un subgrupo de S_n. Sean $\alpha_1, \ldots, \alpha_n$ todas las n raíces distintas de $f(X)$ en algún cuerpo de escisión F de K. Entonces, por el Teorema 1.16 se observa que cada automorfismo induce una permutación en el conjunto de raíces de $f(X)$. Es decir, si para cada automorfismo $\sigma \in Gal(F/K)$ se considera la restricción al conjunto de raíces, $r : Gal(F/K) \longrightarrow S_n$ tal que $r(\sigma) = \sigma|_{\{\alpha_1,\ldots,\alpha_n\}}$, este es un monomorfismo de grupos, luego $G \subseteq S_n$. Se ve a continuación que G es transitivo. Nótese que el polinomio mínimo de todas las α_i es el polinomio mónico asociado a $f(X)$. Si α_i, α_j son dos raíces distintas de $f(X)$, existe un $K-$isomorfismo $\tau : K(\alpha_i) \longrightarrow K(\alpha_j)$ tal que $\tau(\alpha_i) = \alpha_j$. Como F es cuerpo de escisión de $f(X)$ sobre $K(\alpha_i)$ y $K(\alpha_j)$, entonces τ se extiende a un $K-$automorfismo de F. Por tanto, G es transitivo. □

Una observación a tener en cuenta es que, si $m > n$, puede construirse una aplicación natural de inclusión $i : S_n \hookrightarrow S_m$, la cual es claramente inyectiva. Esto permite considerar S_n como un subgrupo de S_m, identificando cada permutación de n elementos con su extensión trivial que fija los elementos restantes. Así, los grupos simétricos forman una familia creciente de grupos, donde cada $S_n \subseteq S_m$ con $m > n$.

Cada permutación puede expresarse de manera no única como producto de trasposiciones, y la paridad del número de trasposiciones en dichas descomposiciones es invariante. La siguiente definición formaliza este concepto.

Definición 1.29. Una permutación $\sigma \in S_n$ es par (o impar) si puede ser expresado mediante un número par (o impar) de trasposiciones. Se define la *signatura* de σ como:

$$\epsilon(\sigma) = \begin{cases} 1 & \text{si } \sigma \text{ es par} \\ -1 & \text{si } \sigma \text{ es impar} \end{cases}$$

Equivalentemente, si s es el número de pares que invierte σ; es decir, los pares $i, j \in S_n$ tal que $i < j$ y $\sigma(j) < \sigma(i)$; entonces $\epsilon(\sigma) = (-1)^s$.

El siguiente resultado es un teorema central sobre las permutaciones en los grupos simétricos, su demostración se aborda con lujo de detalle en [15].

Teorema 1.30. *Sea $\sigma \in S_n$ con $\sigma \neq Id$. Entonces, σ es un ciclo o es una composición de ciclos disjuntos. Además, esta descomposición es única (salvo reordenación de los ciclos).*

En la primera sección del Capítulo 3, dedicado al estudio de los grupos simétricos S_p, con p primo, resultará de gran utilidad describir la naturaleza de sus elementos de orden p. El siguiente lema se ha obtenido de [2] y caracteriza de manera precisa dichos elementos.

Lema 1.31. *Sea p un número primo. Entonces una permutación $\sigma \in S_p$ tiene orden p si y solo si σ es un ciclo de longitud p.*

Demostración. Sea $\sigma \in S_p$ de orden p. Se considera la descomposición de σ en ciclos disjuntos: $\sigma = \gamma_1 \gamma_2 \cdots \gamma_r$, donde cada γ_i es un ciclo de longitud $k_i > 1$. Entonces el orden de σ es $\operatorname{mcm}\big(k_1, k_2, \ldots, k_r\big) = p$. En consecuencia, como p es primo, todos los k_i deben ser igual a p. Entonces σ es el producto de ciclos disjuntos de longitud p, sin embargo en S_p no pueden existir ni siquiera dos ciclos disjuntos de longitud p. Se concluye que σ es un ciclo de longitud p. □

Los polinomios irreducibles son una pieza fundamental en la Teoría de Galois, por esto es importante disponer de condiciones suficientes para determinar si un polinomio es o no irreducible sobre el cuerpo de los racionales. Se introducen dos criterios de irreducibilidad.

Teorema 1.32 (Irreducibilidad módulo p). *Sea $f(X) = a_n X^n + \cdots + a_1 X + a_0 \in \mathbb{Z}[X]$ un polinomio primitivo (es decir, el máximo común divisor de sus coeficientes es 1) con $\deg f(X) \geq 1$ y sea p un primo que no divide a a_n. Si $\overline{f(X)} \in \mathbb{F}_p[X]$ es la reducción de $f(X)$ módulo p, entonces*

$$\overline{f(X)} \text{ irreducible en } \mathbb{F}_p[X] \quad \Longrightarrow \quad f(X) \text{ irreducible en } \mathbb{Z}[X].$$

Demostración. Se probará el contrarrecíproco. Supóngase, por el contrario, que $f(X)$ es reducible en $\mathbb{Z}[X]$. Entonces existe $g(X) = b_r X^r + \cdots + b_0, h(X) = c_s X^s + \cdots + c_0$ en $\mathbb{Z}[X]$, con $r, s \geq 1$ y $f(X) = g(X)h(X)$. Como $f(X)$ es primitivo, no hay factores comunes entre los coeficientes de $g(X)$ y los de $h(X)$, además $a_n = b_r c_s$ no es divisible por p, de modo que $p \nmid b_r$ y $p \nmid c_s$. Al reducir módulo p se obtiene $\overline{f(X)} = \overline{g(X)h(X)} = \overline{g(X)}\,\overline{h(X)}$ y como $\deg \overline{g(X)} = \deg g(X)$ y $\deg \overline{h(X)} = \deg h(X)$ son estrictamente positivos, se deduce que $\overline{f(X)}$ es reducible en $\mathbb{F}_p[X]$. □

Ejemplo 1.33. Se debe destacar que el recíproco del Criterio anterior no es cierto en general. Es sencillo ver que el polinomio $p(X) = X^2 + 2X + 2$ es irreducible en $\mathbb{Z}[X]$, ya que es un polinomio cuadrático cuyas raíces son $\alpha_1 = -1 + i, \alpha_2 = -1 - i$. Sin embargo si se considera su reducción módulo $p = 2$ se obtiene el polinomio $\overline{f(X)} = X^2$, el cual es reducible en $\mathbb{F}_2[X]$. Por lo que la siguiente implicación es falsa.

$$f(X) \text{ irreducible en } \mathbb{Z}[X] \quad \not\Longrightarrow \quad \overline{f(X)} \text{ irreducible en } \mathbb{F}_p[X].$$

Teorema 1.34 (**Criterio de Eisenstein**). *Sea* $f(X) = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$ *un polinomio de grado* $n \in \mathbb{N}$ *con coeficientes enteros. Si existe* $p \in \mathbb{N}$ *primo tal que*

$$p \mid a_i \text{ para todo } i \in \{0, 1, \ldots, n-1\}, \quad p \nmid a_n, \quad p^2 \nmid a_0.$$

Entonces $f(X)$ *es irreducible sobre* $\mathbb{Q}[X]$. *Si, además,* $f(X)$ *es primitivo, entonces* $f(X)$ *es irreducible sobre* $\mathbb{Z}[X]$.

Demostración. Sea $d = \text{mcd}(a_0, \ldots, a_n)$ y $f(X) = df_1(X)$, con $f_1(X) \in \mathbb{Z}[X]$ primitivo. Basta probar que $f_1(X)$ es irreducible en $\mathbb{Z}[X]$. Se razona por reducción al absurdo, supóngase que $f_1(X)$ es reducible, entonces existen

$$g(X) = b_rX^r + \cdots + b_1X + b_0, \quad h(X) = c_sX^s + \cdots + c_1X + c_0$$

en $\mathbb{Z}[X]$, con $r, s \geq 1$, tales que $f_1(X) = g(X)h(X)$. Como $p \nmid a_n$, entonces $p \nmid d$, y por tanto p satisface las hipótesis del Teorema sobre los coeficientes de $f_1(X)$. Se escribe ahora

$$f_1(X) = a_n'X^n + \cdots + a_1'X + a_0'.$$

Por hipótesis, $p \mid a_i'$ para $0 \leq i < n$ por lo que, en concreto, $p \mid a_0'$ y $p^2 \nmid a_0'$. De la factorización $f_1(X) = g(X)h(X)$ se sigue que $p \mid b_0c_0$ pero $p^2 \nmid b_0c_0$, de modo que exactamente uno de entre b_0, c_0 es divisible por p.

Sin pérdida de generalidad se supone que $p \mid b_0$ y $p \nmid c_0$. Si además $p \mid b_i$ para todo $i \leq r$, entonces $f_1(X)$ no sería primitivo, luego se considera k el menor índice con $p \nmid b_k$ (luego $1 \leq k \leq r < n$). Si se observa el coeficiente de X^k en $g(X)h(X)$ se obtiene que,

$$a_k' = b_0c_k + b_1c_{k-1} + \cdots + b_{k-1}c_1 + b_kc_0.$$

Por último, como $p \mid b_i$ para cada $i < k$ y $p \mid a_k'$, se concluye que $p \mid b_kc_0$. Pero $p \nmid b_k$ por definición de k, luego debe ocurrir que $p \mid c_0$, contradicción con que $p^2 \nmid b_0c_0$.

Por tanto f_1 es irreducible en $\mathbb{Z}[X]$. □

Por último se presenta un resultado clásico sobre extensiones necesario en el Capítulo 5.

Proposición 1.35. *Sea* K *un cuerpo de característica distinta de* 2 *y sean* $a, b \in K$, *entonces* $K(\sqrt{a}) = K(\sqrt{b}) \iff \dfrac{a}{b}$ *es un cuadrado en* K.

Demostración. Sea $K(\sqrt{a}) = K(\sqrt{b})$, si $\sqrt{a} \in K$ entonces $K = K(\sqrt{a})$ y $\sqrt{b} \in K$ por lo que $\dfrac{a}{b}$ es un cuadrado en K. Supóngase por el contrario que $\sqrt{a} \notin K$, entonces $\sqrt{a} = x + y\sqrt{b}$ con $x, y \in K$. Al elevar al cuadrado, $a = x^2 + 2xy\sqrt{b} + y^2b$, y como $\sqrt{b} \notin K$ sigue $xy = 0$. Si $y = 0$ sería $\sqrt{a} = x \in K$, imposible, luego $x = 0$ y $a = y^2b$, por lo que $\dfrac{a}{b} = y^2$ es un cuadrado en K. Sea ahora $\dfrac{a}{b} = z^2$ con $z \in K$, entonces $a = bz^2$ por lo que $\sqrt{a} = z\sqrt{b} \in K(\sqrt{b})$ y $\sqrt{b} = \dfrac{\sqrt{a}}{z} \in K(\sqrt{a})$, de donde $K(\sqrt{a}) = K(\sqrt{b})$. □

Capítulo 2

Realización de los grupos Abelianos Finitos.

Como se ha visto anteriormente en este trabajo, existen polinomios sencillos cuyo grupo de Galois es abeliano finito (ver Ejemplo 1.25) luego no es casualidad que el primer instinto al estudiar el Problema Inverso de Galois sea el de considerar estos. Además, se dispone de una clasificación concreta con su Teorema de Estructura 1.3 y sus propiedades son bien conocidas.

Este capítulo se divide en dos secciones, en la primera se dará una prueba formal de que todos los grupos cíclicos finitos son realizables sobre $\mathbb{Q}$ y en la segunda se dará una construcción de los productos de grupos cíclicos. Se seguirán las referencias [9, 15].

2.1. Grupos Cíclicos Finitos.

En esta sección se dará una prueba constructiva y con ejemplos de la realización de los grupos cíclicos finitos. Esta demostración se sustentará principalmente en las propiedades de las extensiones ciclotómicas y en una versión débil del Teorema de Dirichlet sobre primos en progresiones aritméticas.

Primero se expone una proposición fundamental para alcanzar el objetivo, esta da una caracterización del grupo de Galois del polinomio ciclotómico de orden n a partir del grupo multiplicativo de las unidades del anillo $\mathbb{Z}/n\mathbb{Z}$.

Proposición 2.1. *Sea $n \in \mathbb{N}$, se verifica que $Gal(\phi_n(X)) \cong (\mathbb{Z}/n\mathbb{Z})^*$.*

Demostración. $Gal(\phi_n(X))$ está formado por los automorfismos de $\mathbb{Q}(\zeta_n)$ que fijan $\mathbb{Q}$, que estarán unívocamente determinados por la imagen de ζ_n. Además, sabemos que las imágenes deben ser las raíces primitivas n-ésimas de la unidad, por el Teorema 1.16.

Luego se cumple la siguiente igualdad:

$$Gal(\phi_n(X)) = \{\sigma_i : \sigma_i(\zeta_n) = \zeta_n^i, i \in \mathbb{N},\ \text{mcd}(i,n) = 1\}.$$

Consideremos ahora la siguiente aplicación y veamos que es un isomorfismo de grupos:

$$\begin{array}{rccc} f: & Gal(\phi_n(X)) & \longrightarrow & (\mathbb{Z}/n\mathbb{Z})^* \\ & \sigma_i & \longmapsto & i \end{array}$$

En primer lugar f es un morfismo de grupos, pues para todo $x \in \mathbb{Q}(\zeta_n)$ se tiene:

$$\sigma_i \circ \sigma_j(x) = (x^i)^j = x^{ij} = \sigma_{ij}(x), \text{ luego } f(\sigma_i \circ \sigma_j) = i \cdot j = f(\sigma_i) \cdot f(\sigma_j).$$

Además f es claramente una aplicación biyectiva ya que $(\mathbb{Z}/n\mathbb{Z})^*$ está formado por los elementos de $\mathbb{Z}/n\mathbb{Z}$ coprimos con n, luego es un isomorfismo de grupos y se obtiene el resultado requerido. □

A partir de la Proposición 2.1 se obtiene de manera trivial el siguiente resultado que involucra la función φ de Euler:

Corolario 2.2. $|Gal(\phi_n(X))| = \varphi(n)$.

Lema 2.3. *Sea $p \in \mathbb{N}$ primo, entonces $G = (\mathbb{Z}/p\mathbb{Z})^*$ es isomorfo a $\mathbb{Z}/(p-1)\mathbb{Z}$.*

Demostración. Sea $a \in G$, entonces por el Teorema 1.1 se cumple que $a^{p-1} = 1$, además sabemos que el orden de a divide a $p-1$.

Supongamos que existe $r < p-1$ tal que $a^r = 1$ para todo $a \in G$, luego el polinomio $X^r - 1$ tiene $p-1$ raíces en $\mathbb{Z}/p\mathbb{Z}$, pero $\mathbb{Z}/p\mathbb{Z}$ es cuerpo luego tiene a lo sumo tantas raíces como su grado, es decir $r \geq p-1$, lo cual es absurdo.

Luego G contiene algún elemento cuyo orden es el orden del grupo y como G es un grupo abeliano finito entonces este debe ser cíclico. Por unicidad de los grupos cíclicos, como G tiene $p-1$ elementos debe ser isomorfo a $\mathbb{Z}/(p-1)\mathbb{Z}$. □

Para la realización de los grupos cíclicos finitos sobre $\mathbb{Q}$ es fundamental el Teorema de Dirichlet sobre primos en progresiones aritméticas, que enuncia que existe un número infinito de primos en toda progresión aritmética sobre $\mathbb{N}$ y cuya demostración se escapa del contenido de este trabajo.

Sin embargo, solo será necesario un caso específico del teorema cuya demostración se encuentra en [10] y que resulta más sencilla que el caso general. Para la prueba de este teorema se necesitará un lema previo.

Lema 2.4 (**Aritmética de los polinomios ciclotómicos**). *Dados $k, n \in \mathbb{N}$,*

(1) *Los enteros n y $\phi_n(kn)$ son primos entre sí.*

(2) *Existe un entero $m_0 > 1$ tal que $|\phi_n(mn)| > 1$ para todo $m \geq m_0$.*

(3) *Sea p primo, si p divide a $\phi_n(k)$ pero no a n, entonces $p-1$ es múltiplo de n.*

Demostración. **(1)** Se consideran los siguientes polinomios sobre $\mathbb{Z}$:

$$f(X) = X^n - 1, \quad g(X) = \prod_{\substack{d|n \\ d<n}} \phi_d(X),$$

que según se vio en la Proposición 1.7 cumplen la igualdad $f(X) = \phi_n(X) \cdot g(X)$.

Se razona por reducción al absurdo. Si $\text{mcd}(n, \phi_n(kn)) \neq 1$ entonces existe q número primo que divide a ambos. Sea Ψ_q el homomorfismo reducción módulo q definido como:

$$\begin{array}{rccc} \Psi_q : & \mathbb{Z}[X] & \longrightarrow & \mathbb{Z}/q\mathbb{Z}[X] \\ & \displaystyle\sum_{i=0}^{r} a_i \cdot X^i & \longmapsto & \displaystyle\sum_{i=0}^{r} (a_i \text{ mód } q) \cdot X^i \end{array}$$

Aplicando el homomorfismo Ψ_q sobre la igualdad $f(X) = \phi_n(X) \cdot g(X)$ resulta que:

$$\Psi_q(f) = \Psi_q(\phi_n \cdot g) = \Psi_q(\phi_n) \cdot \Psi_q(g).$$

Evaluado en $kn \equiv 0$ mód q (pues $q|n$) se obtiene:

$$-1 \text{ mód } q \equiv \Psi_q(f)(kn) \equiv \Psi_q(\phi_n)(kn) \cdot \Psi_q(g)(kn) \equiv \phi_n(kn) \cdot \Psi_q(g)(kn) \equiv 0 \text{ mód } q,$$

lo cual es una contradicción que proviene de suponer que $\text{mcd}(n, \phi_n(kn)) \neq 1$, por lo que n y $\phi_n(kn)$ deben ser primos entre sí.

(2) Se define el siguiente polinomio sobre $\mathbb{Z}$: $h(X) = (\phi_n(nX)-1) \cdot \phi_n(nX) \cdot (\phi_n(nX)+1)$, el cual no es nulo puesto que ninguno de sus factores lo es. Luego tiene un número finito de raíces reales. Sea m_0 el menor entero positivo tal que $h(m) \neq 0$ para todo $m \geq m_0$. En particular, $\phi_n(nm)$ es un número entero distinto de $-1, 0$ y 1, dicho de otro modo $|\phi_n(nm)| > 1$ para todo $m \geq m_0$.

(3) Recuperando las notaciones del primer apartado, sea p un número primo tal que $f(k) = k^n - 1 = \phi_n(k) \cdot g(k) \equiv 0$ mód p, claramente k no es múltiplo de p. Bajo esta hipótesis se tiene que k mód $p \in (\mathbb{Z}/p\mathbb{Z})^*$, y vamos a probar que su orden es n. Visto esto, se obtendría que $n = o(k \text{ mód } p)$ divide al orden de $(\mathbb{Z}/p\mathbb{Z})^*$ que es $p-1$, como se quería demostrar.

Se define $e = o(k \bmod p)$ que verifica $e \leq n$ ya que $k^n \equiv 1 \bmod p$ y se supone, por reducción al absurdo, que la desigualdad es estricta. En tal caso e es un divisor propio de n, y por tanto existe un polinomio $R(X) \in \mathbb{Z}[X]$ tal que

$$X^n - 1 = \phi_n(X) \cdot \prod_{\substack{d|n \\ d<n}} \phi_d(X) = \phi_n(X) \cdot \prod_{d|e} \phi_d(X) \cdot R(X) = \phi_n(X) \cdot (X^e - 1) \cdot R(X)$$

Sea $\Psi_p : \mathbb{Z}[X] \longrightarrow \mathbb{Z}/p\mathbb{Z}[X]$ el homomorfismo reducción módulo p, se define

$$\hat{f}(X) = X^n - 1 = \Psi_p(X^n - 1) = \Psi_p(\phi_n(X)) \cdot (X^e - 1) \cdot \Psi_p(R(X)).$$

Esto implica que $k \bmod p$ es raíz múltiple de $\hat{f}(X)$, ya que por hipótesis $\phi_n(k) \equiv 0 \bmod p$ y $k^e - 1 \equiv 0 \bmod p$. Luego por la Proposición 1.9, $\hat{f}'(k)$ debe ser nulo pero como k y n no son múltiplos de p sucede que: $\hat{f}'(k) = nk^{n-1} \not\equiv 0 \bmod p$. □

Tras haber probado el Lema 2.4 ya se tienen los resultados previos necesarios para demostrar una forma débil del Teorema de Dirichlet.

Teorema 2.5 (**Forma débil del Teorema de Dirichlet**). *Sea $n \in \mathbb{N}$, entonces existen infinitos números primos $p \equiv 1 \bmod n$.*

Demostración. La prueba consiste en aplicar los diferentes apartados del Lema anterior.

Por el apartado (2) existe un entero positivo m_0 tal que $|\phi_n(m_0 n)| > 1$, por lo que $\phi_n(m_0 n)$ tiene algún divisor primo p_1. Por el apartado (1), p_1 no divide a n y esto, a su vez, implica por el apartado (3) que $p_1 \equiv 1 \bmod n$.

Para finalizar bastará demostrar que dados $p_1, p_2, \ldots, p_r$ primos distintos tales que $p_i \equiv 1 \bmod n$ para $1 \leq i \leq r$, se puede hallar otro primo p_{r+1} distinto de todos los anteriores que cumpla $p_{r+1} \equiv 1 \bmod n$.

Se define $m = p_1 \cdots p_r n$, por el apartado (2) existe un entero positivo t tal que $|\phi_m(tm)| > 1$. Se escoge p_{r+1} un divisor primo arbitrario de $\phi_m(tm)$. Del apartado (1) se obtiene que p_{r+1} no es divisor de m, luego tampoco puede serlo de ningún p_i para todo $1 \leq i \leq r$. Además, por el apartado (3), $p_{r+1} - 1$ es múltiplo de m, luego también de n. Por lo que $p_{r+1} \equiv 1 \bmod n$. □

Aunque el Teorema anterior proporciona una prueba constructiva para hallar primos congruentes con la unidad módulo n para cualquier natural $n \in \mathbb{N}$, es fundamental comprender que estos no serán siempre los más pequeños que cumplan esa relación de congruencia, a continuación se presenta un ejemplo para ilustrar esto.

Ejemplo 2.6. Sea $n = 5$, primero se considera el polinomio ciclotómico de grado 5,

$$\phi_5(X) = X^4 + X^3 + X^2 + X + 1.$$

Siguiendo la prueba del Teorema 2.5, existe un entero $m_0 > 1$ tal que $|\phi_5(5m_0)| > 1$, se observa que basta tomar $m_0 = 2$, de manera que $|\phi_5(5 \cdot 2)| = |\phi(10)| = 11111 = 41 \cdot 271$.

Entonces, efectivamente $p_1 = 41$ es un factor primo de 11111 y se tiene que $p_1 \equiv 1$ mód 5. Sin embargo, está claro que el primer primo congruente con 1 mód 5 es $p_2 = 11$.

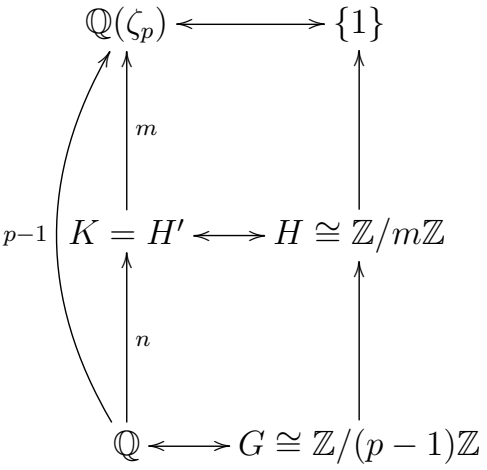
De hecho, si se sigue con la construcción de más primos se aprecia un fenómeno interesante; se define $m = 41 \cdot 5 = 205$ y se puede tomar $t = 2$, de manera que $|\phi_5(m \cdot t)| = |\phi_5(410)| = 28326699511 = 11 \cdot 2711 \cdot 949891$, obteniendo $p_2 = 11$. Esto último pone de manifiesto que, en general, esta generación de primos no seguirá un orden conocido.

Para finalizar esta sección se completa la demostración de que todos los grupos cíclicos finitos aparecen como grupos de Galois de algún polinomio sobre $\mathbb{Q}$, sentando una base sólida para abordar posteriormente casos más complejos del Problema Inverso.

Se ha diseñado un diagrama que proporciona una explicación visual y complementa la prueba al teorema, donde se observan las extensiones y sus grados, con los grupos de automorfismos a la derecha y los respectivos cuerpos que fijan a la izquierda.

Teorema 2.7 (**Realización de los grupos Cíclicos finitos**). *Sea $n \in \mathbb{N}$, entonces existe $K/\mathbb{Q}$ extensión de Galois con $Gal(K/\mathbb{Q}) \cong \mathbb{Z}/n\mathbb{Z}$.*

Demostración. Por el Teorema 2.5 se tiene que existe $m \in \mathbb{N}$ tal que $p = 1 + nm$ es primo. Sea ζ_p una raíz primitiva p-ésima de la unidad, entonces se obtiene por la Proposición 2.1 que $G = Gal(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^*$ y que es cíclico por el Lema 2.3.
Como G es cíclico y de orden $p - 1 = nm$ existe algún subgrupo $H \subseteq G$ con $|H| = m$. Sea $K = H'$ el cuerpo que fija H, como G es abeliano se tiene que H es normal luego por el Teorema 1.20 (Fundamental de la Teoría de Galois), la extensión $K/\mathbb{Q}$ será de Galois y $Gal(K/\mathbb{Q}) \cong G/H \cong \mathbb{Z}/(p-1)\mathbb{Z}\big/\mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}/n\mathbb{Z}$. □



Ejemplo 2.8. Se desea encontrar $p(X) \in \mathbb{Q}[X]$ cuyo grupo de Galois sea $G = \mathbb{Z}/3\mathbb{Z}$.

Basándose en la construcción del Teorema 2.7 anterior. Se escoge $m \in \mathbb{N}$ tal que $p = 1+3m$ es primo, por ejemplo $m = 2$. De esta manera $p = 1 + 3 \cdot 2 = 7$ es primo.

Sea $\alpha = \zeta_7$ una raíz primitiva séptima de la unidad y se considera la extensión ciclotómica $\mathbb{Q}(\alpha)/\mathbb{Q}$ cuyo polinomio mínimo es $\phi_7(X) = X^6 + X^5 + X^4 + X^3 + X^2 + X + 1$ de grado 6 e irreducible, con raíces $\{\alpha^i : 1 \leq i \leq 6\}$. Por tanto, el grupo de automorfismos que fija $\mathbb{Q}$ en $\mathbb{Q}(\alpha)$ estará compuesto por los siguientes seis automorfismos:

$$
\begin{array}{lccc}
\sigma_1: & \mathbb{Q}(\alpha) & \longrightarrow & \mathbb{Q}(\alpha) \\
 & \alpha & \longmapsto & \alpha \\
 & \alpha^2 & \longmapsto & \alpha^2 \\
 & \alpha^3 & \longmapsto & \alpha^3 \\
 & \alpha^4 & \longmapsto & \alpha^4 \\
 & \alpha^5 & \longmapsto & \alpha^5 \\
 & \alpha^6 & \longmapsto & \alpha^6
\end{array}
\qquad
\begin{array}{lccc}
\sigma_2: & \mathbb{Q}(\alpha) & \longrightarrow & \mathbb{Q}(\alpha) \\
 & \alpha & \longmapsto & \alpha^2 \\
 & \alpha^2 & \longmapsto & \alpha^4 \\
 & \alpha^3 & \longmapsto & \alpha^6 \\
 & \alpha^4 & \longmapsto & \alpha \\
 & \alpha^5 & \longmapsto & \alpha^3 \\
 & \alpha^6 & \longmapsto & \alpha^5
\end{array}
\qquad
\begin{array}{lccc}
\sigma_3: & \mathbb{Q}(\alpha) & \longrightarrow & \mathbb{Q}(\alpha) \\
 & \alpha & \longmapsto & \alpha^3 \\
 & \alpha^2 & \longmapsto & \alpha^6 \\
 & \alpha^3 & \longmapsto & \alpha^2 \\
 & \alpha^4 & \longmapsto & \alpha^5 \\
 & \alpha^5 & \longmapsto & \alpha \\
 & \alpha^6 & \longmapsto & \alpha^4
\end{array}
$$

$$
\begin{array}{lccc}
\sigma_4: & \mathbb{Q}(\alpha) & \longrightarrow & \mathbb{Q}(\alpha) \\
 & \alpha & \longmapsto & \alpha^4 \\
 & \alpha^2 & \longmapsto & \alpha \\
 & \alpha^3 & \longmapsto & \alpha^5 \\
 & \alpha^4 & \longmapsto & \alpha^2 \\
 & \alpha^5 & \longmapsto & \alpha^6 \\
 & \alpha^6 & \longmapsto & \alpha^3
\end{array}
\qquad
\begin{array}{lccc}
\sigma_5: & \mathbb{Q}(\alpha) & \longrightarrow & \mathbb{Q}(\alpha) \\
 & \alpha & \longmapsto & \alpha^5 \\
 & \alpha^2 & \longmapsto & \alpha^3 \\
 & \alpha^3 & \longmapsto & \alpha \\
 & \alpha^4 & \longmapsto & \alpha^6 \\
 & \alpha^5 & \longmapsto & \alpha^4 \\
 & \alpha^6 & \longmapsto & \alpha^2
\end{array}
\qquad
\begin{array}{lccc}
\sigma_6: & \mathbb{Q}(\alpha) & \longrightarrow & \mathbb{Q}(\alpha) \\
 & \alpha & \longmapsto & \alpha^6 \\
 & \alpha^2 & \longmapsto & \alpha^5 \\
 & \alpha^3 & \longmapsto & \alpha^4 \\
 & \alpha^4 & \longmapsto & \alpha^3 \\
 & \alpha^5 & \longmapsto & \alpha^2 \\
 & \alpha^6 & \longmapsto & \alpha
\end{array}
$$

Por los órdenes de sus respectivos automorfismos se observa que $Aut_{\mathbb{Q}}(\mathbb{Q}(\alpha)) \cong \mathbb{Z}/6\mathbb{Z}$. Conectando la Proposición 2.1 y el Lema 2.3 se llegaría a la misma conclusión, sin embargo, hallando los órdenes de los elementos se puede encontrar el único subgrupo de $\mathbb{Z}/6\mathbb{Z}$ isomorfo a $\mathbb{Z}/2\mathbb{Z}$, el cual es $H = \{\sigma_1, \sigma_6\}$. Se calcula el subcuerpo K que fija H, de manera que $Gal(K/\mathbb{Q}) \cong Gal(\mathbb{Q}(\alpha)/\mathbb{Q})/H \cong \mathbb{Z}/6\mathbb{Z}\big/\mathbb{Z}/2\mathbb{Z} \cong \mathbb{Z}/3\mathbb{Z}$.

$\sigma_1 \equiv Id_{\mathbb{Q}(\alpha)}$ luego basta con ver que subcuerpo de $\mathbb{Q}(\alpha)$ fija el automorfismo σ_6.

Por definición $K = \{a \in \mathbb{Q}(\alpha) : \sigma_6(a) = a\}$, luego dado $x \in \mathbb{Q}(\alpha)$ se determinará a continuación bajo qué condiciones se cumple que $\sigma_6(x) = x$.

Sea $x \in \mathbb{Q}(\alpha)$, como $\{\alpha^i : 1 \leq i \leq 7\}$ es base para la extensión $\mathbb{Q}(\alpha)/\mathbb{Q}$ se tiene que $x = a_0 + a_1\alpha + a_2\alpha^2 + a_3\alpha^3 + a_4\alpha^4 + a_5\alpha^5 + a_6\alpha^6$ para algunos $a_i \in \mathbb{Q}$, $0 \leq i \leq 6$.

Si $\sigma_6(x) = x$ significa que $\sigma_6(x) = \sigma_6(a_0 + a_1\alpha + a_2\alpha^2 + a_3\alpha^3 + a_4\alpha^4 + a_5\alpha^5 + a_6\alpha^6) = a_0+a_6\alpha+a_5\alpha^2+a_4\alpha^3+a_3\alpha^4+a_2\alpha^5+a_1\alpha^6 = a_0+a_1\alpha+a_2\alpha^2+a_3\alpha^3+a_4\alpha^4+a_5\alpha^5+a_6\alpha^6 = x$.

Se concluye que $a_1 = a_6$, $a_2 = a_5$ y $a_3 = a_4$, es decir, si $x \in K$, este se puede expresar como $x = a_0+a_1\alpha+a_2\alpha^2+a_3\alpha^3+a_3\alpha^4+a_2\alpha^5+a_1\alpha^6 = a_0+a_1(\alpha+\alpha^6)+a_2(\alpha^2+\alpha^5)+a_3(\alpha^3+\alpha^4)$ con $a_i \in \mathbb{Q}$, $0 \leq i \leq 3$. Entonces, ¿cuál es el cuerpo K y cuál es su polinomio mínimo?

Estas preguntas no son fácilmente contestables en general, sin embargo en el contexto de muchas extensiones y de este problema como ejemplo concreto, si se puede comprobar que $\alpha + \alpha^6, \alpha^2 + \alpha^5, \alpha^3 + \alpha^4$ son raíces del mismo polinomio mónico e irreducible en $\mathbb{Q}$, entonces $K = \mathbb{Q}(\alpha + \alpha^6)$ y el polinomio mínimo es el ya mencionado.

Una manera de hallar este polinomio es simplemente comprobar si

$$p(X) = [X - (\alpha + \alpha^6)][X - (\alpha^2 + \alpha^5)][X - (\alpha^3 + \alpha^4)]$$

es un polinomio mónico e irreducible con coeficientes racionales, porque entonces este será el polinomio. A continuación se calcula $p(X)$ teniendo en cuenta que α es tanto raíz de $X^7 - 1$ como de $\phi_7(X)$.

$[X-(\alpha+\alpha^6)][X-(\alpha^2+\alpha^5)][X-(\alpha^3+\alpha^4)] = X^3+[-(\alpha+\alpha^6)-(\alpha^2+\alpha^5)-(\alpha^3+\alpha^4)]X^2+[(\alpha+\alpha^6)(\alpha^2+\alpha^5)+(\alpha+\alpha^6)(\alpha^3+\alpha^4)+(\alpha^2+\alpha^5)(\alpha^3+\alpha^4)]X-(\alpha+\alpha^6)(\alpha^2+\alpha^5)(\alpha^3+\alpha^4) = X^3 + [-\alpha - \alpha^2 - \alpha^3 - \alpha^4 - \alpha^5 - \alpha^6]X^2 + [\alpha^3 + \alpha^6 + \alpha + \alpha^4 + \alpha^4 + \alpha^5 + \alpha^2 + \alpha^3 + \alpha^5 + \alpha^6 + \alpha + \alpha^2]X - (\alpha^3 + \alpha^6 + \alpha + \alpha^4)(\alpha^3 + \alpha^4) = X^3 + X^2 + [2(\alpha + \alpha^2 + \alpha^3 + \alpha^4 + \alpha^5 + \alpha^6)]X - (\alpha^6 + 1 + \alpha^2 + \alpha^3 + \alpha^4 + \alpha^5 + 1 + \alpha) = X^3 + X^2 - 2X - 1.$

Para finalizar, efectivamente $p(X) = X^3 + X^2 - 2X - 1$ es irreducible y mónico, luego $K = \mathbb{Q}(\alpha + \alpha^6)$ y $p(X)$ es su polinomio mínimo que cumple

$$Gal(p(X)) \cong Gal(\phi_7(X))/H \cong \mathbb{Z}/6\mathbb{Z}\Big/\mathbb{Z}/2\mathbb{Z} \cong \mathbb{Z}/3\mathbb{Z}.$$

Como cierre de esta sección, es algo sencillo de probar que el polinomio del ejemplo anterior no es el único de grado 3 con ese grupo de Galois. Entonces, dado que $\mathbb{Z}/3\mathbb{Z}$ es el único grupo finito de orden 3, ¿cualquier polinomio irreducible de grado 3 tiene grupo de Galois $\mathbb{Z}/3\mathbb{Z}$? La respuesta es negativa, salvo que se limite la discusión a extensiones de Galois, donde el grado del polinomio mínimo coincide con el orden del grupo. El hecho sobre el que se sustenta esta contestación es que polinomios de un cierto grado pueden tener como grupo de Galois un grupo de orden mayor, en este caso $S_3 = D_3$ (de orden 6) también puede ser el grupo de automorfismos de un polinomio cúbico. Se puede demostrar que $q(X) = X^3 - 3X + 1$ es también un polinomio irreducible con grupo de Galois $\mathbb{Z}/3\mathbb{Z}$. Sea α una raíz de $q(X)$. Las otras dos raíces β, γ serán raíces de

$$\frac{q(X)}{(X-\alpha)} = X^2 + \alpha X + (\alpha^2 - 3) = (X - \beta)(X - \gamma) = X^2 - (\beta + \gamma)X + \beta\gamma,$$

de manera que $\beta + \gamma = -\alpha$, $\beta\gamma = \alpha^2 - 3$. Es sencillo comprobar que $\beta = \alpha^2 - 2$, $\gamma = -\alpha^2 - \alpha + 2$ son estas raíces, de forma que $\beta, \gamma \in \mathbb{Q}(\alpha)$. Se concluye que la extensión $\mathbb{Q}(\alpha)/\mathbb{Q}$ es de Galois, y por tanto $Gal(q(X)) \cong \mathbb{Z}/3\mathbb{Z}$.

2.2. Grupos Abelianos Finitos.

Se presenta a continuación el último lema que da paso a la solución al Problema Inverso de Galois para Grupos Abelianos Finitos.

Lema 2.9. *Sean $n_1, n_2, \ldots, n_k \in \mathbb{N}$ primos entre sí. Para cada $i \leq k$ sea ζ_i una raíz primitiva n_i-ésima de la unidad, entonces se cumple que $\zeta = \zeta_1\zeta_2 \ldots \zeta_k$ es una raíz $n_1n_2 \ldots n_k$-ésima de la unidad y $Gal(\mathbb{Q}(\zeta)/\mathbb{Q}) \cong (\mathbb{Z}/n_1\mathbb{Z})^* \times (\mathbb{Z}/n_2\mathbb{Z})^* \times \cdots \times (\mathbb{Z}/n_k\mathbb{Z})^*$.*

Demostración. Por definición, cada ζ_i tiene orden n_i en $(\mathbb{C}^*, \cdot)$ y como es un grupo abeliano, tenemos por el Lema 1.2 que ζ tiene orden $n_1n_2 \ldots n_t$, es decir, ζ es una raíz $n_1n_2 \ldots n_t$-ésima primitiva de la unidad. Entonces por la Proposición 2.1 y como $\text{mcd}(n_i, n_j) = 1$ si $i \neq j$ se tiene que

$$Gal(\mathbb{Q}(\zeta)/\mathbb{Q}) \cong (\mathbb{Z}/n_1n_2 \cdots n_k\mathbb{Z})^* \cong (\mathbb{Z}/n_1\mathbb{Z})^* \times (\mathbb{Z}/n_2\mathbb{Z})^* \times \cdots \times (\mathbb{Z}/n_k\mathbb{Z})^*. \qquad \square$$

Ejemplo 2.10. Se toman ζ_3 y ζ_5 raíces primitivas de la unidad cúbica y quinta, respectivamente. Entonces $\zeta = \zeta_3\zeta_5$ es una raíz 15-ésima de la unidad, puesto que $3 \cdot 5 = 15$. Esto supone que $Gal(\mathbb{Q}(\zeta)/\mathbb{Q}) \cong (\mathbb{Z}/15\mathbb{Z})^* \cong (\mathbb{Z}/3\mathbb{Z})^* \times (\mathbb{Z}/5\mathbb{Z})^*$. Por el Lema 2.3 se sabe que $(\mathbb{Z}/3\mathbb{Z})^* = \mathbb{Z}/2\mathbb{Z}$ y $(\mathbb{Z}/5\mathbb{Z})^* = \mathbb{Z}/4\mathbb{Z}$. Como conclusión se obtiene que: $Gal(\mathbb{Q}(\zeta)/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$.

Finalmente, se da la realización de los grupos Abelianos finitos sobre los racionales:

Teorema 2.11 (**Realización de los grupos Abelianos finitos**). *Sea G un grupo abeliano finito, entonces existe una extensión de Galois $K/\mathbb{Q}$ tal que $Gal(K/\mathbb{Q}) \cong G$.*

Demostración. Como G es un grupo abeliano finito, por el Teorema 1.3 (Estructura), este se puede expresar como $G \cong \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z}$, con $n_1, \ldots, n_k \in \mathbb{N}$.

Además, por el Teorema 2.7, existen k números primos $p_1, p_2, \ldots, p_k$ que se puede garantizar que son distintos (ya que hay infinitos por el Teorema 2.5) y k únicos subgrupos asociados $H_1, H_2, \ldots, H_k$ de manera que $H_i \leq (\mathbb{Z}/p_i\mathbb{Z})^*$, que tienen índice n_i y orden $m_i = \dfrac{p_i - 1}{n_i}$. Por tanto se tiene que $(\mathbb{Z}/p_i\mathbb{Z})^*/H_i \cong \mathbb{Z}/n_i\mathbb{Z}$, para todo $1 \leq i \leq k$.

Sea $\zeta = \zeta_1\zeta_2 \cdots \zeta_k$ una raíz $p_1p_2 \cdots p_k$-ésima de la unidad, utilizando la notación del Lema 2.9 previo se tiene que $Gal(\mathbb{Q}(\zeta)/\mathbb{Q}) \cong (\mathbb{Z}/p_1\mathbb{Z})^* \times (\mathbb{Z}/p_2\mathbb{Z})^* \times \cdots \times (\mathbb{Z}/p_k\mathbb{Z})^*$.

Se define ahora $H = H_1 \times \cdots \times H_k$ subgrupo normal de $Gal(\mathbb{Q}(\zeta)/\mathbb{Q})$ porque este es abeliano y sea $K = H'$ el cuerpo que fija. Por el Teorema 1.20 (Fundamental de la Teoría de Galois), K es una extensión de Galois sobre $\mathbb{Q}$ y se obtiene que

$$Gal(K/\mathbb{Q}) \cong Gal(\mathbb{Q}(\zeta)/\mathbb{Q})/H \cong G. \qquad \square$$

Como ejemplo final se calcula un polinomio cuyo grupo de Galois sea abeliano finito.

Ejemplo 2.12. Se desea encontrar $p(X) \in \mathbb{Q}[X]$ cuyo grupo de Galois sea el grupo

$$G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}.$$

Como en el Teorema 2.11, se realiza $\mathbb{Z}/2\mathbb{Z}$ sobre $\mathbb{Q}$ de dos maneras distintas, y distintas también del cuerpo con el que se realice $\mathbb{Z}/4\mathbb{Z}$.

Primero, se buscan primos p_1 y p_2 distintos de manera que $p_i = 2m_i + 1$ para algunos $m_1, m_2 \in \mathbb{N}$ y $p_3 = 4m_3 + 1$ con $m_3 \in \mathbb{N}$. Como ejemplo óptimo se toman $m_1 = 1$, $m_2 = 3$ y $m_3 = 1$ que generan los primos $p_1 = 3$, $p_2 = 7$, $p_3 = 5$. Esto quiere decir por el Lema 2.9, que $\zeta_{105} = \zeta_3 \cdot \zeta_7 \cdot \zeta_5$ es una raíz 105-ésima de la unidad y que

$$Gal(\mathbb{Q}(\zeta_{105})/\mathbb{Q}) \cong (\mathbb{Z}/3\mathbb{Z})^* \times (\mathbb{Z}/7\mathbb{Z})^* \times (\mathbb{Z}/5\mathbb{Z})^* \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}.$$

Aunque el objeto principal de estudio sea la extensión $\mathbb{Q}(\zeta_{105})/\mathbb{Q}$, un aspecto esencial que surge a la hora de realizar ejemplos, es que resulta fundamental analizar también como se comportan las subextensiones $\mathbb{Q}(\zeta_3)/\mathbb{Q}$, $\mathbb{Q}(\zeta_7)/\mathbb{Q}$ y $\mathbb{Q}(\zeta_5)/\mathbb{Q}$ por separado. Así se consigue comprender cómo interactúan entre sí dentro de la estructura de la extensión mayor.

A continuación se listan los grupos de automorfismos de $\mathbb{Q}(\zeta_3)$, $\mathbb{Q}(\zeta_5)$ y $\mathbb{Q}(\zeta_7)$.

$Aut_{\mathbb{Q}}(\mathbb{Q}(\zeta_3)) = \{\tau_1, \tau_2\}$, donde:

$$\begin{array}{rccc} \tau_1: & \mathbb{Q}(\zeta_3) & \longrightarrow & \mathbb{Q}(\zeta_3) \\ & \zeta_3 & \longmapsto & \zeta_3 \end{array} \qquad \begin{array}{rccc} \tau_2: & \mathbb{Q}(\zeta_3) & \longrightarrow & \mathbb{Q}(\zeta_3) \\ & \zeta_3 & \longmapsto & \zeta_3^2 \end{array}$$

$Aut_{\mathbb{Q}}(\mathbb{Q}(\zeta_7)) = \{\sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5, \sigma_6\}$, donde:

$$\begin{array}{rccc} \sigma_1: & \mathbb{Q}(\zeta_7) & \longrightarrow & \mathbb{Q}(\zeta_7) \\ & \zeta_7 & \longmapsto & \zeta_7 \end{array} \qquad \begin{array}{rccc} \sigma_2: & \mathbb{Q}(\zeta_7) & \longrightarrow & \mathbb{Q}(\zeta_7) \\ & \zeta_7 & \longmapsto & \zeta_7^2 \end{array}$$

$$\begin{array}{rccc} \sigma_3: & \mathbb{Q}(\zeta_7) & \longrightarrow & \mathbb{Q}(\zeta_7) \\ & \zeta_7 & \longmapsto & \zeta_7^3 \end{array} \qquad \begin{array}{rccc} \sigma_4: & \mathbb{Q}(\zeta_7) & \longrightarrow & \mathbb{Q}(\zeta_7) \\ & \zeta_7 & \longmapsto & \zeta_7^4 \end{array}$$

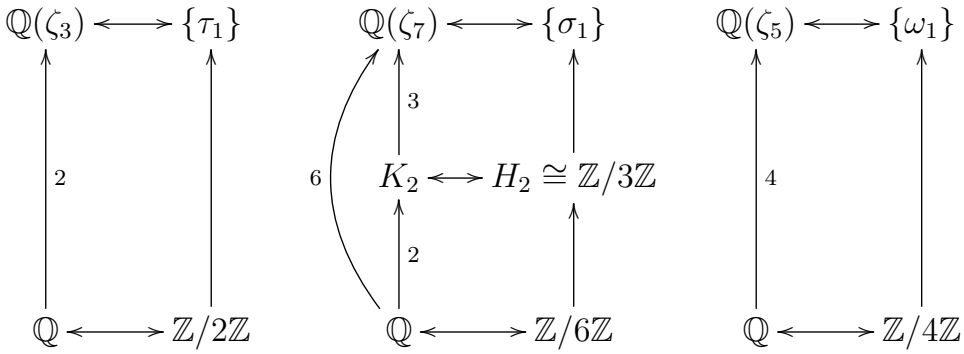
$$\begin{array}{rccc} \sigma_5: & \mathbb{Q}(\zeta_7) & \longrightarrow & \mathbb{Q}(\zeta_7) \\ & \zeta_7 & \longmapsto & \zeta_7^5 \end{array} \qquad \begin{array}{rccc} \sigma_6: & \mathbb{Q}(\zeta_7) & \longrightarrow & \mathbb{Q}(\zeta_7) \\ & \zeta_7 & \longmapsto & \zeta_7^6 \end{array}$$

$Aut_{\mathbb{Q}}(\mathbb{Q}(\zeta_5)) = \{\omega_1, \omega_2, \omega_3, \omega_4\}$, donde:

$$\begin{array}{rccc} \omega_1: & \mathbb{Q}(\zeta_5) & \longrightarrow & \mathbb{Q}(\zeta_5) \\ & \zeta_5 & \longmapsto & \zeta_5 \end{array} \qquad \begin{array}{rccc} \omega_2: & \mathbb{Q}(\zeta_5) & \longrightarrow & \mathbb{Q}(\zeta_5) \\ & \zeta_5 & \longmapsto & \zeta_5^2 \end{array}$$

$$\begin{array}{rccc} \omega_3: & \mathbb{Q}(\zeta_5) & \longrightarrow & \mathbb{Q}(\zeta_5) \\ & \zeta_5 & \longmapsto & \zeta_5^3 \end{array} \qquad \begin{array}{rccc} \omega_4: & \mathbb{Q}(\zeta_5) & \longrightarrow & \mathbb{Q}(\zeta_5) \\ & \zeta_5 & \longmapsto & \zeta_5^4 \end{array}$$

Bajo la notación del capítulo, se aprecia de forma directa que: $H_1 = \{\tau_1\}$ fija $\mathbb{Q}(\zeta_3)$ con grupo de Galois $\mathbb{Z}/2\mathbb{Z}$ y $H_3 = \{\omega_1\}$ fija $\mathbb{Q}(\zeta_5)$ con grupo de Galois $\mathbb{Z}/4\mathbb{Z}$. Luego basta encontrar $H_2 \subseteq Aut_{\mathbb{Q}}(\mathbb{Q}(\zeta_7))$ de orden $m_2 = 3$.



Una comprobación sencilla es suficiente para observar que $H_2 = \{\sigma_1, \sigma_2, \sigma_4\}$ es un grupo de orden 3 cuyo cuerpo fijo es $K_2 = \mathbb{Q}(\zeta_7+\zeta_7^2+\zeta_7^4)$. De manera breve, σ_1 es la identidad en $\mathbb{Q}(\zeta_7)$ y tanto σ_2 como σ_4 tienen orden 3. Además los elementos fijados por H_2 se pueden expresar de la forma $a + b(\zeta_7 + \zeta_7^2 + \zeta_7^4) + c(\zeta_7 + \zeta_7^2 + \zeta_7^4)^2$.

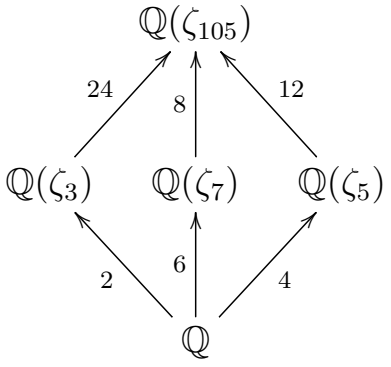
Siguiendo la construcción del Teorema 2.11 el último paso es considerar $H = H_1 \times H_2 \times H_3$ junto con el subcuerpo que fija dentro de $\mathbb{Q}(\zeta_{105})$. Aunque los elementos de H_1, H_2 y H_3 son automorfismos en $\mathbb{Q}(\zeta_3)$, $\mathbb{Q}(\zeta_7)$ y $\mathbb{Q}(\zeta_5)$, respectivamente, luego las siguientes cuestiones se plantean de manera espontánea:

1. ¿Cómo se puede interpretar $H = H_1 \times H_2 \times H_3$ dentro de $Aut_{\mathbb{Q}}(\mathbb{Q}(\zeta_{105}))$?
2. ¿Qué cuerpo fija H y qué vínculo guarda con los subcuerpos fijados por H_1, H_2 y H_3?

La respuesta a la primera pregunta no es inmediata, y su resolución requiere explorar en profundidad la naturaleza de $Aut_{\mathbb{Q}}(\mathbb{Q}(\zeta_{105})) = \{\rho_j : \rho_j(\zeta_n) = \zeta_n^j, j \in \mathbb{N},\ \text{mcd}(j, 105) = 1\}$.

Resulta habitual en Matemáticas el estudio de un objeto a través de su representación en formas diversas, para extraer de su comparación una comprensión más profunda.

En este contexto, el paso esencial es entender $\mathbb{Q}(\zeta_{105})$ como $\mathbb{Q}(\zeta_3, \zeta_7, \zeta_5)$, de manera que cada automorfismo de $\mathbb{Q}(\zeta_{105})$ se puede reinterpretar unívocamente como una composición de uno de $\mathbb{Q}(\zeta_3)$ con otro de $\mathbb{Q}(\zeta_7)$ y otro de $\mathbb{Q}(\zeta_5)$. Entre los $\varphi(105) = 48$ automorfismos que hay en $\mathbb{Q}(\zeta_{105})$, en este caso reciben especial interés los siguientes:
$\rho_1 = \tau_1 \circ \sigma_1 \circ \sigma_1$, $\rho_{16} = \tau_1 \circ \sigma_2 \circ \sigma_1$, $\rho_{46} = \tau_1 \circ \sigma_4 \circ \sigma_1$.
De manera que $H = H_1 \times H_2 \times H_3$ el cual se traduce como $\{\tau_1\} \times \{\sigma_1, \sigma_2, \sigma_4\} \times \{\omega_1\} = \{\rho_1, \rho_{16}, \rho_{46}\}$.



En cuanto a la segunda cuestión, su resolución resulta más delicada. A continuación se determina el cuerpo fijo por H y su polinomio mínimo. Para ello, se comienza analizando la forma que presentan los elementos de $\mathbb{Q}(\zeta_{105})$ que son invariantes bajo la acción de H:

Sea $I = \{i \in \mathbb{N} : i < 105,\ \text{mcd}(i, 105) = 1\}$, entonces dado $x \in \mathbb{Q}(\zeta_{105})$, este se escribe:

$$x = \sum_{i \in I} a_i \cdot \zeta_{105}^i \in \mathbb{Q}(\zeta_{105}), \quad \text{con } a_i \in \mathbb{Q} \text{ para todo } i \in I$$

Entonces $\rho_1 = Id$ lo deja siempre invariante, luego el siguiente paso es hallar la forma que tienen los elementos fijados tanto por ρ_{16} como por ρ_{46}, de modo que si se simplifican las expresiones $\rho_{16}(x) = x$ y $\rho_{46}(x) = x$ simultáneamente, se obtiene que los elementos fijos en el cuerpo extensión bajo la acción de H son

$$a_1(\zeta_{105}^1+\zeta_{105}^{16}+\zeta_{105}^{46})+a_2(\zeta_{105}^2+\zeta_{105}^{32}+\zeta_{105}^{92})+a_4(\zeta_{105}^4+\zeta_{105}^{64}+\zeta_{105}^{79})+a_8(\zeta_{105}^8+\zeta_{105}^{23}+\zeta_{105}^{53})+$$
$$a_{11}(\zeta_{105}^{11}+\zeta_{105}^{71}+\zeta_{105}^{86})+a_{13}(\zeta_{105}^{13}+\zeta_{105}^{103}+\zeta_{105}^{73})+a_{17}(\zeta_{105}^{17}+\zeta_{105}^{62}+\zeta_{105}^{47})+a_{19}(\zeta_{105}^{19}+\zeta_{105}^{94}+\zeta_{105}^{34})+$$
$$a_{22}(\zeta_{105}^{22}+\zeta_{105}^{37}+\zeta_{105}^{67})+a_{26}(\zeta_{105}^{26}+\zeta_{105}^{101}+\zeta_{105}^{41})+a_{29}(\zeta_{105}^{29}+\zeta_{105}^{44}+\zeta_{105}^{74})+a_{31}(\zeta_{105}^{31}+\zeta_{105}^{76}+\zeta_{105}^{61})+$$
$$a_{38}(\zeta_{105}^{38}+\zeta_{105}^{83}+\zeta_{105}^{68})+a_{43}(\zeta_{105}^{43}+\zeta_{105}^{58}+\zeta_{105}^{88})+a_{52}(\zeta_{105}^{52}+\zeta_{105}^{97}+\zeta_{105}^{82})+a_{59}(\zeta_{105}^{59}+\zeta_{105}^{104}+\zeta_{105}^{89}).$$

Se han omitido los cálculos debido a su extensión, pero es entendible que se ha hecho de manera análoga al Ejemplo 2.8. Con una metodología similar al Ejemplo ya mencionado, aunque de manera más costosa (es por ello que de nuevo se omite), se ha comprobado que los siguientes 16 elementos de $\mathbb{Q}(\zeta_{105})$

α_1	$\zeta_{105} + \zeta_{105}^{16} + \zeta_{105}^{46}$
α_2	$\zeta_{105}^{2} + \zeta_{105}^{32} + \zeta_{105}^{92}$
α_4	$\zeta_{105}^{4} + \zeta_{105}^{64} + \zeta_{105}^{79}$
α_8	$\zeta_{105}^{8} + \zeta_{105}^{23} + \zeta_{105}^{53}$
α_{11}	$\zeta_{105}^{11} + \zeta_{105}^{71} + \zeta_{105}^{86}$
α_{13}	$\zeta_{105}^{13} + \zeta_{105}^{103} + \zeta_{105}^{73}$
α_{17}	$\zeta_{105}^{17} + \zeta_{105}^{62} + \zeta_{105}^{47}$
α_{19}	$\zeta_{105}^{19} + \zeta_{105}^{94} + \zeta_{105}^{34}$

α_{22}	$\zeta_{105}^{22} + \zeta_{105}^{37} + \zeta_{105}^{67}$
α_{26}	$\zeta_{105}^{26} + \zeta_{105}^{101} + \zeta_{105}^{41}$
α_{29}	$\zeta_{105}^{29} + \zeta_{105}^{44} + \zeta_{105}^{74}$
α_{31}	$\zeta_{105}^{31} + \zeta_{105}^{76} + \zeta_{105}^{61}$
α_{38}	$\zeta_{105}^{38} + \zeta_{105}^{83} + \zeta_{105}^{68}$
α_{43}	$\zeta_{105}^{43} + \zeta_{105}^{58} + \zeta_{105}^{88}$
α_{52}	$\zeta_{105}^{52} + \zeta_{105}^{97} + \zeta_{105}^{82}$
α_{59}	$\zeta_{105}^{59} + \zeta_{105}^{104} + \zeta_{105}^{89}$

Cuadro 2.1: Valores de α_i como combinaciones de raíces primitivas de la unidad ζ_{105}.

son las raíces del polinomio mónico e irreducible

$$p(X) = X^{16} + X^{15} + 2X^{14} + 5X^{13} + 5X^{12} - X^{11} + 6X^{10} - 5X^9 - 21X^8$$
$$-10X^7 + 24X^6 - 8X^5 + 80X^4 + 160X^3 + 128X^2 + 128X + 256.$$

Como conclusión, el cuerpo fijado por H en $\mathbb{Q}(\zeta_{105})$ es $K = \mathbb{Q}(\zeta_{105}+\zeta_{105}^{16}+\zeta_{105}^{46})$, este tiene polinomio mínimo $p(X)$ y como grupo de Galois

$$Gal(p(X)) \cong \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/6\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}\Big/H \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}.$$

2.3. Teorema de Kronecker-Weber.

Uno de los resultados fundamentales dentro del Problema Inverso de Galois es el Teorema de Kronecker-Weber (1853). La primera demostración completa fue publicada por David Hilbert en 1896, se puede encontrar dicha prueba en [12].

Teorema 2.13 (**Kronecker-Weber**). *Sea $K/\mathbb{Q}$ una extensión cuyo grupo de Galois es abeliano y finito, entonces existe $n \in \mathbb{N}$ tal que $K \subseteq \mathbb{Q}(\zeta_n)$.*

De entrada, podría parecer simplemente una reformulación del Teorema 2.11 expuesto en la sección anterior: "Todos los grupos Abelianos finitos pueden realizarse como grupos de Galois de subextensiones ciclotómicas". Sin embargo, este aporta una diferencia tan sutil como esencial, no solo se tiene que los grupos abelianos finitos pueden realizarse dentro de extensiones ciclotómicas, sino que afirma que absolutamente todas las extensiones de $\mathbb{Q}$ cuyo grupo de Galois sea abeliano están contenidas en ellas.

Este resultado proporciona una percepción global dentro de la Teoría de Cuerpos, las extensiones ciclotómicas no son solamente un método para construir ejemplos, sino el marco universal que rige todas las extensiones abelianas sobre $\mathbb{Q}$.

Desde los trabajos de Gauss sobre construcciones con regla y compás hasta la formulación moderna del Teorema de Kronecker–Weber, la idea de entender cuerpos abelianos a través de raíces de la unidad ha sido un hilo conductor en la historia del álgebra. Como toda extensión finita con grupo de Galois abeliano se incorpora de manera natural a un cuerpo generado por raíces de la unidad, los elementos de dicha extensión admiten una descripción explícita en términos de las raíces primitivas. Este hecho determina que existe una forma de escribir cualquier entero algebraico cuyo grupo de Galois sea abeliano como combinación lineal de dichas raíces.

Corolario 2.14. *Sea $K/\mathbb{Q}$ una extensión finita con grupo de Galois abeliano finito entonces para cualquier entero algebraico $\alpha \in K$ existe $n \in \mathbb{N}$ tal que α se escribe de modo único como:*

$$\alpha = \sum_{k=1}^{n} a_k \cdot \zeta_n^k, \quad \text{con } a_k \in \mathbb{Q} \text{ para todo } k \in \mathbb{N},\ mcd(k,n) = 1.$$

Ejemplo 2.15. Las raíces cuadradas $\sqrt{5}$ y $\sqrt{7}$ son elementos algebraicos en $\mathbb{Q}$, puesto que son raíces de los polinomios $X^2 - 5$ y $X^2 - 7$, respectivamente. Además, su grupo de Galois es, en ambos casos $\mathbb{Z}/2\mathbb{Z}$ (ver Ejemplo 1.25). Según el resultado anterior, se pueden expresar como sumas y restas de raíces de la unidad, concretamente

$$\sqrt{5} = \zeta_5 - \zeta_5^2 - \zeta_5^3 + \zeta_5^4,$$

$$\sqrt{7} = \zeta_{28} + \zeta_{28}^3 - \zeta_{28}^5 - \zeta_{28}^{23} + \zeta_{28}^{25} + \zeta_{28}^{27}.$$

Capítulo 3

Realización del grupo Simétrico S_n.

Tras el estudio de los grupos abelianos finitos, cuya realización se cimienta en la teoría de cuerpos ciclotómicos y la manipulación directa de raíces de la unidad, este capítulo se adentra en un territorio de una complejidad mayor: los grupos simétricos. Para S_n es preciso forzar la aparición de transposiciones y asegurar la existencia de ciclos de longitud n. De este modo, se revela una dinámica completamente distinta a la de las extensiones abelianas.

En este capítulo se seguirán diversas referencias. En primer lugar, se examinan algunos resultados concretos [18], estos van a permitir ilustrar y contextualizar el problema mediante casos más sencillos. Para finalizar el capítulo, la construcción general de S_n se fundamentará en las ideas de van der Waerden recogidas en su libro *Algebra* [22].

3.1. Grupos Simétricos de orden primo.

Como ya se ha mencionado, existe un conjunto de grupos simétricos cuya realización resulta más directa que el caso general. Efectivamente, si $p \in \mathbb{N}$ es primo entonces se puede ver que S_p es fácilmente realizable sobre $\mathbb{Q}$, utilizando únicamente herramientas de teoría de grupos elemental.

Para alcanzar el objetivo, en las siguientes líneas se expone una caracterización de S_p. Aunque se enuncie de manera equivalente, esta dice que si un subgrupo $H \subseteq S_p$ contiene una transposición y un ciclo de tamaño p entonces $H = S_p$.

Lema 3.1. *Sea $p \in \mathbb{N}$ primo, entonces para cualquier transposición $\sigma \in S_p$ y cualquier ciclo $\tau \in S_p$ de tamaño p, se tiene que el grupo simétrico $S_p =< \sigma, \tau >$.*

Demostración. Sea $\sigma \in S_p$ una transposición, renombrando los elementos de S_p se puede suponer sin pérdida de generalidad que $\sigma = (1\ 2)$.

Sea $\tau \in S_p$ un ciclo de tamaño p, entonces este se puede reordenar de tal manera que $\tau = (1\ \ n_2\ \ ...\ \ n_p)$ para algunos $n_i \in \mathbb{N}$, con $n_i \neq n_j$ si $i \neq j$.

Se observa que existe $k < p$ tal que $c = \tau^k$ verifica $c(1) = 2$, es decir, $c = (1\ \ 2\ \ m_3\ \ ...\ \ m_p)$. Nuevamente, renombrando eficazmente los elementos de S_p se tiene que $c = (1\ \ 2\ \ 3\ \ ...\ \ p)$.

Ahora, se consideran las permutaciones $\sigma_i = c^i \circ \sigma \circ c^{-i}$, para cada $i \in \{1, \ldots, p-1\}$. Como es un ciclo, el orden de c es su longitud, entonces $c^{m+p} = c^m$ para todo $m \in \mathbb{N}$, luego no cobra sentido considerar potencias de c con exponentes mayores que $p-1$.

Por último, se puede comprobar que $\sigma_i = (i+1 \quad i+2)$, donde se entiende que la trasposición $\sigma_{p-1} = (p\ \ 1)$ ya que $(p \quad p+1) \notin S_p$. Además, las permutaciones σ_i se han generado a partir de la transposición σ y el ciclo τ, luego como el conjunto de transposiciones $(i+1 \quad i+2)$ genera S_p, se tiene que $< \sigma, \tau >= S_p$. □

A parte del lema anterior, será necesario el Teorema de Cauchy sobre teoría de grupos que se enuncia a continuación y cuya demostración parcial puede encontrarse en [15].

Teorema 3.2 (**Cauchy**). *Sea G un grupo finito y p un número primo. Si p divide al cardinal de G, entonces G tiene al menos un elemento de orden p.*

Demostración. Primero se probará el caso abeliano y después se generalizará a cualquier grupo finito. Se procederá por inducción sobre $n = |G|$. El caso base en ambos casos es $n = p$, donde G tiene orden p y del Teorema de clasificación de grupos abelianos finitos 1.3 se obtiene que $G = \mathbb{Z}/p\mathbb{Z}$ y cualquier elemento distinto del neutro cumple la hipótesis. Supóngase que G es abeliano y sea $a \in G$, distinto del elemento neutro. Sea $A = \langle a \rangle$ el subgrupo cíclico que genera a. Si $p \mid |A|$, entonces $a^{|A|/p}$ es un elemento de orden p.
En caso contrario, p no divide $|A|$, y como $|G| = |A|\,[G : A]$ se cumple que $p \mid [G : A]$. Por la hipótesis inductiva, el cociente G/A contiene una clase de orden p; sea xA con $x \in G$ dicha clase y $m = \mathrm{ord}_G(x)$, entonces $(xA)^m = A$, por lo que $p \mid m$, y finalmente $x^{m/p}$ tiene orden p en G. Con esto se concluye el caso abeliano.

Supóngase ahora que G es un grupo no abeliano, entonces se considera el centro de G: $Z(G) = \{g \in G : \forall h \in G, g \cdot h = h \cdot g\}$, que es abeliano para cualquier grupo. Si $p \mid |Z(G)|$ se aplica inmediatamente el apartado anterior. Se supone por último que $p \nmid |Z(G)|$. Entonces, $p \mid |G|$ y G es la unión disjunta de $Z(G)$ y las clases de conjugación de elementos que no están en $Z(G)$. Como $p \mid |G|$ y $|G| = |Z| + \sum_{i=1}^{r} [G : C_G(a_i)]$, si $p \nmid Z|G|$ debe existir un i tal que $[G : C_G(a_i)] = \dfrac{|G|}{|C_G(a_i)|}$ con $p \nmid [G : C_G(a_i)]$ y entonces $p \mid |C_G(a_i)|$, donde $C_G(a_i)$ es un subgrupo de G abeliano, por lo que se aplica el primer apartado para concluir que existe un elemento de orden p. □

Para acabar esta sección se demuestra que dado un primo p, si las raíces de un polinomio de grado p verifican unas ciertas propiedades, entonces su grupo de Galois es S_p.

A diferencia de capítulos anteriores, esta vez no se trata de una prueba constructiva si no que simplemente se demuestra la existencia.

Teorema 3.3 (**Realización de los grupos Simétricos de orden primo**). *Sea $f(X)$ un polinomio irreducible de grado p primo en $\mathbb{Q}[X]$. Si $f(X)$ tiene exactamente dos raíces complejas (no reales), entonces $Gal(f(X)) \cong S_p$.*

Demostración. Sea K el cuerpo de escisión de $f(X)$ y $\alpha \in K$ una raíz de $f(X)$. Por hipótesis, $f(X)$ es irreducible, luego $[\mathbb{Q}(\alpha) : \mathbb{Q}] = deg(f(X)) = p$, y por tanto p divide a $[K : \mathbb{Q}] = |Gal(f(X))|$. Por el Teorema 3.2, $Gal(f(X))$ contiene algún elemento de orden p, sin embargo el Lema 1.31 muestra que los únicos elementos de orden p en S_p son los ciclos de tamaño p.

Como $f(X)$ tiene exactamente dos raíces complejas, estas deben ser conjugadas y existe un automorfismo $\sigma \in Gal(f(X)$ que transforma una en la otra y deja fijas el resto de raíces. Como $\sigma^2 \equiv Id$, entonces es una trasposición.

Por el Teorema 1.28 y su observación posterior, $Gal(f(X)) \subseteq S_p$ y este contiene un ciclo de orden p y una transposición, por el Lema 3.1 se obtiene que

$$Gal(f(X)) \cong S_p. \qquad \square$$

Tras este teorema surge naturalmente la siguiente cuestión, ¿no funcionaría esta demostración para cualquier grupo simétrico? La respuesta es negativa, y el argumento reside en el mencionado Lema 1.31: cualquier elemento de orden p debe ser necesariamente un ciclo de longitud p. Esta propiedad es esencial para asegurar la aparición de un ciclo de tamaño p en el grupo de Galois y, por ende, para concluir que este es S_p.

Sin embargo, cuando n es compuesto este razonamiento deja de ser válido, en S_n pueden existir elementos de orden n que no sean ciclos de longitud n. Se considera en S_6 la permutación $\sigma = (1\ 2\ 3)(4\ 5)$. Como los ciclos $(1\ 2\ 3)$ y $(4\ 5)$ son disjuntos se tiene que $O(\sigma) = \text{mcm}\{2, 3\} = 6$, de manera que σ es una permutación de orden 6 en S_6 pero no es un ciclo de tamaño 6. Esto pone de manifiesto que se requerirán técnicas adicionales para tratar el caso general de S_n.

Como ya es habitual en el estudio del Problema Inverso de Galois, la parte más difícil suele ser encontrar ejemplos concretos que muestren cómo un grupo aparece como grupo de Galois de un polinomio con coeficientes racionales. En particular, el Teorema 3.3 afirma que, para cada primo p, se puede realizar el grupo simétrico S_p como grupo de Galois.

Sin embargo, falta un detalle importante: hay que demostrar que, para cada primo p, existe un polinomio irreducible de grado p con exactamente dos raíces complejas (no reales).

Proposición 3.4. *Sea $p \in \mathbb{N}$ primo, entonces existe un polinomio $f(X) \in \mathbb{Q}[X]$ irreducible, de grado p y con exactamente dos raíces complejas (no reales).*

Demostración. Si $p = 2$ entonces $f(X) = X^2 + 1$ tiene exactamente dos raíces complejas.

Se puede suponer que $p \geq 3$. Se toma $m \in \mathbb{N}$ un número par y $n_1 < n_2 < \cdots < n_{p-2}$ números enteros pares. Se considera ahora el polinomio:

$$g(X) = (X^2 + m)(X - n_1)(X - n_2) \cdots (X - n_{p-2})$$

Bajo estas hipótesis, es evidente que $g(X)$ tiene como raíces reales $n_1, n_2, \ldots, n_{p-2}$, además $g(X)$ no tiene máximos ni mínimos locales en ninguno de esos puntos porque son raíces simples por definición.

Esto último significa que $\varepsilon = \min_{\{x \in \mathbb{R} : g'(x) = 0\}} |g(x)| > 0$, y por tanto se puede escoger $n \in \mathbb{N}$ impar tal que $\varepsilon > \frac{2}{n}$. Ahora se puede tomar el polinomio $f(X) = g(X) - \frac{2}{n}$.

Entonces, $f(X)$ también tendrá exactamente $p-2$ raíces reales, por lo que también tendrá exactamente dos raíces complejas conjugadas (ver Figura 3.1).

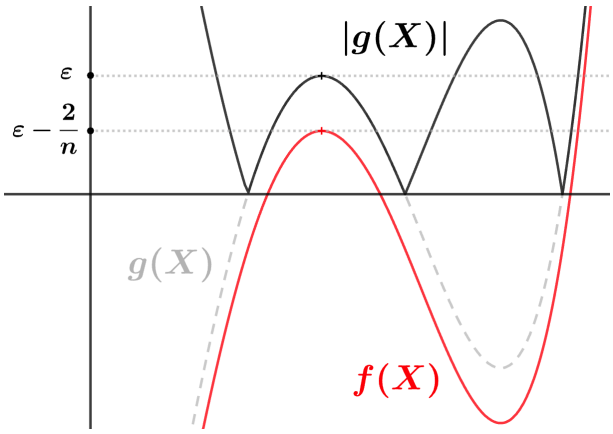


Figura 3.1: El polinomio $g(X)$ tiene como raíces reales $n_1, n_2, \ldots, n_{p-2}$.

El punto clave de la demostración viene a continuación, si se considera

$$nf(X) = nX^p + a_{p-1}X^{p-1} + \cdots + a_0,$$

se tiene que los coeficientes de $nf(X)$ son los mismos que los de $g(X)$ (salvo el de mayor grado y el término independiente) y estos son pares porque son los polinomios simétricos elementales sobre los n_i, además n es impar y $a_0 = -nmn_1 \cdots n_{p-2} - 2$ no es divisible por 2^2. Por el Criterio de Eisenstein 1.34 para $p = 2$, se obtiene que $nf(X)$ es irreducible y por tanto, también $f(X)$. □

Este método es la pieza que faltaba en el puzzle y complementa al Teorema 3.3, luego ya se disponen de los conocimientos necesarios para calcular polinomios cuyos grupos de Galois son los grupos simétricos de orden primo.

Ejemplo 3.5. A continuación se encuentra $f(X) \in \mathbb{Q}[X]$ cuyo grupo de Galois es S_5.

En primer lugar, a partir de la Proposición 3.4, tomando $m = 2, n_1 = -2, n_2 = 0$ y $n_3 = 2$ se considera el polinomio

$$g(X) = (X^2 + 2)(X + 2)X(X - 2) = X^5 - 2X^3 - 8X.$$

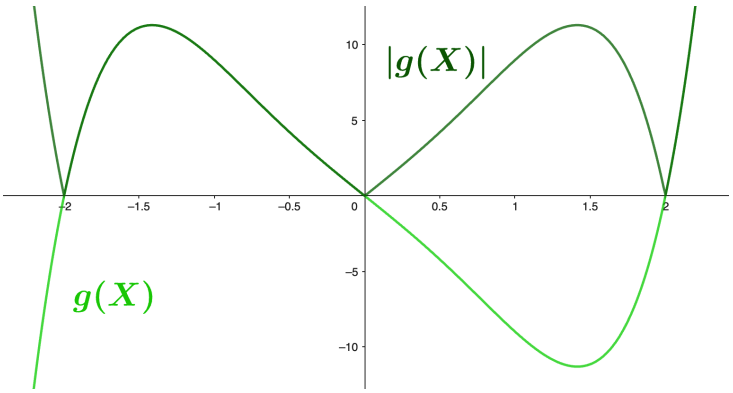


Figura 3.2: El polinomio $g(X)$ tiene como raíces reales $-2, 0$ y 2.

El siguiente paso es hallar los puntos donde se anula $g'(X) = 5X^4 - 6X^2 - 8$.

Realizando el cambio de variable $T = X^2$ se obtiene la ecuación $5T^2 - 6T - 8 = 0$, cuyas raíces son $T_1 = 2, T_2 = -\frac{4}{5}$,

Deshaciendo el cambio de variable únicamente se obtienen las soluciones reales

$$X_1 = \sqrt{2}, X_2 = -\sqrt{2}.$$

Además se tiene que $|g(\sqrt{2})| = |g(-\sqrt{2})| \approx 11{,}31$. Y por tanto

$$\varepsilon = \min_{\{x \in \mathbb{R} \,:\, g'(x) = 0\}} |g(x)| \approx 11{,}31,$$

y que un n impar tal que $\varepsilon > \frac{2}{n}$ puede ser por ejemplo $n = 1$. Por último se considera

$$f(X) = g(X) - \frac{2}{n} = X^5 - 2X^3 - 8X - 2$$

el cual además de tener exactamente dos raíces no reales, es irreducible por el Criterio de Eisenstein 1.34 para el primo $p = 2$. Luego finalmente por el Teorema 3.3 se obtiene que:

$$Gal(f(X)) \cong S_5.$$

Aunque para el caso anterior no se han necesitado más herramientas que lápiz y papel, es evidente que para primos más grandes el grado y la dificultad de los polinomios aumenta acorde a este. Es por eso que para casos más complejos, se pueden utilizar software de cálculo para hallar los extremos relativos del polinomio:

Ejemplo 3.6. A continuación se encuentra $f(X) \in \mathbb{Q}[X]$ cuyo grupo de Galois es S_{11}. Análogamente al ejemplo anterior, se considera el polinomio:

$$\begin{aligned} g(X) &= (X^2+2)(X-8)(X-6)(X-4)(X-2)X(X+2)(X+4)(X+6)(X+8) \\ &= X^{11} - 118X^9 + 4128X^7 - 43744X^5 + 42496X^3 + 294912X \end{aligned}$$

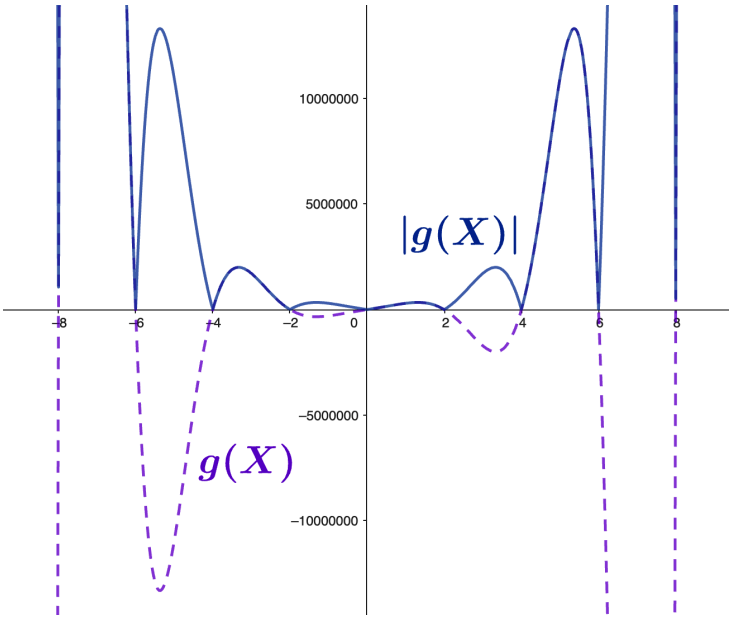


Figura 3.3: El polinomio $g(X)$ tiene exactamente 9 raíces reales.

Se aprecia en la gráfica de $|g(X)|$ y se constata con el software WolframAlpha que:

$$\varepsilon = \min_{\{x \in \mathbb{R} \,:\, g'(x)=0\}} |g(x)| \approx |g(1{,}32)| \approx 339137.$$

Por lo que un n impar tal que $\varepsilon > \dfrac{2}{n}$ puede ser $n = 1$. Por último se considera

$$f(X) = g(X) - \frac{2}{n} = X^{11} - 118X^9 + 4128X^7 - 43744X^5 + 42496X^3 + 294912X - 2,$$

el cual además de tener exactamente dos raíces no reales, es irreducible por el Criterio de Eisenstein 1.34 para el primo $p = 2$. Luego finalmente por el Teorema 3.3 se obtiene que

$$Gal(p(X)) \cong S_{11}.$$

3.2. Grupos Simétricos.

La realización de S_p (con p primo) como grupo de Galois aprovecha propiedades específicas de los primos que no se generalizan, en general, a grados compuestos. En contraste con la factorización de enteros, donde conocer la descomposición de enteros en primos permite manejar cualquier número natural mediante sus factores, la realización de S_n exige técnicas adicionales que no surgen de la mera combinación de casos primos. Para llevarla a cabo serán necesarios únicamente tres resultados previos. El primero es el Teorema de Dedekind, cuya prueba [4] no se incluye por su extensión. Es una herramienta fundamental que muestra cómo son ciertas permutaciones del grupo de Galois de un polinomio $f(X) \in \mathbb{Z}[X]$ con coeficientes enteros a través de su factorización módulo un único primo.

Teorema 3.7 (Dedekind). *Sea $f(X) \in \mathbb{Z}[X]$ un polinomio de grado n mónico y sin raíces múltiples. Sea $p \in \mathbb{N}$ primo tal que $f(X)$ se puede descomponer en $\mathbb{F}_p[X]$ como*

$$\tilde{f}(X) \equiv \tilde{f}_1(X)\tilde{f}_2(X)\cdots\tilde{f}_k(X) \in \mathbb{F}_p[X]$$

donde $\tilde{f}_1(X), \tilde{f}_2(X), \ldots, \tilde{f}_k(X)$ son mónicos e irreducibles. Sea d_i el grado de cada polinomio $\tilde{f}_i(X)$, entonces se cumple que el grupo de Galois de $f(X)$ sobre $\mathbb{Q}$, entendido como un subgrupo de S_n, contiene un elemento que es producto de ciclos disjuntos de la forma

$$\sigma_1 \circ \sigma_2 \circ \cdots \circ \sigma_k$$

donde cada σ_i es un ciclo de orden d_i en S_n.

Igual que para los grupos simétricos de orden primo, para el caso general se necesita garantizar la existencia de ciertos tipos de polinomios usados en el Teorema de realización.

Lema 3.8. *Sea $p \in \mathbb{N}$ primo, entonces para todo $n \in \mathbb{N}$ existe un polinomio mónico e irreducible de grado n en $\mathbb{F}_p[X]$.*

Demostración. Sea $p \in \mathbb{N}$ un primo, se probará por inducción sobre n:

Sea $n = 1$, es trivial que cualquier polinomio mónico de grado 1 en $\mathbb{F}_p[X]$ es irreducible.

Se supone que el resultado es cierto para todos los números naturales hasta n.

Se considera el polinomio $f(X) = X^{p^n} - X \in \mathbb{F}_p[X]$. Sea L el cuerpo de escisión de $f(X)$ en $\mathbb{F}_p[X]$, y R el conjunto de raíces de $f(X)$ en L.

Se observa que la derivada formal es $f'(X) \equiv p^n X^{p^n-1} - 1 \equiv -1$, por lo que $f'(X)$ no tiene raíces y por la Proposición 1.9, $f(X)$ no tiene raíces múltiples. Esto último indica que $|R| = \deg(f(X)) = p^n$.

Además se tiene que R puede ser dotado de estructura de cuerpo:

I) Como $f(0) = f(1) = 0$ se tiene que $0, 1 \in R$.

II) Es evidente que $a \in R$ si y solo si $f(a) = a^{p^n} - a$, o equivalentemente $a^{p^n} = a$. Luego si $a, b \in R$, $(ab)^{p^n} = a^{p^n} b^{p^n} = ab$ y por tanto $ab \in R$.

III) Dado $a \in R \setminus \{0\}$ se tiene que $(a^{-1})^{p^n} = a^{-p^n} = (a^{p^n})^{-1} = a^{-1}$, luego $a^{-1} \in R$.

IV) Dados $a, b \in R$ se tiene que, $(a+b)^p \equiv a^p + b^p$ mód p, luego concretamente: $(a+b)^{p^n} \equiv (a^p + b^p)^{p^{n-1}} \equiv (a^{p^2} + b^{p^2})^{p^{n-2}} \equiv \cdots \equiv a^{p^n} + b^{p^n} \equiv a + b$ mód p. Entonces se tiene que $a + b \in R$

En conclusión, R es un cuerpo que contiene todas las raíces de $f(X)$, por lo que este debe ser un cuerpo de escisión en $\mathbb{F}_p[X]$, por tanto $R = L$. Además, el grupo multiplicativo de cualquier cuerpo finito es cíclico, por lo que en concreto se tiene $L^* = \langle \alpha \rangle$ para algún $\alpha \in L$. Se ve que $L = \mathbb{F}_p(\alpha)$ y finalmente, el polinomio mínimo de α en $\mathbb{F}_p$ es irreducible y de grado $[L : \mathbb{F}_p] = n$. □

Teorema 3.9 (**Realización de los grupos Simétricos**). *Sea $n \in \mathbb{N}$, entonces existe una extensión de Galois $K/\mathbb{Q}$ tal que $Gal(K/\mathbb{Q}) \cong S_n$.*

Demostración. Si $n = 3$, entonces se puede comprobar que $Gal(X^3 - 2) \cong S_3$.
Si $n > 3$, en virtud del Lema 3.8 se escogen los siguientes polinomios:

$f_1(X) \in \mathbb{F}_2[X]$ irreducible y mónico de grado n.

$f_2(X) \equiv g_1(X)g_2(X) \in \mathbb{F}_3[X]$, con $g_1(X), g_2(X)$ irreducibles y mónicos de grados $n-1$ y 1, respectivamente.

$f_3(X) \equiv h_1(X)h_2(X) \in \mathbb{F}_5[X]$ con $h_1(X), h_2(X)$ irreducibles y mónicos de grados 2 y $n-2$, respectivamente. (si n es impar)
$f_3(X) \equiv h_1(X)h_2(X)h_3(X) \in \mathbb{F}_5[X]$ con $h_1(X), h_2(X), h_3(X)$ irreducibles y mónicos de grados $2, n-3$ y 1, respectivamente. (si n es par)

A continuación se escoge $f(X)$ de manera que:

$$f(X) \equiv f_1(X) \text{ mód } 2.$$
$$f(X) \equiv f_2(X) \text{ mód } 3.$$
$$f(X) \equiv f_3(X) \text{ mód } 5.$$

Se puede tomar, por ejemplo $f(X) = -15f_1(X) + 10f_2(X) + 6f_3(X) \in \mathbb{Z}[X]$. De manera que, además de cumplir los requisitos de reducción a los respectivos cuerpos $\mathbb{F}_p[X]$, se tiene que $f(X)$ es mónico. Sea $G = Gal(f(X))$ el grupo de Galois de $f(X)$ sobre $\mathbb{Q}$, se demuestra a continuación que $G \cong S_n$.

Como $f(X) \equiv f_1(X)$ mód 2, y este es irreducible en $\mathbb{F}_2[X]$, por el Criterio de Irreducibilidad 1.32 de reducción módulo $p = 2$, $f(X)$ es irreducible sobre $\mathbb{Q}[X]$.

Además, $f(X) \equiv f_2(X) \equiv g_1(X)g_2(X)$ mód 3. Como $g_1(X)$ no tiene raíces múltiples, es irreducible y no tiene raíces en común con $g_2(X)$; $f(X)$ tampoco tiene raíces múltiples en $\mathbb{F}_3[X]$. Bajo estas hipótesis se puede aplicar el Teorema 3.7, del que se obtiene que G contiene un ciclo de tamaño $n-1$. Aplicando este mismo Teorema en $\mathbb{F}_5[X]$, G posee:

Si n es impar, una permutación $\sigma_1 \circ \sigma_2$, donde σ_1 tiene orden $n-2$ y σ_2 es una trasposición.
Si n es par, una permutación $\sigma_3 \circ \sigma_4$, donde σ_3 tiene orden $n-3$ y σ_4 es una trasposición.

De esta forma, elevando ambas permutaciones a un exponente impar idóneo, $n-2$ ó $n-3$ en respectivos casos, se concluye que G contiene una trasposición.

Supóngase, sin pérdida de generalidad, que G contiene los ciclos $(1\ 2\ \cdots\ n-1)$ y $(i\ j)$. Ahora se demuestra que en G aparece alguna transposición de la forma $(k\ n)$ para algún $k < n$. Además, se supone que $i < j < n$ y se define $s = n - j$. Se observa que $(1\ 2\ \cdots\ n-1)(i\ j)(1\ 2\ \cdots\ n-1)^{-1} = (i+1 \quad j+1)$, y al repetir esta operación s veces se obtiene $(i+s \quad n) \in G$.

Además, al aplicar el ciclo $(1\ 2\ \cdots\ n-1)$ sobre la trasposición $(i\ n)$ se consigue $(i+1 \quad n)$, y al aplicar la permutación inversa se consigue $(i-1 \quad n)$. En consecuencia, para todo $i \in \{1, 2, \ldots, n-1\}$ se cumple $(i\ n) \in G$. Dado que $(i\ j) = (i\ n)(j\ n)(i\ n)$, toda trasposición pertenece a G, y por ser las trasposiciones generadoras de S_n se tiene

$$G \cong S_n \qquad \square$$

Aunque el Teorema 3.9 solo requiera de la existencia de polinomios mónicos e irreducibles de grado arbitrario, que se garantiza por el Lema 3.8. Es cierto que en la práctica se utilizan métodos más simples. El siguiente resultado caracteriza estos polinomios irreducibles:

Teorema 3.10. *Sea $n \in \mathbb{N}$ y $\mathbb{F}_p$ el cuerpo finito de orden p. Entonces el polinomio*

$$p_n(X) = X^{p^n} - X \in \mathbb{F}_p[X]$$

es el producto de todo polinomio mónico e irreducible en $\mathbb{F}_p[X]$ cuyo grado divida a n.

Ejemplo 3.11. Del teorema anterior se deduce que es posible determinar todos los polinomios mónicos e irreducibles de cierto grado n sobre cualquier cuerpo finito $\mathbb{F}_p$, sencillamente se necesita factorizar $p(X) = X^{p^n} - X \in \mathbb{F}_p[X]$.

Sin embargo, en la práctica, para evitar tener que factorizar polinomios se determinarán los polinomios irreducibles necesarios directamente por ensayo y error.

En principio, se podría pensar que la comprobación pertinente para determinar si un polinomio $f(X) \in \mathbb{F}_p[X]$ de grado n es irreducible es, efectivamente, comprobar si es factor de $X^{p^n} - X$; este argumento es falso puesto que podría darse el caso que $f(X)$ sea el producto de dos o más polinomios irreducibles cuyos grados dividan a n.

En $\mathbb{F}_2[X]$, el polinomio $g(X) = X^{10} + X^8 + X^7 + X^5 + X^3 + X^2 + 1$ divide a $X^{2^{10}} - X$, pero no porque sea irreducible, sino porque se puede factorizar como

$$g(X) \equiv (X^5 + X^2 + 1)(X^5 + X^3 + 1),$$

donde cualquiera de estos dos polinomios es irreducible y de un grado divisor de 10.

Entonces, si esto no funciona, ¿cómo es posible garantizar la irreducibilidad? Para usar un argumento parecido al anterior es menester "eliminar" del polinomio $X^{p^n} - X$ los polinomios irreducibles de grado menor que n.

Los polinomios irreducibles de grado 1 en $\mathbb{F}_2[X]$ tendrán como producto $p_1(X) = X^2 - X$; los de grado 2, $p_2(X) = \dfrac{X^{2^2} - X}{p_1(X)}$; los de grado 5, $p_5(X) = \dfrac{X^{2^5} - X}{p_1(X)}$.

En definitiva, los polinomios irreducibles de grado 10 en $\mathbb{F}_2[X]$ tendrán como producto $p_{10}(X) = \dfrac{X^{2^{10}} - X}{p_1(X) \cdot p_2(X) \cdot p_5(X)}$, luego para saber si un polinomio $f(X)$ de grado 10 es irreducible bastará ver si $mcd(f(X), p_{10}(X))$ es de grado 10.

Ejemplo 3.12. A continuación se encuentra $p(X) \in \mathbb{Q}[X]$ cuyo grupo de Galois es S_8.

Se aprovecha que el Teorema 3.9 proporciona una prueba constructiva y se escogen los siguientes polinomios, todos mónicos e irreducibles sobre los respectivos cuerpos finitos que se indican.

$\mathbb{F}_2[X]$	—	$f_1(X) = X^8 + X^4 + X^3 + X + 1$
$\mathbb{F}_3[X]$	$g_1(X) = X^7 + X^2 + 2$ $g_2(X) = X$	$f_2(X) = X^8 + X^3 + 2X$
$\mathbb{F}_5[X]$	$h_1(X) = X^2 + 2$ $h_2(X) = X^5 + X^2 + 2$ $h_3(X) = X$	$f_3(X) = X^8 + 2X^6 + X^5 + 4X^3 + 4X$

Cuadro 3.1: Polinomios en $\mathbb{F}_2[X]$, $\mathbb{F}_3[X]$ y $\mathbb{F}_5[X]$.

En consecuencia, si se toma el polinomio

$$f(X) = -15f_1(X) + 10f_2(X) + 6f_3(X) = X^8 + 12X^6 + 6X^5 - 15X^4 + 19X^3 + 29X - 15,$$

se concluye que

$$Gal(f(X)) \cong S_8.$$

De la misma forma se pueden construir más ejemplos de grupos simétricos:

Ejemplo 3.13. A continuación se encuentra $p(X) \in \mathbb{Q}[X]$ cuyo grupo de Galois es S_{10}.

Análogamente al ejemplo anterior, se escogen los siguientes polinomios, todos mónicos e irreducibles sobre los respectivos cuerpos finitos que se indican.

$\mathbb{F}_2[X]$	—	$f_1(X) = X^{10} + X^3 + 1$
$\mathbb{F}_3[X]$	$g_1(X) = X^9 + X^4 + 2$ $g_2(X) = X$	$f_2(X) = X^{10} + X^5 + 2X$
$\mathbb{F}_5[X]$	$h_1(X) = X^2 + 2$ $h_2(X) = X^7 + X + 1$ $h_3(X) = X$	$f_3(X) = X^{10} + 2X^8 + X^4 + X^3 + 2X^2 + 2X$

Cuadro 3.2: Polinomios en $\mathbb{F}_2[X]$, $\mathbb{F}_3[X]$ y $\mathbb{F}_5[X]$.

En consecuencia, si se toma el polinomio

$$f(X) = -15f_1(X)+10f_2(X)+6f_3(X) = X^{10}+12X^8+10X^5+6X^4-9X^3+12X^2+32X-15,$$

se concluye que

$$Gal(f(X)) \cong S_{10}.$$

Sin embargo, el argumento de van der Waerden cambia ligeramente si n es impar:

Ejemplo 3.14. A continuación se encuentra $p(X) \in \mathbb{Q}[X]$ cuyo grupo de Galois es S_{15}.

Se escogen los siguientes polinomios, todos mónicos e irreducibles sobre los respectivos cuerpos finitos que se indican, la única diferencia con los ejemplos anteriores es en el cálculo de $f_2(X)$, en este caso $n = 15$ es impar y solo se construye mediante dos polinomios.

$\mathbb{F}_2[X]$	—	$f_1(X) = X^{15} + X + 1$
$\mathbb{F}_3[X]$	$g_1(X) = X^{14} + X + 2$ $g_2(X) = X$	$f_2(X) = X^{15} + X^2 + 2X$
$\mathbb{F}_5[X]$	$h_1(X) = X^2 + 2$ $h_2(X) = X^{13} + X^4 + X^2 + 1$	$f_3(X) = X^{15} + 2X^{13} + X^6$ $+ 3X^4 + 3X^2 + 2$

Cuadro 3.3: Polinomios en $\mathbb{F}_2[X]$, $\mathbb{F}_3[X]$ y $\mathbb{F}_5[X]$.

En consecuencia, si se toma el polinomio

$$f(X) = -15f_1(X) + 10f_2(X) + 6f_3(X) = X^{15} + 12X^{13} + 6X^6 + 18X^4 + 28X^2 + 5X - 3,$$

se concluye que

$$Gal(f(X)) \cong S_{15}.$$

Capítulo 4

Realización del grupo Alternado A_n.

Habiendo completado en el capítulo anterior la construcción de polinomios en $\mathbb{Q}[x]$ con grupo de Galois S_n, resulta natural plantear a continuación la realización de su subgrupo alternado A_n. Sería suficiente un teorema que garantizara la realizabilidad de todo subgrupo de S_n, ya que junto al Teorema de Cayley, que enuncia que cualquier grupo finito es subgrupo de un simétrico, permitiría resolver el Problema Inverso de Galois. Por ello, el estudio de A_n requiere un enfoque distinto, basado en el análisis del discriminante de los polinomios y en el uso del Teorema de Irreducibilidad de Hilbert, un hito fundamental en el Problema Inverso de Galois, que permite extraer infinitas especializaciones en $\mathbb{Q}$ manteniendo el grupo de Galois dentro de A_n. En este capítulo se expondrán dichos métodos y construirán familias explícitas de polinomios cuyo grupo de Galois sea isomorfo a A_n.

4.1. Grupos Alternados.

Una herramienta básica es el discriminante de un polinomio, se define a continuación.

Definición 4.1. Sea $f(X) \in \mathbb{Q}[X]$ un polinomio no constante de grado n. Se considera $f(X) = c(X-\alpha_1)\cdots(X-\alpha_n)$ su factorización sobre un cuerpo de escisión, donde los α_i no son necesariamente distintos. Se define el *discriminante* de $f(X)$ como

$$\Delta(f) = \prod_{i<j}(\alpha_j - \alpha_i)^2$$

Esta definición omite el coeficiente líder de $f(X)$ y depende solo de sus raíces. Por ejemplo, X^2+3 y $2X^2+6$ tendrían el mismo discriminante, 12. La siguiente proposición sobre el discriminante de un cierto trinomio ha sido obtenida de la sección 2.8 de [20], resultará útil para asegurar que el grupo de Galois de ciertos polinomios es A_n, y no S_n.

Proposición 4.2. *Sea $f(X) = X^n + aX + b \in K[X]$ entonces se tiene que*

$$\Delta(f) = (-1)^{\frac{n(n-1)}{2}}(n^n b^{n-1} + (-1)^{n-1}(n-1)^{n-1}a^n).$$

El siguiente Teorema [2] es un resultado central en el capítulo, este caracteriza mediante el discriminante los polinomios cuyo grupo de Galois es un subgrupo del grupo alternado.

Teorema 4.3. *Sea $f(X) \in K[X]$ un polinomio de grado n sin raíces múltiples en un cuerpo de escisión L. Entonces el grupo de Galois de $f(X)$ es un subgrupo de A_n sí y solo sí su discriminante es un cuadrado perfecto en K, esto es, $\Delta(f) = \delta^2$, con $\delta \in K$.*

Demostración. Sean $\alpha_1, \ldots, \alpha_n$ las raíces de $f(X)$ en el cuerpo de escisión $L = K(\alpha_1, \ldots, \alpha_n)$. Se considera ahora $\delta = \prod_{i<j}(\alpha_j - \alpha_i)$, que no es nulo, pues $f(X)$ no tiene raíces múltiples. Entonces $\delta^2 = \Delta(f)$ y este será un cuadrado perfecto en K sí y solo sí $\delta \in K$.

Sea $\sigma \in Gal(L/K)$, entonces se tiene que

$$\sigma(\delta) = \prod_{i<j}(\sigma(\alpha_j) - \sigma(\alpha_i)) = \epsilon(\sigma)\prod_{i<j}(\alpha_j - \alpha_i) = \epsilon(\sigma)\delta,$$

donde $\epsilon(\sigma)$ es la signatura de σ.

Se observa que σ pertenece a A_n exactamente cuando es par, es decir, cuando $\epsilon(\sigma) = 1$, lo cual a su vez equivale a que $\sigma(\delta) = \delta$. Por tanto, el grupo de Galois será un subgrupo de A_n sí y solo sí $Gal(L/K)$ fija δ, lo que implica que δ pertenece al cuerpo base K. □

La siguiente proposición [3] es crucial para la realización de los grupos alternados, esta caracteriza los subgrupos transitivos de S_n mediante la longitud de ciertos ciclos.

Proposición 4.4. *Sea $n \geq 3$, entonces un subgrupo transitivo de S_n que contiene un ciclo de longitud 3 y un ciclo de longitud q para algún primo $q > \frac{n}{2}$, es bien S_n o bien A_n.*

Finalmente, se puede enunciar un Teorema de realización de los grupos Alternados. Aunque se recopilan los lemas anteriores en diversos documentos sobre el problema inverso de Galois para grupos Alternados, esta estructura no está materializada en ninguno de ellos.

Teorema 4.5 (Realización de los grupos Alternados). *Sea $f(X) \in \mathbb{Q}[X]$ un polinomio irreducible de grado $n \geq 3$ sin raíces múltiples, con $\Delta(f)$ cuadrado perfecto en $\mathbb{Q}$. Si el grupo de Galois de $f(X)$ contiene un ciclo de longitud 3 y un ciclo de longitud q para algún primo $q > \frac{n}{2}$, entonces $Gal(f(X)) \cong A_n$.*

Demostración. Sea $G = Gal(f(X))$. Por hipótesis, $f(X)$ es irreducible en $\mathbb{Q}[X]$ y no tiene raíces múltiples, luego por el Teorema 1.28, G es un subgrupo transitivo de S_n. Además, G contiene un ciclo de longitud 3 y un ciclo de longitud q para algún primo $q > \frac{n}{2}$, entonces por la Proposición 4.4, bien $G \cong S_n$ o bien $G \cong A_n$. Sin embargo, su discriminante es un cuadrado perfecto en $\mathbb{Q}$, luego por el Teorema 4.3, G es un subgrupo de A_n. Como $S_n \not\subseteq A_n$ se concluye que $G \cong A_n$. □

La base teórica que garantiza la existencia de polinomios capaces de satisfacer las hipótesis del enunciado se desarrollará en la siguiente sección. Mientras tanto, con las herramientas adquiridas hasta ahora, la estrategia práctica consiste en ensayar distintos candidatos y verificar que cumplan todas las premisas del teorema.

Ejemplo 4.6. A continuación se encuentra un polinomio cuyo grupo de Galois es A_8. Primero, se considera el polinomio $g(X) = X^8 + 2X + 2$ y se comprueba si su grupo de Galois es, efectivamente, A_8.

- Aplicando el Criterio de Eisenstein 1.34 para el primo $p = 2$ se obtiene que el polinomio $g(X)$ es irreducible en $\mathbb{Q}[X]$.
- Además, si se considera la reducción en factores irreducibles módulo 3 de $g(X)$,

$$g(X) \equiv (X^3 + X^2 + 2X + 1)(X^5 + 2X^4 + 2X^3 + 2X^2 + X + 2) \text{ mód } 3.$$

  Por el Teorema de Dedekind 3.7, existe una permutación $\sigma \in Gal(g(X))$, de la forma $\sigma = \sigma_1 \circ \sigma_2$ tal que $\text{ord}(\sigma_1) = 3$ y $\text{ord}(\sigma_2) = 5$. Así, $\sigma^5, \sigma^3 \in Gal(g(X))$ y estos serán ciclos de longitud 3 y $5 > \frac{8}{2}$, respectivamente.

Bajo estas hipótesis, se podría pensar que por el Teorema 4.5 se tiene $Gal(g(X)) \cong A_8$. Sin embargo se omite una hipótesis crucial.

- Si se calcula el discriminante de $g(X)$ como en la Proposición 4.2, se obtiene que

$$\sqrt{\Delta(g)} = \sqrt{1936656640} \notin \mathbb{Q}.$$

De manera que no es posible aplicar el Teorema 4.5. De hecho, si se considera la reducción en factores irreducibles módulo 11 se tiene que

$$g(X) \equiv (X^2 + 5X + 2)(X^3 + X^2 + 3X + 2)(X^3 + 5X^2 + 4X + 6) \text{ mód } 11.$$

Además, la reducción en factores irreducibles módulo 41 es

$$g(X) \equiv (X + 6)(X^7 + 35X^6 + 36X^5 + 30X^4 + 25X^3 + 14X^2 + 39X + 14) \text{ mód } 41.$$

Por el Teorema de Dedekind 3.7, existen permutaciones $\sigma, \tau \in Gal(g(X))$ de manera que τ es un ciclo de longitud 7 y σ^3 es una trasposición, entonces por un argumento análogo al de la demostración del Teorema 3.9, se puede concluir que

$$Gal(g(X)) \cong S_8.$$

Por el contrario, se considera $f(X) = 8X^8 - 8X + 7$, el cual es irreducible en $\mathbb{Q}[X]$. Aplicando la fórmula de la Proposición 4.2 al polinomio $h(X) = \dfrac{f(X)}{8}$, se obtiene que $\Delta(f) = \Delta(h) = 5764801 = 2401^2$, es un cuadrado perfecto en $\mathbb{Q}$.

Por último, si se consideran sus factores irreducibles módulo 3,

$$f(X) \equiv (X^3 + X^2 + 2X + 1)(X^5 + 2X^4 + 2X^3 + 2X^2 + X + 2) \text{ mód } 3.$$

Por el Teorema de Dedekind 3.7, existe una permutación $\sigma \in Gal(f(X))$, de la forma $\sigma = \sigma_1 \circ \sigma_2$ tal que $\text{ord}(\sigma_1) = 3$ y $\text{ord}(\sigma_2) = 5$. Así, $\sigma^5, \sigma^3 \in Gal(f(X))$ serán ciclos de longitud 3 y $5 > \dfrac{8}{2}$, respectivamente. En virtud del Teorema 4.5, se obtiene que

$$Gal(f(X)) \cong A_8.$$

Ejemplo 4.7. A continuación se encuentra $f(X) \in \mathbb{Q}[X]$ cuyo grupo de Galois es A_{19}. Se considera el polinomio $f(X) = X^{19} - 380X + 360$, se demostrará que cumple todas las hipótesis del Teorema 4.5.

- Aplicando el Criterio de Eisenstein 1.34 para $p = 5$ se obtiene que el polinomio $f(X)$ es irreducible en $\mathbb{Q}[X]$. Se verifica que $5 \mid 360$, $5 \mid 380$, $5 \nmid 1$ y además $25 \nmid 360$.

- Se utiliza la Proposición 4.2 para hallar el discriminante de $f(X)$, se observa que es un cuadrado perfecto en $\mathbb{Q}$, concretamente se tiene que

  $$\Delta(f) = (62267082347345700053031321 6 \cdot 10^9)^2.$$

- Se considera la reducción en factores irreducibles módulo 29 de $f(X)$

  $f(X) \equiv (X^2+6X+21)(X^3+14X^2+18X+26)(X^{14}+9X^{13}+16X^{12}+X^{11}+6X^{10}+27X^9+3X^8+6X^7+10X^6+7X^5+18X^4+10X^3+10X^2+25X+15)$ mód 29.

  Por el Teorema de Dedekind 3.7, existe una permutación $\sigma \in Gal(f(X))$ cuya descomposición en ciclos disjuntos es de la forma $\sigma = \sigma_1 \circ \sigma_2 \circ \sigma_3$, donde $\text{ord}(\sigma_1) = 2$, $\text{ord}(\sigma_2) = 3$ y $\text{ord}(\sigma_3) = 14$. De manera que $\sigma^{14} = \sigma_2^2 \in Gal(f(X))$ y este será un ciclo de longitud 3.

- Se considera ahora la reducción en factores irreducibles módulo 41 de $f(X)$,

  $f(X) \equiv (X+31)(X+35)(X^{17}+16X^{16}+32X^{15}+3X^{14}+14X^{13}+3X^{12}+28X^{11}+22X^{10}+25X^9+23X^8+16X^7+24X^6+39X^5+4X^4+20X^3+39X^2+39X+6)$ mód 41.

  De nuevo, por el Teorema de Dedekind 3.7, existe un ciclo $\tau \in Gal(f(X))$ de longitud $q = 17$, el cual es un número primo mayor que $\dfrac{19}{2}$.

Por el Teorema 4.5 de realización de los grupos alternados, se concluye que

$$Gal(f(X)) \cong A_{19}.$$

4.2. Teorema de Irreducibilidad de Hilbert.

Esta elección de polinomios en los ejemplos anteriores puede parecer arbitraria, sin embargo se encuentra oculto, en realidad, un método sistemático detallado [14, 16] que garantiza la existencia de infinidad de polinomios con grupo de Galois A_n para cada n. El siguiente resultado es una piedra angular en el problema inverso de Galois para grupos alternados, se le atribuye a Hilbert y se presenta aquí sin demostración, dado que su complejidad técnica excede al alcance de este trabajo. Esta demostración se puede encontrar en [11].

Teorema 4.8 (**Irreducibilidad de Hilbert**). *Sea $f(T_1, \ldots, T_n, X) \in \mathbb{Q}(T_1, \ldots, T_n)[X]$ un polinomio irreducible. Entonces existen infinitas n-tuplas $(a_1, \ldots, a_n) \in \mathbb{Q}^n$ tales que la especialización $f_a(X) = f(a_1, \ldots, a_n, X) \in \mathbb{Q}[X]$ está bien definida y es irreducible, y además se cumple que:* $\mathrm{Gal}_{\mathbb{Q}(T_1,\ldots,T_n)}(f(T_1, \ldots, T_n, X)) \cong \mathrm{Gal}_{\mathbb{Q}}(f_a(X))$.

Donde $\mathbb{Q}(T_1, \ldots, T_n)$ denota el cuerpo de fracciones del anillo de polinomios en las indeterminadas $T_1, \ldots, T_n$; es decir, $\mathbb{Q}[T_1, \ldots, T_n]$. Para la realización de A_n, se parte de una familia de polinomios con grupo de Galois S_n sobre $\mathbb{Q}(t)$. Se debe destacar que este teorema no desacredita de ninguna manera la construcción del Capítulo 3 ya que el marco teórico usado ahí era sustancialmente más simple que el que se usa ahora.

Teorema 4.9. *Se considera $f(t, X) = X^n - ntX + (n-1)t \in \mathbb{Q}(t)[X]$. Entonces el grupo de Galois de $f(X, t)$ sobre $\mathbb{Q}(t)$ es isomorfo a S_n. En particular, existen infinitos $t \in \mathbb{Q}$ tal que $f(X, t) \in \mathbb{Q}[X]$ es irreducible y tiene grupo de Galois S_n.*

Por último, se introduce un cambio de variable adecuado que fuerza el discriminante a ser un cuadrado en $\mathbb{Q}$, y entonces el grupo de Galois de la extensión será A_n. Se aplica el Teorema de Irreducibilidad de Hilbert para especializar t en infinitos valores racionales. Entonces quedará demostrado que no solo existen ejemplos aislados, sino una familia infinita de polinomios en $\mathbb{Q}[x]$ cuyo grupo de Galois es isomorfo a A_n.

Teorema 4.10. *Sea $f(t, X) = X^n - ntX + (n-1)t \in \mathbb{Q}(t)[X]$. Se considera el cambio*

$$t = \begin{cases} 1 - (-1)^{\frac{n(n-1)}{2}} nu^2, & \text{si } n \text{ es impar.} \\ \dfrac{1}{1 + (-1)^{\frac{n(n-1)}{2}} (n-1)u^2}, & \text{si } n \text{ es par.} \end{cases}$$

Entonces el grupo de Galois de $f(u, X)$ sobre $\mathbb{Q}(u)$ es A_n. En particular, por el Teorema de Irreducibilidad de Hilbert, existen infinitos $a \in \mathbb{Q}$ tales que $Gal(f(a, X)) \cong A_n$.

En efecto, los mencionados polinomios de los Ejemplos 4.6, 4.7 fueron obtenidos como especializaciones del tipo $f(1, X)$ en el contexto del último teorema. Aunque dicho resultado no asegure que toda especialización lo satisfaga, permite justificar que, al probar ejemplos concretos, algunos cumplan las condiciones para tener grupo de Galois A_n.

Capítulo 5

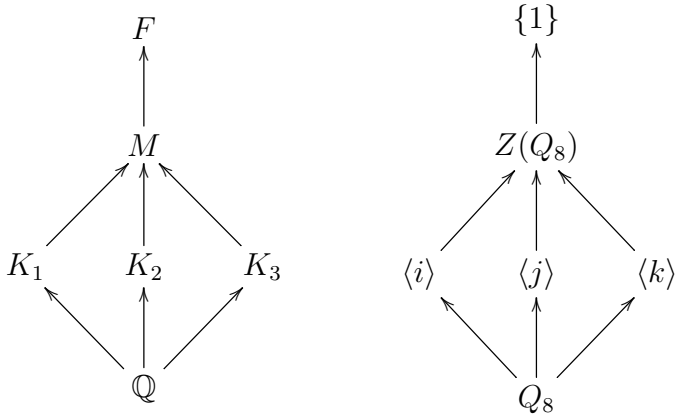
Realización del grupo de los Cuaterniones Q_8.

Un caso particularmente interesante en la Teoría de Galois inversa es el grupo de los cuaterniones: $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$, es un grupo no abeliano que se define mediante las relaciones $i^2 = j^2 = k^2 = ijk = -1$.

Su centro es $Z(Q_8) = \{g \in Q_8 : \forall h \in Q_8,\ gh = hg\}$, donde basta observar que $ij = -ji$ y $ik = -ki$ para ver que $Z(Q_8) = \{\pm 1\}$. Además, posee tres subgrupos cíclicos de orden 4:

$$\langle i\rangle = \{\pm 1, \pm i\}, \quad \langle j\rangle = \{\pm 1, \pm j\}, \quad \langle k\rangle = \{\pm 1, \pm k\},$$

cada uno de los cuales, junto con el centro, forma la única colección de subgrupos en Q_8. Entonces, si $F/\mathbb{Q}$ es una extensión con grupo de Galois Q_8, el Teorema Fundamental de la Teoría de Galois 1.20 muestra que la correspondencia entre subgrupos de Q_8 y subcuerpos de F se rige según el esquema siguiente:



Además, se tiene que el grupo de Galois de $M/\mathbb{Q}$ es $Q_8\big/Z(Q_8) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, porque $|Q_8 : Z(Q_8)| = 8 : 2 = 4$ y no es difícil observar que las cuatro clases del grupo cociente son: $\{\pm 1\}, \{\pm i\}, \{\pm j\}, \{\pm k\}$, todas de orden 2.

5.1. Grupo de los Cuaterniones.

Si se desea encontrar una extensión de Galois $F/\mathbb{Q}$ cuyo grupo de Galois sea el grupo Q_8, se deben estudiar con detenimiento las extensiones cíclicas de orden 4, pues el grupo de los cuaterniones es el único grupo de orden 8 con tres subgrupos cíclicos de orden 4. Serán indispensables los dos teoremas que se enuncian a continuación [6], donde el segundo es el recíproco del primero. Si bien habría sido posible presentarlos bajo un único enunciado, se ha optado por separarlos para mayor claridad.

Teorema 5.1. *Sea F/K una extensión de Galois con grupo de Galois cíclico de orden 4. Entonces existe $d \in K$, que no es un cuadrado en K y existen $e, f \in K$ tales que*

$$F = K\Big(\sqrt{e + f\sqrt{d}}\Big),$$

y además $d(e^2 - f^2 d)$ es un cuadrado en K.

Demostración. Como el grupo de Galois de F/K es cíclico de orden 4, F tiene un subcuerpo M de grado 2 tal que $K \subset M \subset F$. Es fácil ver que cualquier extensión de grado 2 de un cuerpo K es $K(\sqrt{d})$ para algún d no cuadrado en K, y además por el mismo razonamiento existen $e, f \in K$ tales que

$$F = M(\alpha), \quad \text{donde } \alpha^2 = e + f\sqrt{d} \in M.$$

Dado que $\alpha^2 - e = f\sqrt{d}$, entonces $(\alpha^2 - e)^2 = (f\sqrt{d})^2$ y por ello α es raíz del polinomio

$$p(X) = X^4 - 2eX^2 + (e^2 - f^2 d).$$

Este polinomio no tiene ningún factor cúbico irreducible, pues 3 no divide a $[F : K] = 4$, además si se descompusiera en dos factores cuadráticos, α pertenecería a M, el único subcuerpo cuadrático de F. Por tanto $p(X)$ es irreducible sobre K. Sus raíces son $\pm\alpha$ y $\pm\beta$, donde $\beta^2 = e - f\sqrt{d}$. El discriminante de $p(X)$ es

$$\Delta(p) = [(2\alpha)(2\beta)(\alpha-\beta)(\alpha+\beta)(-\alpha-\beta)(-\alpha+\beta)]^2 = 16(\alpha\beta)^2(\alpha^2-\beta^2)^4 = 16(e^2-f^2d)f^4d^2,$$

y como $Gal(F/K)$ es cíclico de orden 4, entonces no es un subgrupo de A_4, pues este grupo no contiene subgrupos cíclicos de orden 4. De modo que por el Teorema 4.3 $\sqrt{\Delta} = \sqrt{16(e^2 - f^2 d)f^4 d^2} \notin K$. Esto implica que $(e^2 - f^2 d)$ no es un cuadrado en K. Para ver que $d(e^2 - f^2 d)$ sí lo es, obsérvese que $M(\alpha) = M(\beta)$ y $[F : M] = 2$, esto implica por la Proposición 1.35 que $\dfrac{\beta}{\alpha}$ es un cuadrado en M, y además

$$\frac{\beta^2}{\alpha^2} = \frac{e - f\sqrt{d}}{e + f\sqrt{d}} = \frac{(e - f\sqrt{d})^2}{e^2 - f^2 d}, \quad \text{por lo que } \frac{\beta}{\alpha} = \frac{e - f\sqrt{d}}{\sqrt{e^2 - f^2 d}}.$$

De aquí se deduce que $e^2 - f^2 d$ es un cuadrado en M y por tanto existen $r, s \in K$ tales que $e^2 - f^2 d = (r + s\sqrt{d})^2 = r^2 + s^2 d + 2rs\sqrt{d}$, entonces $2rs = 0$. Si $s = 0$, se contradice que $e^2 - f^2 d$ no sea un cuadrado en K, luego $r = 0$ y $e^2 - f^2 d = s^2 d$ de forma que $d(e^2 - f^2 d) = s^2 d^2$ es un cuadrado en K. □

Teorema 5.2. *Si $d \in K$ no es un cuadrado en K y $d(e^2 - f^2 d)$ es un cuadrado en K para ciertos $e, f \in K$. Entonces la extensión $F = K\big(\sqrt{e + f\sqrt{d}}\big)$ tiene grupo de Galois cíclico de orden 4 sobre K y el polinomio mínimo es $p(X) = X^4 - 2eX^2 + (e^2 - f^2 d)$.*

Demostración. Supóngase que d no es un cuadrado en K y $d(e^2 - f^2 d)$ sí lo es.

Entonces $e^2 - f^2 d$ no es un cuadrado en K y además $e + f\sqrt{d}$ no puede tener raíz cuadrada en $M = K(\sqrt{d})$, pues de lo contrario existirían $r, s \in K$ tales que $e + f\sqrt{d} = (r + s\sqrt{d})^2$ y esto implicaría que $f = 2rs$ y $e = r^2 + s^2 d$, de manera que $e^2 - f^2 d = (r^2 - s^2 d)^2$ sería un cuadrado perfecto en K, contradiciendo la hipótesis.

Sea, ahora $\alpha^2 = e + f\sqrt{d}$. Como α es raíz de

$$p(X) = X^4 - 2eX^2 + (e^2 - f^2 d) = \big(X^2 - (e + f\sqrt{d})\big)\big(X^2 - (e - f\sqrt{d})\big),$$

y cada factor cuadrático es irreducible sobre M, se concluye que $p(X)$ es irreducible sobre K. Su grupo de Galois, de orden 4, sólo puede ser cíclico o isomorfo a $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Puesto que $\Delta(p)$ no es un cuadrado en K, por el Teorema 4.3, no está contenido en A_4, y por tanto $Gal(F/K) \cong \mathbb{Z}/4\mathbb{Z}$. □

Ejemplo 5.3. Para la construcción de Q_8 sobre $\mathbb{Q}$, se puede considerar $M = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, de modo que los subcuerpos de índice 2 son $K_1 = \mathbb{Q}(\sqrt{2})$, $K_2 = \mathbb{Q}(\sqrt{3})$ y $K_3 = \mathbb{Q}(\sqrt{6})$. Se considera $\alpha^2 = (2 + \sqrt{2})(2 + \sqrt{3})(3 + \sqrt{6}) = 18 + 12\sqrt{2} + 10\sqrt{3} + 7\sqrt{6}$ de forma que admite las siguientes tres representaciones:

$$\alpha^2 = \begin{cases} e_1 + f_1\sqrt{d_1} = (18 + 12\sqrt{2}) + (10 + 7\sqrt{2})\sqrt{3} & \in K_1(\sqrt{3}) = M. \\ e_2 + f_2\sqrt{d_2} = (18 + 10\sqrt{3}) + (12 + 7\sqrt{3})\sqrt{2} & \in K_2(\sqrt{2}) = M. \\ e_3 + f_3\sqrt{d_3} = (18 + 7\sqrt{6}) + (12 + 5\sqrt{6})\sqrt{2} & \in K_3(\sqrt{2}) = M. \end{cases}$$

Se comprueba que, efectivamente, $d_i(e_i^2 - f_i^2 d_i)$ es un cuadrado en K_i para cada $i = 1, 2, 3$.

$$\begin{aligned} &\text{En } K_1: \quad 3[(18 + 12\sqrt{2})^2 - (10 + 7\sqrt{2})^2 \cdot 3] = [3(2 + \sqrt{2})]^2. \\ &\text{En } K_2: \quad 2[(18 + 10\sqrt{3})^2 - (12 + 7\sqrt{3})^2 \cdot 2] = [2(3 + 2\sqrt{3})]^2. \\ &\text{En } K_3: \quad 2[(18 + 7\sqrt{6})^2 - (12 + 5\sqrt{6})^2 \cdot 2] = [2(3 + \sqrt{6})]^2. \end{aligned}$$

Ahora, se debe observar que las definiciones de $F_i = K_i(\alpha)$ son coherentes, es decir, hay que comprobar que $F_1 = F_2 = F_3 = M(\alpha)$, y este cuerpo se denominará F. Primero, se ve que $F_1 = M(\alpha)$, es decir $\mathbb{Q}(\sqrt{2})(\alpha) = \mathbb{Q}(\sqrt{2}, \sqrt{3})(\alpha)$. De manera trivial $\mathbb{Q}(\sqrt{2})(\alpha) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3})(\alpha)$. Entonces, basta ver que $\sqrt{3} \in \mathbb{Q}(\sqrt{2})(\alpha)$, y efectivamente se tiene que

$$\sqrt{3} = \frac{\alpha^2 - (18 + 12\sqrt{2})}{10 + 7\sqrt{2}} \in \mathbb{Q}(\sqrt{2})(\alpha),$$

el resto de igualdades se demuestran de forma análoga.

Se concluye por el Teorema 5.2 que cada extensión $F = K_i(\alpha)$ tiene grupo de Galois cíclico de orden 4 sobre cada cuerpo intermedio K_i. Por tanto $[F : \mathbb{Q}] = [F : K_i][K_i : \mathbb{Q}] = 4 \cdot 2 = 8$. En conclusión, $Gal(F/\mathbb{Q}) \cong Q_8$, ya que este tiene 3 subgrupos cíclicos de orden 4 asociados a las tres subextensiones cíclicas F/K_i, $i = 1, 2, 3.$. El último paso es hallar el polinomio mínimo de la extensión $F/\mathbb{Q}$.

Según el Teorema 5.2 se puede observar que F es el cuerpo de escisión en K_1 del polinomio

$$\begin{aligned} p(X) = &\ X^4 - 2e_1X^2 + (e_1^2 - f_1^2 d_1) \\ = &\ X^4 - 2(18 + 12\sqrt{2})X^2 + (18 + 12\sqrt{2})^2 - 3(10 + 7\sqrt{2})^2 \\ = &\ X^4 - (36 + 24\sqrt{2})X^2 + (18 + 12\sqrt{2}) \end{aligned}$$

Para finalizar, se considera el automorfismo σ en M que fija $\sqrt{3}$ y tal que $\sigma(\sqrt{2}) = -\sqrt{2}$. Bajo esta conjugación se obtienen $\bar{e}_1 = 18 - 12\sqrt{2}$, $\bar{f}_1 = 10 - 7\sqrt{2}$, $\bar{d}_1 = 3$. Se toma $\beta^2 = (2 - \sqrt{2})(2 + \sqrt{3})(3 - \sqrt{6})$, de forma que β es raíz del polinomio

$$\begin{aligned} \overline{p(X)} = &\ X^4 - 2\bar{e}_1X^2 + (\bar{e}_1^2 - \bar{f}_1^2 \bar{d}_1) \\ = &\ X^4 - 2(18 - 12\sqrt{2})X^2 + (18 - 12\sqrt{2})^2 - 3(10 - 7\sqrt{2})^2 \\ = &\ X^4 - (36 - 24\sqrt{2})X^2 + (18 - 12\sqrt{2}) \end{aligned}$$

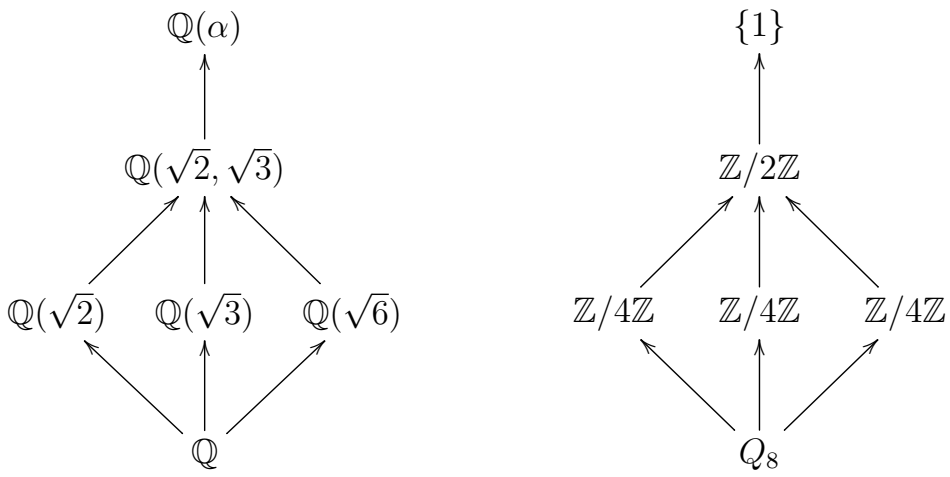
sobre $K_1 = \mathbb{Q}(\sqrt{2})$. Una observación es que $\alpha^2\beta^2 = 6(2 + \sqrt{3})^2$, por lo que

$$\beta = \frac{\sqrt{6}(2 + \sqrt{3})}{\alpha} \in F.$$

En virtud, de nuevo, del Teorema 5.2, $\overline{p(X)}$ es irreducible sobre K_1. En conclusión, α y β serán raíces del polinomio resultado del producto $p(X)\overline{p(X)}$,

$$q(X) = p(X)\overline{p(X)} = X^8 - 72X^6 + 180X^4 - 144X^2 + 36 \in \mathbb{Q}[X],$$

se verifica que $q(X)$ escinde en $F = K_1(\alpha) = K_1(\beta)$ pero no en ningún subcuerpo propio. Por tanto, F es el cuerpo de escisión de $q(X)$ sobre $\mathbb{Q}$, y $Gal(q(X)) \cong Q_8$. Esta configuración muestra los subgrupos de Q_8 y los subcuerpos de $\mathbb{Q}(\alpha)$ que fijan en la construcción de este ejemplo.



Capítulo 6

Realizaciones adicionales: grupo Diédrico D_n y grupos simples finitos.

6.1. Grupos Diédricos.

En preliminares ya se mostró el caso específico del grupo diédrico D_4 (ver Ejemplo 1.26), lo que presagia que, en general, cualquier grupo diédrico D_n sea realizable sobre $\mathbb{Q}$.

Los grupos diédricos D_n son los grupos de simetrías de un polígono regular de n lados, y se describe como el producto semidirecto $D_n \cong \mathbb{Z}/n\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$. Para demostrar que D_n se puede realizar como grupo de Galois sobre $\mathbb{Q}$ será importante la siguiente noción.

Definición 6.1. Sea G un grupo finito, se dice que G es *resoluble* si existe una cadena de subgrupos $\{1\} = G_n \subset G_{n-1} \subset \cdots \subset G_1 \subset G_0 = G$, tales que para todo $i \in \{1, \ldots, n\}$:

I) G_i es normal en G_{i-1}.

II) El grupo cociente G_{i-1}/G_i es abeliano.

El próximo teorema es considerado todo un hito en el Problema Inverso de Galois, su enunciado y demostración fueron inicialmente propuestas por Šafarevič en 1954, aunque con errores.

Teorema 6.2 (**Šafarevič**). *Todo grupo finito resoluble es realizable sobre* $\mathbb{Q}$.

A principios de este milenio, tres matemáticos alemanes motivados por la desinformación extendida en torno a este teorema, decidieron remendar estas imperfecciones, esta prueba definitiva se puede encontrar en [19]. La demostración de este resultado se basa en métodos de ramificación, cuya dificultad técnica excede a la de este trabajo.

El Teorema 6.2 aporta una técnica adicional al Problema Inverso, basta con demostrar que un grupo es resoluble para ver que es realizable. En particular este será el método que se usará para demostrar la realizabilidad de los grupos diédricos.

Teorema 6.3 (**Realización de los grupos diédricos**). *Sea $n \in \mathbb{N}$, existe $K/\mathbb{Q}$ extensión de Galois con $Gal(K/\mathbb{Q}) \cong D_n$.*

Demostración. Primero se observa que los grupos diédricos son resolubles. Considérese la sucesión de subgrupos normales $\{1\} \subset \mathbb{Z}/n\mathbb{Z} \subset D_n$, donde $\mathbb{Z}/n\mathbb{Z}$ es el subgrupo normal de D_n formado por las rotaciones, es el único de índice 2 en D_n, entonces

$$D_n\big/\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z}, \quad \mathbb{Z}/n\mathbb{Z}\big/\{1\} \cong \mathbb{Z}/n\mathbb{Z}.$$

Como ambos cocientes son grupos abelianos, se cumple la definición de grupo resoluble. Por el Teorema de Šafarevič 6.2, se tiene que existe una extensión $K/\mathbb{Q}$ tal que

$$Gal(K/\mathbb{Q}) \cong D_n. \qquad \square$$

6.2. Grupos Simples Finitos.

Un grupo G es *simple* si sus únicos subgrupos normales son el trivial y el propio grupo. A finales del s. XIX, el interés, impulsado por Otto Hölder [13], por conocer qué grupos finitos son simples fue uno de los problemas más abordados en la teoría de grupos. Ahí dio comienzo el denominado *proyecto Hölder*, una ambiciosa búsqueda que durante décadas motivó a matemáticos a aportar avances significativos en la clasificación de estos grupos, una tarea que marcaría el rumbo de la teoría de grupos moderna. Fue el punto de partida para el esfuerzo sistemático que culminaría en el famoso Teorema de clasificación de los grupos simples finitos. La demostración completa se anunció en 2004 [1], esta se extiende a lo largo de miles de páginas, en cientos de artículos y es obra de decenas de autores.

Teorema 6.4 (**Clasificación de los grupos simples finitos**). *Sea G un grupo simple finito, entonces G es isomorfo a uno de los siguientes grupos:*

I) Un grupo cíclico de orden primo.

II) Un grupo alternado A_n con $n \geq 5$.

III) Un grupo de Lie finito.

IV) Uno de los 26 grupos esporádicos.

V) El grupo de Tits.

La clasificación de grupos simples finitos deja 26 grupos esporádicos sin patrón, que no se incluyen dentro del resto de grupos. En el s. XX se demostró que la mayoría pueden realizarse sobre $\mathbb{Q}$. Cuatro de los cinco grupos de Mathieu: $M_{11}, M_{12}, M_{22}, M_{24}$ son realizables. Utilizando métodos computacionales, se pueden obtener, por ejemplo, polinomios con grupo de Galois M_{11} y M_{12} [5].

$$\begin{aligned} f_1(X) =& X^{11} + 101X^{10} + 4151X^9 + 87851X^8 + 976826X^7 \\ &+ 4621826X^6 - 5948674X^5 - 113111674X^4 - 12236299X^3 \\ &+ 1119536201X^2 - 1660753125X - 332150625 \end{aligned}$$

$$\begin{aligned} f_2(X) =& X^{12} + 100X^{11} + 4050X^{10} + 83700X^9 + 888975X^8 \\ &+ 3645000X^7 - 10570500X^6 - 107163000X^5 + 100875375X^4 \\ &+ 1131772500X^3 - 329614375X^2 + 1328602500X + 332150625. \end{aligned}$$

De esta forma, se evidencia que incluso estructuras tan complejas y excepcionalmente construidas pueden obtenerse como grupos de Galois sobre $\mathbb{Q}$.

Un hito en este campo fue la construcción del denominado grupo Monstruo, el más grande de los grupos finitos, como grupo de Galois sobre $\mathbb{Q}$, un resultado de Thompson [21]. En resumen, todos los 26 grupos esporádicos, salvo quizá M_{23}, se sabe que aparecen como grupos de Galois sobre $\mathbb{Q}$. En el s. XXI, se han refinado estas técnicas mediante herramientas modernas. Aún así, el caso de M_{23} sigue sin resolverse: no se conoce ningún polinomio sobre $\mathbb{Q}$ con grupo de Galois M_{23}.

Se sabe que prácticamente todas las familias de grupos de Lie finitos simples se pueden realizar como grupos de Galois sobre $\mathbb{Q}$ [17] gracias a la existencia de polinomios genéricos en $\mathbb{Q}(t)$ y al Teorema de Irreducibilidad de Hilbert 4.8. En particular, se han construido familias paramétricas para grupos de Lie como $\mathrm{PSL}(n,q)$, $\mathrm{PSp}(2n,q)$, $G_2(q)$, entre otros, de modo que al especializar t se obtienen extensiones de $\mathbb{Q}$ con esos grupos de Galois.

El grupo de Tits (${}^2F_4(2)'$) es singular, no forma parte de ninguna otra familia infinita, por ello algunos le consideran el grupo Esporádico número 27. Su realización definitiva como grupo de Galois sobre $\mathbb{Q}$ se atribuye a técnicas de rigidez [17]. Este último ejemplo pone de manifiesto que incluso el único grupo "rebelde" de la clasificación acaba sometiéndose a las mismas normas que rigen la realización del resto de grupos simples.

«Je n'ai pas le temps»

-Évariste Galois.

Bibliografía

[1] M. Aschbacher. «The Status of the Classification of the Finite Simple Groups». En: *Notices of the American Mathematical Society* Vol. 51, No. 7, 2004, págs. 736-740.

[2] K. Conrad. *Galois Groups as Permutation Groups*. URL: https://kconrad.math.uconn.edu/blurbs/galoistheory/galoisaspermgp.pdf (último acceso 14-06-2025).

[3] K. Conrad. *Recognizing Galois Groups S_n and A_n*. URL: https://kconrad.math.uconn.edu/blurbs/galoistheory/galoisSnAn.pdf (último acceso 14-06-2025).

[4] D. A. Cox. *Galois Theory*. 2.ª ed. Hoboken, NJ: John Wiley & Sons, Inc., 2012. ISBN: 978-1-118-07205-9.

[5] H. Darmon y D. Ford. «Computational Verification of M_{11} and M_{12} as Galois Groups over Q». En: *Communications in Algebra* 17 1989, págs. 2941-2943.

[6] R. A. Dean. «A Rational Polynomial Whose Group Is the Quaternions». En: *The American Mathematical Monthly* Vol. 88, No. 1, 1981, págs. 42-45.

[7] D. S. Dummit y R. M. Foote. *Abstract Algebra*. 3.ª ed. Wiley-Interscience. Hoboken, NJ: John Wiley & Sons, Inc., 2004. Cap. 13. ISBN: 0-471-43334-9.

[8] L. Euler. «Theorematum Quorundam ad Numeros Primos Spectantium Demonstratio.» En: *Commentarii academiae scientiarum Petropolitanae* 8, 1736, págs. 141-146.

[9] P. Fernández-Ferreirós. *Teoría de Galois*. Universidad de Cantabria, Departamento de Matemáticas, Estadística y Computación, 2023.

[10] J. F. Fernando y J. M. Gamboa. *Ecuaciones algebraicas: extensión de cuerpos y teoría de Galois*. Madrid, Sanz y Torres, D.L., 2015. ISBN: 978-84-15550-98-3.

[11] D. Hilbert. «Ueber die Irreducibilität ganzer rationaler Functionen mit ganzzahligen Coefficienten.» En: *Journal für die reine und angewandte Mathematik* 110 1892, págs. 104-129. URL: http://eudml.org/doc/148853.

[12] D. Hilbert. «Ein neuer Beweis des Kronecker'schen Fundamentalsatzes über Abel'sche Zahlkörper». En: *Nachrichten der Gesellschaft der Wissenschaften zu Göttingen* 1896, págs. 29-39.

[13] O. Hölder. «Die einfachen Gruppen in ersten und zweiten Hundert der Ordnungszahlen». En: *Mathematische Annalen* Vol. 40, No. 1, 1892, págs. 55-88.

[14] C. U. Jensen, A. Ledet y N. Yui. *Generic Polynomials: Constructive Aspects of the Inverse Galois Problem*. Mathematical Sciences Research Institute Publications. Cambridge University Press, 2002. ISBN: 0521819989.

[15] J. J. Jiménez Garrido. *Estructuras Algebraicas*. 4.ª ed. Universidad de Cantabria, Departamento de Matemáticas, Estadística y Computación, 2024.

[16] M. Kumar, G. Shekar y L. Misra. «A Study on the Inverse Galois Problem in Galois Theory». En: *International Journal of Modern Electronics and Communication Engineering,* Volume No.-3, Issue No.-3, 2015, págs. 15-19.

[17] G. Malle y B. H. Matzat. *Inverse Galois Theory*. Vol. 328. Grundlehren der Mathematischen Wissenschaften. Springer, 1999. ISBN: 978-3-540-65462-6.

[18] J. S. Milne. *Fields and Galois Theory (v5.10)*. 2022.

[19] J. Neukirch, A. Schmidt y K. Wingberg. *Cohomology of Number Fields*. 1.ª ed. Vol. 323. Grundlehren der Mathematischen Wissenschaften. Berlin, Heidelberg: Springer-Verlag, 2000. Cap. IX. ISBN: 978-3-540-37888-4.

[20] P. Samuel. *Algebraic Theory of Numbers*. Paris, France: Hermann, 1970.

[21] J. G. Thompson. «Some finite groups which appear as Gal L/K, where $K \subseteq \mathbb{Q}(\mu_n)$». En: *Journal of Algebra* Vol. 89, No. 2, 1984, págs. 437-499.

[22] B. L. van der Waerden. *Algebra*. Vol. I. Springer, 2003.