UNIVERSIDAD DE PANAMÁ

VICERRECTORÍA DE INVESTIGACIÓN Y POSTGRADO

FACULTAD DE CIENCIAS NATURALES Y EXACTAS

PROGRAMA DE MAESTRÍA EN MATEMÁTICA PURA

TÍTULO DE LA TESIS:
TEORÍA DE GALOIS EN EXTENSIONES ALGEBRAICAS DE GRADO INFINITO

Presentado por

Irving J. Urieta R.

c.i.p. 9-721-1838

Profesor Asesor:

Dr. José Félix Solanilla

COCLÉ, REPÚBLICA DE PANAMÁ

-2021-

Agradecimientos

A todos los profesores que contribuyeron a mi formación durante la maestría y, en especial, al Dr. José Solanilla por su asesoría en este trabajo.

Dedicatoria

A mi familia.

Resumen

En este trabajo se presenta una teoría de Galois para extensiones algebraicas de grado infinito, en particular, la generalización de la versión clásica del Teorema Fundamental de la Teoría de Galois. Iniciamos dotando al grupo de Galois, $\mathrm{Gal}(L/K)$, con la topología de Krull. Como primera consecuencia, se obtiene que los subgrupos cerrados son los que se corresponden con los subcuerpos intermedios de la extensión. Adicionalmente, el grupo de Galois adquiere la propiedad de Hausdorff, totalmente disconexo y compacto. Finalmente, utilizamos la teoría de grupos profinitos para caracterizar al grupo de Galois y calcularlo para ciertas extensiones de $\mathbb{Q}$, $\mathbb{F}_p$ y $\mathbb{C}(t)$.

Abstract

In this paper we present a Galois theory for algebraic extensions of infinite degree, in particular, the generalization of the classical version of the fundamental theorem of Galois theory. We start by endowing the Galois group $\mathrm{Gal}(L/K)$ with the Krull topology. As a first consequence, we obtain that the closed subgroups are those corresponding to the intermediate subfields of the extension. Additionally, the Galois group acquires the Hausdorff property, totally disjoint and compact. Finally, we use the theory of profinite groups to characterize the Galois group and calculate it for certain extensions of $\mathbb{Q}$, $\mathbb{F}_p$ and $\mathbb{C}(t)$.

Índice general

Introducción

Nuestra primera experiencia con la teoría de Galois se limita al estudio del grupo de Galois de extensiones de grado finito, cuyo resultado central es el *Teorema Fundamental de la Teoría de Galois* que afirma que cuando una extensión L/K es de grado finito, normal y separable, se establece una correspondencia uno a uno entre todos los subgrupos del grupo de Galois de la extensión, $\mathrm{Gal}\,(L/K)$, y todos los subcuerpos intermedios de la misma. La correspondencia asigna a cada subcuerpo intermedio de L el subgrupo de $\mathrm{Gal}\,(L/K)$ cuyos elementos son todos los automorfismos de L que fijan el subcuerpo y, recíprocamente, a cada subgrupo de $\mathrm{Gal}\,(L/K)$ asigna el subcuerpo intermedio de elementos de L que quedan fijos por todos los automorfismos que pertenecen al subgrupo. La demostración de tal correspondencia de Galois depende en gran medida de la finitud de la extensión y ya solo en este caso, es una idea poderosa que permite la aplicación de la teoría de grupos al estudio de los cuerpos. Sin embargo, al profundizar sobre otro tipo de extensiones, observamos que existen extensiones como, por ejemplo, la de los números algebraicos sobre los racionales que no son grado finito y para las cuales el teorema fundamental no es cierto. Este hecho ha sido la principal fuente de motivación para el desarrollo de la presente tesis, la cual hemos orientado sobre la base de las siguientes interrogantes: ¿Qué sucede si L/K es una extensión de grado infinito? ¿Es posible desarrollar una teoría de Galois para extensiones de grado infinito? ¿Cómo establecer una correspondencia (si es posible) entre los subcuerpos intermedios de la extensión y los subgrupos de su grupo de Galois? ¿Qué resultados de la teoría de Galois para extensiones de grado finito son generalizables y cómo?

Hemos considerado dividir la tesis en tres capítulos. Previo a ellos, se considera un capítulo 0 sobre el desarrollo histórico de la teoría de Galois con el propósito de ilustrar al lector cómo se ha gestado, *grosso modo*, las ideas de Galois hasta la actualidad.

En el primer capítulo presentamos preliminares algebraicos y topológicos. Iniciamos con la teoría general de extensiones de cuerpos; en particular, nos limitaremos a las extensiones algebraicas, normales, separables y de Galois, para las cuales proporcionamos los hechos más relevantes que se necesitarán en los capítulos siguientes. El resultado principal en esta área es el Teorema 1.21, conocido como Teorema Fundamental de la Teoría de Galois para extensiones de grado finito:

Teorema 1.21. (Teorema Fundamental de la Teoría de Galois) *Sea L/K una extensión de Galois finita y $G = \mathrm{Gal}(L/K)$. Entonces existe una correspondencia uno a uno, que revierte inclusiones, entre los cuerpos intermedios E de L/K y los subgrupos de H de G, dado por*

$$E \overset{*}{\mapsto} \mathrm{Gal}(L/E), \quad H \overset{\star}{\mapsto} \mathcal{F}(H)$$

Se tiene además que si $E \leftrightarrow H$ entonces

(1) $[L : E] = |H|$ *y* $|G : H| = [E : K]$, *donde* $|G : H|$ *denota el índice de* H *en* G.

(2) $H \triangleleft G$ *si y sólo si* E/K *es de Galois. Cuando esto ocurre,* $\mathrm{Gal}(E/K) \cong G/H$.

Finalizamos el capítulo con ejemplos de extensiones de grado infinito y mostramos cómo una de ellas no cumple el teorema fundamental.

El capítulo dos es el más importante de la tesis y en él abordamos la generalización de la correspondencia de Galois a las extensiones de grado infinito. El teorema principal del capítulo es el *Teorema de Krull* (Teorema 2.3), generalización del teorema fundamental. La clave para llevar a cabo tal generalización es considerar la colección $\mathcal{N} = \{N_i \mid i \in I\}$, donde cada $N_i = \mathrm{Gal}(L/E_i)$ es un subgrupo del grupo de Galois de la extensión L/K, con E_i/K una extensión de Galois de grado finito; de este modo obtenemos el Teorema 2.1,

Teorema 2.1. *La colección* $\mathcal{B} = \{\sigma N_i : \sigma \in \mathrm{Gal}(L/K),\, N_i \in \mathcal{N}\}$ *es una base para una topología sobre* $\mathrm{Gal}(L/K)$.

La topología generada por $\mathcal{B}$ sobre el grupo de Galois es llamada *topología de Krull*. Como consecuencia, los subgrupos que son cerrados en la topología son los que se corresponden uno a uno con los subcuerpos intermedios de la extensión, resultado que queda plasmado en el Teorema de Krull.

Teorema 2.3. (Teorema de Krull) *Sea* L/K *una extensión de Galois y* $G = \mathrm{Gal}(L/K)$. *Con la topología de Krull, existe una correspondencia uno a uno, que revierte inclusiones, entre los cuerpos intermedios* E *de* L/K *y los subgrupos cerrados* H *de* G, *dado por*

$$E \overset{*}{\mapsto} \mathrm{Gal}(L/E), \quad H \overset{\star}{\mapsto} \mathcal{F}(H)$$

Además, si $E \leftrightarrow H$ *entonces*

(1) $|G : H| < \infty$ *si y solo si* $[E : K] < \infty$ *si y solo si* H *es abierto. Cuando esto ocurre,* $|G : H| = [E : K]$.

(2) $H \triangleleft G$ *si y sólo si* E/K *es de Galois. Cuando esto ocurre,* $\mathrm{Gal}(E/K) \cong G/H$.

Salvo ciertos detalles en el inciso (1) del teorema, las afirmaciones que acompañan al Teorema de Krull son las mismas que las del teorema fundamental en la versión finita. La sección final del capítulo describe la estructura topológica del grupo de Galois y, en este sentido, se prueba que el grupo es Hausdorff, totalmente disconexo y compacto. La demostración de la compacidad del grupo de Galois es especialmente relevante ya que muestra que el grupo de Galois puede ser visto como un subgrupo del producto directo de cocientes finitos sobre sus subgrupos normales, lo que inspira el tercer capítulo de la tesis.

Para concluir la tesis, en el tercer capítulo caracterizamos el grupo de Galois por medio de los grupos finitos $X_i = \mathrm{Gal}(L/K)/N_i$, donde $N_i = \mathrm{Gal}(L/E_i)$ y E_i/K es finita y de Galois. En la primera sección presentamos la noción de sistema inverso de grupos y mostramos que todo sistema inverso de grupos tiene un límite inverso. En la segunda sección, contextualizamos la

teoría al caso del grupo de Galois para establecer nuestro principal resultado: la caracterización del grupo de Galois como grupo profinito.

Teorema 3.3. *Sea L/K una extensión de Galois y $\{X_i, \varphi_{ij}, I\}$ el sistema inverso para el cual $X_i = \mathrm{Gal}(E_i/K)$, con E_i/K es una extensión de Galois finita. Entonces la función*

$$\chi : \mathrm{Gal}(L/K) \to \varprojlim \mathrm{Gal}(E_i/K)$$

definida por

$$\sigma \mapsto \mathbf{x}, \text{ tal que } \mathbf{x}(i) = \sigma|_{E_i} \quad (i \in I)$$

es un isomorfismo de grupos.

Finalmente, la tercera sección de la tesis aplica los resultados del tercer capítulo al cálculo del grupo de Galois de ciertas extensiones algebraicas de $\mathbb{Q}$, $\mathbb{F}_p$ y $\mathbb{C}(t)$.

Capítulo 0

Desarrollo de la teoría de Galois

Las ideas originales contenidas en los artículos de E. Galois experimentaron un largo y lento desarrollo hasta la formulación que conocemos hoy en día como teoría de Galois. Los cimientos fueron establecidos por Lagrange en 1770 y finalmente concretados, en la versión moderna, por E. Artin en 1926.

Este primer capítulo es breve y su propósito es describir el desarrollo que tuvo la teoría de Galois, desde sus antecedentes hasta su versión definitiva. Para un análisis más extenso y detallado de este desarrollo, recomendamos la lectura de Kiernan (1971) y Gray (2018).

0.1. Antecedentes

La actividad algebraica clásica consistió en tratar de resolver ecuaciones algebraicas mediante fórmulas a partir de sus coeficientes; tales fórmulas involucran sumas, restas, multiplicaciones, divisiones y extracción de raíces. A esto también le llamamos resolver la ecuación por radicales. Los babilonios ya sabían, hace 4 000 años, cómo resolver las ecuaciones cuadráticas y las soluciones generales de las ecuaciones de grado tres y cuatro se obtuvieron en el siglo XVI por Cardano y Ferrari, respectivamente.

Lagrange fue el primer matemático que trabajó sobre el problema de resolución de ecuaciones de quinto grado o más. Su principal contribución fue el artículo *Réflexions sur la*

résolution algébrique des équations, en el cual examina en detalle los métodos conocidos para resolver las ecuaciones de segundo, tercer y cuarto grado, con el propósito de abstraer algún procedimiento general. Lagrange estudió cómo las expresiones racionales en las raíces de la ecuación cambiaban bajo las permutaciones de dichas raíces (Kiernan, 1971). Barrera (2011) describe, por ejemplo, el proceso utilizado por Lagrange para la ecuación de tercer grado como sigue: Lagrange introduce un elemento, $V = x_1 + \zeta x_2 + \zeta^2 x_3$, donde ζ es una raíz cúbica de la unidad diferente de 1 y x_1, x_2, x_3 son las raíces de la ecuación cúbica. Al permutar las raíces, V tiene seis valores posibles $V = V_1, V_2, V_3, V_4, V_5, V_6$. Lagrange construye una ecuación de sexto grado cuyas raíces son estos seis valores posibles,

$$g(X) = (X - V_1)(X - V_2)(X - V_3)(X - V_4)(X - V_5)(X - V_6).$$

A esta ecuación Lagrange la llamó *resolvente de la ecuación*. Los coeficientes de la ecuación son simétricos en los seis valores de V y, por tanto, son simétricos en x_1, x_2, x_3. Luego, utilizando la identidad $1 + \zeta + \zeta^2$, la resolvente se reduce a

$$g(X) = X^6 - \left(V_1^3 + V_4^3\right) X^3 + (V_1 V_4)^3 = 0,$$

la cual es una ecuación de segundo grado en X^3 y se puede resolver. Similarmente, para una ecuación de cuarto grado se obtiene como resolvente una ecuación de grado 24, que resulta ser la cuarta potencia de una ecuación de grado seis, y esta a su vez se reduce a una cúbica que ya se sabe resolver. Cuando trató de aplicar este proceso a la ecuación de quinto grado, sospechó la imposibilidad de resolverla mediante fórmulas; dejó pendiente este caso, afirmando que dudaba de sus procedimientos. Sin embargo, estos constituyeron la base para que Ruffini (en 1799) y Abel (en 1824) lograrán demostrar la imposibilidad de resolver, en general, la ecuación de quinto grado por medio de fórmulas. La prueba de Abel fue mejor recibida por los matemáticos de la época y puede consultarse en Kiernan (1971), p.p. 67-72.

0.2. Galois

En su *Mémoire sur les conditions de résolubilité des équations par radicaux* de 1831, Galois retoma la idea de resolvente de una ecuación introducida por Lagrange y establece una correspondencia entre ecuaciones y el grupo de permutaciones de sus raíces. Como una aplicación de su teoría, consigue una respuesta completa al problema de resolver ecuaciones por medio de fórmulas. La memoria original no fue publicada sino hasta 1846 de la mano de J. Liouville y está disponible en francés con traducción simultánea a inglés en Neumann (2011, p.p. 106-144). También puede consultarse (en inglés) en Edwards (1984, p.p. 101-113).

Galois inicia su memoria definiendo algunos conceptos como permutación y sustitución. Luego presenta cuatro lemas: Los Lemas II y III, en lenguaje moderno, equivalen al Teorema del Elemento Primitivo para extensiones separables de grado finito; el Lema IV muestra la relación que existe entre los conjugados del resolvente y las raíces de la ecuación original. Ahora Galois proporciona resultados propios enunciados en las Proposiciones I a VIII. En la Proposición I define el grupo de permutaciones de las raíces de un polinomio (el grupo de Galois); en las II a IV, establece propiedades de este grupo y en la Proposición V aborda la pregunta:

Problema. ¿En cuáles casos una ecuación es soluble por radicales?

Aquí da condiciones necesarias y suficientes para que una ecuación sea soluble por radicales. El *Teorema Fundamental de la Teoría de Galois* aparece implícitamente en la demostración de este resultado (Barrera, 2011). En las Proposiciones VI a VIII, Galois aplica su teoría a las ecuaciones irreducibles de grado primo para determinar una condición necesaria y suficiente para que esta sea soluble por radicales.

La idea original de Galois contenida en la Proposición V para determinar si una ecuación es soluble por radicales es, *grosso modo*, la siguiente: Considere, por ejemplo, la ecuación cuadrática $x^2 + bx + c = 0$. Los coeficientes de la ecuación y sus raíces r_1, r_2 se relacionan por

medio de las funciones polinómicas simétricas

$$b = -(r_1 + r_2)$$

$$c = r_1 r_2.$$

Aquí, r_1 y r_2 se consideran como variables arbitrarias. Teniendo en cuenta que la fórmula para resolver esta ecuación es

$$\frac{-b \pm \sqrt{b^2 - 4c}}{2},$$

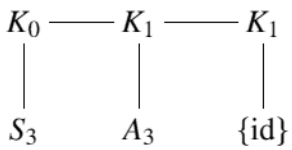
observamos que el radical $\sqrt{b^2 - 4c}$ transforma una función simétrica en r_1 y r_2, a saber, $b^2 - 4c = (r_1 + r_2)^2 - 4r_1 r_2$, en dos funciones no simétricas $\sqrt{b^2 - 4c} = \pm(r_1 - r_2)$. Ahora, considere el conjunto K_0 de todas la expresiones (fórmulas) que se obtienen a partir de b y c por medio de sumas, restas, multiplicaciones y divisiones. Una propiedad que tiene este conjunto es que sus elementos son invariantes bajo permutaciones de r_1 y r_2. Por ejemplo, los elementos de K_0,

$$\begin{aligned} b^2 - 4c &= (r_1 + r_2)^2 - 4r_1 r_2 \\ -\frac{b}{2} + c &= \frac{r_1 + r_2}{2} + r_1 r_2 \\ 2c - b &= 2r_1 r_2 + (r_1 + r_2), \end{aligned}$$

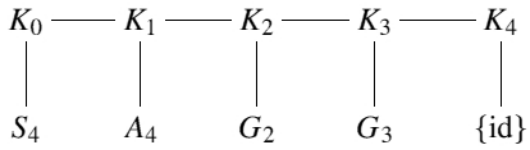
son invariantes bajo permutaciones de r_1 y r_2. En consecuencia, Galois asocia K_0 con el grupo S_2, de permutaciones de dos elementos. Ahora, definamos K_1 de la misma manera, pero permitiendo operar con $\sqrt{b^2 - 4c}$. Entonces, $K_0 \subseteq K_1$ y $r_1, r_2 \in K_1$, de modo que el paso de K_0 a K_1 representa resolver la ecuación. Como los elementos de K_1 donde aparece $\sqrt{b^2 - 4c}$ no resultan ser funciones simétricas de las raíces, le asociamos el grupo trivial de simetrías $\{\mathrm{id}\}$. En un diagrama,

$$\begin{array}{ccc} K_0 & \text{———} & K_1 \\ | & & | \\ S_2 & & \{\mathrm{id}\} \end{array}$$

De forma análoga, en el caso de la ecuación de tercer grado se tiene el esquema



donde A_3 es el grupo alternante. Y para la ecuación de cuarto grado,



donde G_2 y G_3 son ciertos subgrupos de S_4 de orden cuatro y dos, respectivamente. De esta forma, resolver la ecuación de segundo, tercer y cuarto grado implica reducir su grupo sucesivamente hasta que contenga solo una permutación (Galois, en Edwards, 1984). En lenguaje moderno esto quiere decir que existe una cadena de subgrupos que empieza en S_n y termina en {id}; además, cada subgrupo es normal en el anterior y su cociente es de orden un número primo. Esta es la condición necesaria y suficiente para que la ecuación sea soluble por radicales.

En el caso de la ecuación general de grado cinco (o más), no existe tal cadena de subgrupos con las propiedades deseadas, lo que permite concluir que no existe una fórmula para resolver la ecuación de quinto grado (o más) por radicales.

0.3. Formulación actual

El siguiente avance en la teoría de Galois se debe al desarrollo de la teoría de cuerpos que se dio en Alemania a raíz de los trabajos de Gauss en teoría de números, los cuales inspiraron a matemáticos como Kronecker y Dedekind a desarrollar la teoría de cuerpos y relacionarla, posteriormente, con la teoría de Galois. En particular, Kronecker fue el primero en describir el grupo de Galois no en términos de permutaciones de las raíces, sino como un grupo de

automorfismos del cuerpo de coeficientes y Dedekind reformuló, en 1984, la teoría de Galois en términos de extensiones de cuerpos, las cuales interpreta como un espacio vectorial sobre subcuerpos de números complejos. Gray (2018) señala que el historiador Walther Purkert mostró que Dedekind fue el primer matemático que ofreció un seminario sobre teoría de Galois en Göttingen en 1857-1858.

Muchos de los resultados de Dedekind fueron fundamentales para la formulación posterior y definitiva de Emil Artin de la teoría de Galois. En una conferencia de 1926, Artin presenta la versión definitiva de la teoría de Galois en términos de automorfismos de cuerpos y enfatiza que el objetivo de lo que hoy llamamos teoría de Galois no debería ser determinar las condiciones para la solubilidad de ecuaciones algebraicas, sino expresar las relaciones entre extensiones de cuerpos y grupo de automorfismos. Así, reúne todas las conclusiones importantes en un *Teorema Fundamental de la Teoría de Galois*, el cual establece una correspondencia uno a uno entre los subcuerpos intermedios de una extensión y los subgrupos de su grupo de Galois. La conferencia se publicó posteriormente en dos notas: *Foundations of Galois Theory* en el año 1938 y *Galois Theory* en 1942.

0.3.1. Sobre las extensiones de grado infinito

Cabe resaltar que la teoría original de Galois y sus consideraciones posteriores hacían referencia a extensiones de grado finito. Fue Dedekind, en 1901, el primero en investigar el grupo de Galois de una extensión de grado infinito (Koch, 2002).

Dedekind estudió la extensión ciclotómica $\mathbb{Q}(\zeta_\infty) = \cup_{n\in\mathbb{N}}\mathbb{Q}\left(\zeta_{p^n}\right)$, donde p es primo y ζ_{p^n} es una raíz p^n-ésima primitiva de la unidad sobre $\mathbb{Q}$ y determinó una correspondencia entre los subcuerpos de $\mathbb{Q}(\zeta_\infty)$ y una familia propia de subgrupos del grupo de Galois de esta extensión, demostrando así que el teorema fundamental falla al considerarlo al caso infinito. Además, reconoció que el grupo de Galois tiene una importante topología. En 1920, Krull abstrajo esta topología para grupos de Galois arbitrarios, logrando una generalización de la teoría de Galois finita a extensiones algebraicas de grado infinito y demostrando que los subgrupos cerrados son

los que se corresponden con los subcuerpos intermedios de la extensión.

0.4. Generalizaciones

La teoría clásica de Galois ha tomado diversas direcciones, por lo que en la actualidad no hablamos de teoría de Galois, sino de *teorías de Galois*. Otras versiones de la teoría de Galois se han generalizado para anillos, sistema de ecuaciones diferenciales, etc. Un diagrama que ilustra estas generalizaciones puede consultarse en Borceux y Janelidze (2001, p. ix).

Este trabajo lo abordaderemos desde el enfoque dado por la topología de Krull, ya que nos delimitaremos a las extensiones algebraicas de grado infinito.

Capítulo 1

Preliminares

Iniciamos presentando los conceptos y las notaciones que se utilizarán a lo largo del trabajo. Las primeras tres secciones tienen como contexto las extensiones algebraicas en general; la cuarta está dedicada a la teoría de Galois para extensiones de grado finito, la cual a menudo se le conoce como teoría de Galois clásica.

En la última sección se presentan las ideas topológicas involucradas en el estudio de la teoría de Galois en extensiones algebraicas de grado infinito.

1.1. Extensiones de cuerpos

Definición 1.1. Si L y K son cuerpos, diremos que L es una *extensión* de K si existe un monomorfismo $f : K \hookrightarrow L$.

De esta definición se deduce que L contiene un subcuerpo isomomorfo a K. Así, que L sea una extensión de K a menudo se interpreta como $K \subseteq L$ y lo denotaremos por L/K. También, las extensiones muchas veces se indican con diagramas reticulares como el siguiente:

$$\begin{array}{c} L \\ | \\ K \end{array}$$

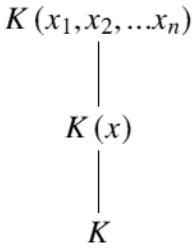
Ejemplo 1.1.

(i) Por medio del homomorfismo inclusión ι, el cual es inyectivo, se tiene que

$$\mathbb{Q} \overset{\iota}{\hookrightarrow} \mathbb{R} \overset{\iota}{\hookrightarrow} \mathbb{C}.$$

Por lo tanto, el cuerpo $\mathbb{C}$, de números complejos, es una extensión del cuerpo $\mathbb{R}$, de números reales, y éste es, a su vez, una extensión del cuerpo $\mathbb{Q}$, de números racionales. Indicamos tales extensiones en el siguiente diagrama reticular:

(ii) Sea K un cuerpo arbitrario. Consideremos los cuerpos de cocientes de los anillos de polinomios $K[x]$ y $K[x_1, x_2, ..., x_n]$ (donde $x, x_1, x_2, ..., x_n$ son indeterminadas), denotados por $K(x)$ y $K(x_1, x_2, ..., x_n)$, respectivamente. Se tiene entonces que, por medio del homomorfismo inclusión, $K(x_1, x_2, ...x_n)$ es una extensión de $K(x)$ y éste es a su vez una extensión de K. Indicamos sus relaciones en el siguiente diagrama reticular



Observación 1.1. Los cuerpos intermedios (o subcuerpos) que aparecen en los diagramas reticulares anteriores reciben el nombre de subextensiones. Es decir, si L es una extensión de E y E es una extensión de K, entonces el cuerpo E es una subextensión de L/K.

En la extensión L/K, el cuerpo L puede ser visto como un $K-$ espacio vectorial, considerando la multiplicación definida en L como un producto escalar. Esta afirmación se justifica en el siguiente teorema.

Teorema 1.1. *Si L/K es una extensión de cuerpos, entonces L es un espacio vectorial sobre K.*

Demostración. En primer lugar, el cuerpo L es un grupo abeliano con la operación de adición. Dotamos a L con la estructura de $K-$ espacio vectorial, definiendo un producto escalar para $\alpha \in K$ y $v \in L$ por $\alpha \cdot v = \alpha v$; esto es, la multiplicación de α por v en L. De los axiomas de cuerpo para L, se tiene que para este producto escalar se cumple:

- la propiedad asociativa: $\alpha \cdot (\beta \cdot v) = (\alpha \cdot \beta) \cdot v$, para todo α, β en K y todo v en L.
- la existencia del elemento neutro $1 \in K$: $1 \cdot v = v$, para todo v en L.
- la propiedad distributiva respecto a la suma vectorial: $\alpha \cdot (u+v) = \alpha \cdot u + \alpha \cdot v$, para todo α en K y todo u, v en L.
- la propiedad distributiva respecto a la suma escalar: $(\alpha+\beta) \cdot v = \alpha \cdot v + \beta \cdot v$, para todo α, β en K y todo v en L.

Por lo tanto, L es un espacio vectorial sobre K. □

Este resultado permite utilizar el álgebra lineal en el estudio de la teoría de cuerpos, como veremos a continuación.

Definición 1.2. A la dimensión de L como espacio vectorial sobre K lo denotamos $[L : K]$ y se le llama *grado de la extensión*. La extensión L/K es de *grado finito* si $[L : K] < \infty$. En caso contrario, la extensión es de *grado infinito.*

El siguiente resultado relaciona el grado de una extensión L/K con el grado de sus subextensiones.

Teorema 1.2 (Teorema de la Torre)**.** *Sean L/E y E/K extensiones de cuerpos. Entonces*

$$[L : K] = [L : E]\,[E : K]\,.$$

Demostración. Sea $\{a_i : i \in I\}$ una base para E como espacio vectorial sobre K y $\{b_j : j \in J\}$ una base para L sobre E. Consideremos el conjunto $\{a_i b_j : i \in I, j \in J\}$ y probemos que es una base para L sobre K.

Para la independencia lineal supongamos que para una combinación lineal finita

$$\sum_{i,j} k_{ij} a_i b_j = 0, \text{ con } k_{ij} \in K.$$

Reagrupando,

$$\sum_j \left(\sum_i k_{ij} a_i \right) b_j = 0.$$

Como los coeficientes $\sum_i k_{ij} a_i$ están en E y los b_j son linealmente independientes sobre E se tiene

$$\sum_i k_{ij} a_i = 0.$$

Repitiendo el argumento llegamos a $k_{ij} = 0$ para todo $i \in I, j \in J$. Por lo tanto, los elementos $a_i b_j$ son linealmente independientes sobre K.

Ahora mostramos que los $a_i b_j$ generan a L sobre K. Si $x \in L$ entonces

$$x = \sum_j \lambda_j b_j$$

para ciertos $\lambda_j \in E$ y donde un número finito de los $b_j \in L$ no son nulos. De forma similar, para cada j tenemos

$$\lambda_j = \sum_i \lambda_{ij} a_i$$

para ciertos $\lambda_{ij} \in K$ y donde solo un número finitos de los a_i no son nulos. Así,

$$x = \sum_{i,j} \lambda_{ij} a_i b_j .$$

Por lo tanto, $\{a_i b_j : i \in I, j \in J\}$ es una base para L sobre K. Luego,

$$\begin{aligned} [L : K] &= \left|\{a_i b_j : i \in I, j \in J\}\right| \\ &= |\{a_i : i \in I\}| \cdot \left|\{b_j : j \in J\}\right| \\ &= [L : E]\,[E : K] . \end{aligned}$$

□

Un tipo de extensión de cuerpos que usaremos con frecuencia se obtiene adjuntando elementos, generalmente raíces de polinomios, a un cuerpo dado. Los cuerpos así obtenidos son llamados cuerpos generados.

Definición 1.3. Sea L una extensión de K y $S \subseteq L$. El cuerpo $K(S)$ generado por K y S es la intersección de todos los subcuerpos de L que contienen a K y a S. Si $S = \{\alpha_1, \alpha_2, ..., \alpha_n\}$ es finito, escribimos $K(S) = K(\alpha_1, \alpha_2, ..., \alpha_n)$ y diremos que el cuerpo $K(S)$ es *finitamente generado* por S.

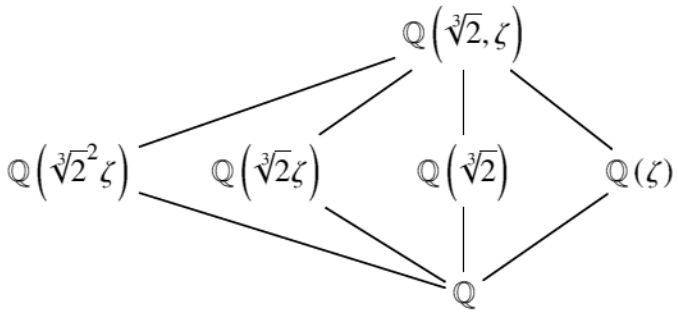
De la definición se deduce que $K(S)$ es el cuerpo más pequeño que contiene a K y a S, y que $K(S)$ es una extensión de K.

Ejemplo 1.2.

(i) Si al cuerpo $\mathbb{R}$ le adjuntamos el número imaginario i, donde $i^2 = -1$, entonces $\mathbb{R}(i)$ es una extensión de $\mathbb{R}$. Esta extensión es, precisamente, el cuerpo de números complejos.

(ii) Si $\zeta = \frac{-1+\sqrt{3}i}{2}$, los cuerpos $\mathbb{Q}\left(\sqrt[3]{2}^2\zeta\right)$, $\mathbb{Q}\left(\sqrt[3]{2}\zeta\right)$, $\mathbb{Q}\left(\sqrt[3]{2}\right)$ y $\mathbb{Q}(\zeta)$ son extensiones de $\mathbb{Q}$, y a su vez, $\mathbb{Q}\left(\sqrt[3]{2}, \zeta\right)$ es una extensión de todos los cuerpos anteriores. Indicamos las relaciones

entre ellos en el diagrama reticular:



Observación 1.2. Los siguientes resultados, que pueden consultarse en Morandi (1996), dan una descripción de los cuerpos generados.

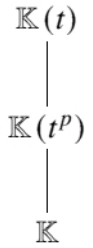
(i) Los cuerpos finitamente generados pueden ser descritos como cuerpos de cociente de anillos de polinomios. Si $\alpha_1,\alpha_2,...,\alpha_n$ son elementos de L, entonces $K(\alpha_1,\alpha_2,...,\alpha_n)$ es el conjunto

$$\left\{\frac{f(\alpha_1,...,\alpha_n)}{g(\alpha_1,...,\alpha_n)} \in L \mid f(x_1,...,x_n), g(x_1,...,x_n) \in K[x_1,...,x_n], g(\alpha_1,...,\alpha_n) \neq 0\right\}.$$

(ii) $K(S)$ es la unión de todos los cuerpos finitamente generados por subconjuntos finitos de S; es decir,

$$K(S) = \cup\{K(\alpha_1,\alpha_2,...,\alpha_n) \mid \alpha_1,\alpha_2,...,\alpha_n \in S\}.$$

Ejemplo 1.3. Sea p un número primo, t una indeterminada y $\mathbb{K} = \mathbb{Z}/p\mathbb{Z}$. Entonces $\mathbb{K}(t)$ y $\mathbb{K}(t^p)$ son extensiones de cuerpo de $\mathbb{K}$, relacionadas como sigue:



Definición 1.4. Se dice que un polinomio $f(x) \in K[x]$ es *reducible* sobre K si es el producto de dos polinomios de $K[x]$, de menor grado. En caso contrario, diremos que el polinomio $f(x)$ es *irreducible*.

Ejemplo 1.4.

(i) Todos los polinomios de grado uno son irreducibles, ya que no pueden expresarse como el producto de otros polinomios de menor grado.

(ii) Por el Criterio de Eisentein, el polinomio $x^2 - 5$ es irreducible sobre $\mathbb{Q}$. Sin embargo, $x^2 - 5$ no es irreducible sobre $\mathbb{R}$ puesto que

$$x^2 - 5 = \left(x + \sqrt{5}\right)\left(x - \sqrt{5}\right).$$

(iii) Sea t una indeterminada, p un número primo y $\mathbb{K} = \mathbb{Z}/p\mathbb{Z}$. Considere el polinomio $x^p - t^p$ en $\mathbb{K}(t^p)[x]$. Como la característica de $\mathbb{K}(t^p)$ es p, el polinomio $x^p - t^p$ se factoriza como $(x-t)^p$. Puesto que $t \notin \mathbb{K}_p(t^p)$, el polinomio $x^p - t^p$ es irreducible sobre $\mathbb{K}_p(t^p)$.

Definición 1.5. Un elemento $\alpha \in L$ es *algebraico sobre* K si existe un polinomio no nulo $f(x)$ en $K[x]$ tal que α es raíz de $f(x)$. La extensión L/K es algebraica si todos sus elementos son algebraicos sobre K. Un elemento $\alpha \in L$ que no es algebraico sobre K se dice que es *trascendente sobre* K.

Ejemplo 1.5.

(i) Sea $\alpha = 1 + i$. Tenemos que $\alpha - 1 = i$, de donde $(\alpha - 1)^2 = -1$, o sea, $\alpha^2 - 2\alpha + 2 = 0$. Luego, α es raíz de $f(x) = x^2 - 2x + 2 \in \mathbb{R}[x]$, lo cual implica que α es algebraico sobre $\mathbb{R}$.

(ii) Sea t una indeterminada, p un número primo y $\mathbb{K} = \mathbb{Z}/p\mathbb{Z}$. Como t es raíz del polinomio $x^p - t^p \in \mathbb{K}(t^p)[x]$, se tiene que $t \in \mathbb{K}(t)$ es algebraico sobre $\mathbb{K}(t^p)$.

(iii) En 1873 Hermite probó que el número e es trascendente sobre $\mathbb{Q}$ y, nueve años más tarde, Lindemann probó que π también lo es sobre $\mathbb{Q}$. La demostración de estos resultados no

es relevante para los fines de este trabajo, pero puede consultarse en Stewart (2015, pp. 285-291).

Observación 1.3.

(i) Es fácil comprobar que si L/K es una extensión algebraica y E es un cuerpo intermedio de la extensión ($K \subseteq E \subseteq L$), entonces, tanto L/E como E/K son extensiones algebraicas.

(ii) Dada la extensión L/K, si $S \subseteq L$ es un conjunto de elementos algebraicos sobre K, entonces $K(S)$ es una extensión algebraica de K. Las extensiones que se obtienen adjuntando al cuerpo dado las raíces de los polinomios dados en (i) y (ii) del ejemplo anterior son algebraicas. En cambio, las que se obtienen en (iii) son trascendentes.

En adelante, todas las extensiones consideradas serán algebraicas. Las extensiones de grado finito son de este tipo como lo muestra el siguiente teorema.

Teorema 1.3. *Toda extensión de grado finito es algebraica.*

Demostración. Sea L/K finita y $\alpha \in L$. Denotemos $n = [L : K] < \infty$. Entonces $\{1, \alpha, \alpha^2, ..., \alpha^n\}$ es un subconjunto de L con $n+1$ elementos. Como el grado de la extensión L/K es n, este conjunto no es linealmente independiente, por lo que existen $a_0, ..., a_n \in K$ no todos nulos tales que

$$a_0 + a_1\alpha + ... + a_n\alpha^n = 0.$$

Definamos

$$f(x) = a_0 + a_1x + ... + a_nx^n.$$

Entonces $f(x) \in K[x]$, con $f(\alpha) = 0$. Esto significa que α es algebraico sobre K. Por lo tanto, L/K es una extensión algebraica. □

Cabe señalar que la recíproca no es cierta. Por ejemplo, la extensión de los elementos algebraicos sobre $\mathbb{Q}$ es una extensión algebraica de grado infinito.

Teorema 1.4. *Sea L/K una extensión y $\alpha \in L$ algebraico sobre K. Entonces existe un único polinomio $p(x) \in K[x]$ que satisface las siguientes propiedades:*

i) *El coeficiente del término de mayor grado es* 1.

ii) $p(\alpha) = 0$.

iii) *El grado de $p(x)$ es mínimo entre todos los polinomios $q(x)$ en $K[x]$ para los cuales* $q(\alpha) = 0$.

Este polinomio $p(x)$ es irreducible sobre K. Cuando $q(x) \in K[x]$ satisface $q(\alpha) = 0$ entonces $p(x)$ divide a $q(x)$.

Demostración. Tomemos $p(x) \in K[x]$ de grado mínimo entre aquellos polinomios en $K[x]$ que satisfacen $p(\alpha) = 0$, además podemos asumir que el coeficiente del término de mayor grado de $p(x)$ es 1. Este polinomio satisface las tres propiedades dadas.

Ahora, si $p(x)$ se puede descomponer como producto de dos polinomios en $K[x]$, entonces α es raíz de uno de ellos, lo cual no puede ser porque $p(x)$ es de grado mínimo. Esto implica que $p(x)$ es irreducible sobre K. Además, si $q(x) \in K[x]$ satisface $q(\alpha) = 0$, al considerar el algoritmo de la división de $q(x)$ entre $p(x)$ podemos escribir

$$q(x) = f(x)\,p(x) + r(x), \quad \text{con } r(x) = 0 \text{ o } \deg r(x) < \deg p(x).$$

Entonces

$$r(\alpha) = q(\alpha) - f(\alpha)\,p(\alpha) = 0,$$

lo que no es posible si $\deg r(x) < \deg p(x)$, ya que contradice la minimalidad de $p(x)$.

Así se tiene que $r(x) = 0$. Por lo cual, $p(x)$ divide a $q(x)$. □

Definición 1.6. El polinomio descrito en el teorema anterior es llamado *polinomio mínimo de α sobre K* y se denota $\text{mín}(\alpha, K)$.

Ejemplo 1.6.

(i) $\sqrt{5}$ es raíz del polinomio x^2-5, el cual es irreducible sobre $\mathbb{Q}$. Así, $\text{mín}\left(\sqrt{5},\mathbb{Q}\right)=x^2-5$.

(ii) $\alpha=1+i$ es raíz del polinomio $x^2-2x+2\in\mathbb{R}[x]$, el cual es irreducible sobre $\mathbb{R}$ pues sus raíces no son reales. Así, $\text{mín}(\alpha,\mathbb{R})=x^2-2x+2$.

(iii) Sea $K=\mathbb{Q}(\pi)$. Entonces π es raíz de $x^2-\pi\in K[x]$, lo que muestra que π es algebraico sobre K y que $\text{mín}(\pi,K)$ tiene grado a lo sumo dos. Como $\mathbb{Q}(\pi)\cong\mathbb{Q}(y)$, donde y es una indeterminada, y $\sqrt{y}$ no está en $\mathbb{Q}(y)$, entonces $\sqrt{\pi}\notin\mathbb{Q}(\pi)$ y por lo tanto, $\text{mín}(\alpha,K)$ tiene grado mayor que 1. De esto se deduce que $\text{mín}(\alpha,F)$ tiene que ser $x^2-\pi$.

(iv) Sea t una indeterminada, p un número primo y $\mathbb{K}=\mathbb{Z}/p\mathbb{Z}$. Hemos determinado que el polinomio $x^p-t^p\in\mathbb{K}(t^p)[x]$ es irreducible sobre $\mathbb{K}(t^p)$. Por lo tanto, el polinomio mínimo $\text{mín}(t,\mathbb{K}(t^p))$ es x^p-t^p.

Las extensiones finitas son caracterizadas en términos de cuerpos finitamente generados como sigue.

Teorema 1.5. *La extensión L sobre K es de grado finito si y solo si L es algebraica y finitamente generada sobre K.*

Demostración. Supongamos que L/K es de grado finito. Ya se probó que toda extensión finita es algebraica. Sea $\{\alpha_1,\alpha_2,...,\alpha_n\}$ una base para L sobre K. Entonces todo elemento de L tiene la forma $\sum_i a_i\alpha_i$ donde $a_i\in K$, lo que significa que $L=K(\alpha_1,\alpha_2,...,\alpha_n)$. Así, L/K es algebraica y finitamente generada.

Recíprocamente, supongamos que L es algebraica sobre K y finitamente generada por $\{\alpha_1,\alpha_2,...,\alpha_n\}$. Como L/K es algebraica, cada α_i es algebraico sobre K y, por lo tanto, sobre todo cuerpo intermedio entre K y L. Así, $K(\alpha_1)$ es algebraica sobre K, $K(\alpha_1,\alpha_2)$ lo es sobre $K(\alpha_1)$, ..., y $K(\alpha_1,\alpha_2,...,\alpha_n)$ lo es sobre $K(\alpha_1,\alpha_2,...,\alpha_{n-1})$. Luego, al aplicar el Teorema de la Torre a la cadena de extensiones finita

$$K\subseteq K(\alpha_1)\subseteq...\subseteq K(\alpha_1,\alpha_2,...,\alpha_{n-1})\subseteq K(\alpha_1,\alpha_2,...,\alpha_n)$$

se tiene que

$$[L:K] = [K(\alpha_1,...,\alpha_n) : K(\alpha_1,...,\alpha_{n-1})] \cdot ... \cdot [K(\alpha_1,\alpha_2) : K(\alpha_1)] \cdot [K(\alpha_1) : K] < \infty,$$

lo que prueba que L/K es de grado finito. □

Observación 1.4. El cuerpo $K(\alpha)$ que se obtiene adjuntando a K una raíz del polinomio $p(x)$ en $K[x]$ es, por definición, el cuerpo más pequeño que contiene a K y a α. La extensión $K(\alpha)/K$ es algebraica de grado finito y su grado es el grado del polinomio mínimo de α sobre K. Además, si n es el grado de mín(α, K), una base para $K(\alpha)$ como K-espacio vectorial es $\{1, \alpha, ..., \alpha^{n-1}\}$.

Veamos un ejemplo de extensión algebraica, pero que no es finitamente generada. Este tipo de extensiones son de interés para este trabajo.

Ejemplo 1.7. Consideremos $S = \{\sqrt{p} \mid p \text{ primo}\}$ y sea $L = \mathbb{Q}(S)$ el cuerpo generado por los elementos de S sobre $\mathbb{Q}$. Entonces L es una extensión de $\mathbb{Q}$. Además, si $p_1, p_2, ..., p_n, ...$ es la lista de números primos, entonces para cada $n \in \mathbb{N}$ tenemos que

$$[L:\mathbb{Q}] \geq \left[\mathbb{Q}\left(\sqrt{p_1}, \sqrt{p_2}, ..., \sqrt{p_n}\right) : \mathbb{Q}\right] = 2^n,$$

lo que significa que $L/\mathbb{Q}$ es una extensión algebraica de grado infinito.

Definición 1.7. Un cuerpo K se dice *algebraicamente cerrado* si todo polinomio no constante de $K[x]$ tiene una raíz en K.

Equivalentemente, un cuerpo K se dice *algebraicamente cerrado* si todo polinomio no constante de $K[x]$ se puede descomponer como producto de factores lineales de $K[x]$.

Definición 1.8. Sea K un cuerpo. Llamamos *clausura algebraica* de K, y la representamos por $\overline{K}$, a una extensión algebraicamente cerrada de K.

Ejemplo 1.8. (i) $\overline{\mathbb{R}} = \mathbb{C}$; (ii) $\overline{\mathbb{C}} = \mathbb{C}$, y a este resultado se le conoce como Teorema Fundamental del Álgebra.

Supondremos siempre que las extensiones L/K están contenidas en la clausura algebraica de K.

1.2. Automorfismos de cuerpos

Definición 1.9. Sea L/K una extensión algebraica y sean $\alpha, \beta \in L$. Decimos que α y β son *conjugados* sobre K si son raíces del mismo polinomio irreducible sobre K.

Teorema 1.6. *Sean $\alpha, \beta \in L$ algebraicos sobre K y $n = \deg \min(\alpha, K)$. Entonces*

$$\psi_{\alpha,\beta} : K(\alpha) \to K(\beta)$$
$$a_0 + a_1\alpha + \ldots a_{n-1}\alpha^{n-1} \longmapsto a_0 + a_1\beta + \ldots + a_{n-1}\beta^{n-1}$$

es un isomorfismo si y solo si α y β son conjugados sobre K.

Definición 1.10. Sean L, K y M cuerpos.

(1) Un isomorfismo $\sigma : L \to L$ es llamado *automorfismo* de L.

(2) Si L y M son extensiones de un cuerpo K, $\sigma : L \to M$ es un $K-$*homomorfismo* si $\sigma(a) = a$ para todo $a \in K$. Si σ es biyectiva entonces σ es un K*-isomorfismo*. Y un K-isomorfismo de un cuerpo en sí mismo es un K*-automorfismo*.

Lo relevante de los $K-$homomorfismos de un cuerpo L es que "permutan" las raíces de los polinomios irreducibles de $K[x]$. Por ejemplo, la imagen del número complejo $\sqrt{3}i$ por medio de la conjugación compleja $z \mapsto \overline{z}$ (la cual es un $\mathbb{R}-$homomorfismo de $\mathbb{C}$) es $-\sqrt{3}i$. Este número es conjugado de $\sqrt{3}i$ sobre $\mathbb{R}$, puesto que ambos son raíces del polinomio irreducible $x^2 + 3 \in \mathbb{R}[x]$. Resaltamos este resultado en el siguiente teorema.

Teorema 1.7. *Sea $\tau : L \to M$ un K-homomorfismo. Entonces α y $\tau(\alpha)$ son conjugados sobre K.*

Demostración. Sea $f(x) = a_0 + a_1 x + ... + a_n x^n$ irreducible sobre K y $\alpha \in L$ una raíz de $f(x)$. Entonces,

$$\begin{aligned} 0 = \tau(0) = \tau(f(\alpha)) &= \tau(a_0 + a_1\alpha + ... + a_n\alpha^n) \\ &= \tau(a_0) + \tau(a_1)\tau(\alpha) + ... + \tau(a_n)\tau(\alpha)^n \end{aligned}$$

Como τ fija los elementos de $a_0, a_1, ..., a_n$ de K, se tiene

$$0 = a_0 + a_1\tau(\alpha) + ... + a_n\tau(\alpha)^n = f(\tau(\alpha)),$$

por lo que $\tau(\alpha)$ es también raíz de $f(x)$. □

El conjunto de todos los automorfismos de L con la operación de composición forma un grupo que se denota por $\mathrm{Aut}(L)$. El conjunto de todos los $K-$automorfismos de L, denotado por $\mathrm{Gal}(L/K)$, es un subgrupo $\mathrm{Aut}(L)$.

Definición 1.11. El conjunto

$$\mathrm{Gal}(L/K) = \{\sigma \in \mathrm{Aut}(L) \mid \sigma(a) = a, \text{ para todo } a \in K\}.$$

es el *grupo de Galois* de la extensión L/K.

Teorema 1.8. *Sea $L = K(S)$ una extensión de K generada por $S \subseteq L$. Si σ y τ son elementos del grupo de Galois* $\mathrm{Gal}(L/K)$ *tal que $\sigma|_S = \tau|_S$, entonces $\sigma = \tau$.*

Demostración. Sea $\alpha \in L$. De la Observación 1.2, existe un conjunto finito $\{\alpha_1, ..., \alpha_n\}$ de S tal que $\alpha \in K(\alpha_1, ..., \alpha_n)$ y, por consiguiente, polinomios f y g en $K[x_1, ...x_n]$ tales que

$$\alpha = \frac{f(\alpha_1, ..., \alpha_n)}{g(\alpha_1, ..., \alpha_n)}.$$

Escribamos

$$f(x_1,...,x_n) = \sum a_{i_1 i_2 ... i_n} x_1^{i_1} x_2^{i_2} ... x_n^{i_n}, \;\; g(x_1,...,x_n) = \sum b_{i_1 i_2 ... i_n} x_1^{i_1} x_2^{i_2} ... x_n^{i_n},$$

donde los coeficientes están en K. Como σ y τ son automorfismos de L que fijan los elementos de K, tenemos

$$\begin{aligned}\sigma(\alpha) &= \sum \frac{a_{i_1 i_2 ... i_n} \sigma(\alpha_1)^{i_1} ... \sigma(\alpha_n)^{i_n}}{b_{i_1 i_2 ... i_n} \sigma(\alpha_1)^{i_1} ... \sigma(\alpha_n)^{i_n}} \\ &= \sum \frac{a_{i_1 i_2 ... i_n} \tau(\alpha_1)^{i_1} ... \tau(\alpha_n)^{i_n}}{b_{i_1 i_2 ... i_n} \tau(\alpha_1)^{i_1} ... \tau(\alpha_n)^{i_n}} \\ &= \tau(\alpha).\end{aligned}$$

Por lo tanto, $\sigma = \tau$. □

El teorema anterior indica que cuando $L = K(S)$, donde $S \subseteq L$, los $K-$automorfismos de L están determinados por su acción sobre el conjunto generador S. En particular, si la extensión L/K está generada por las raíces de un polinomio, el grupo de Galois se puede interpretar, como lo fue originalmente descrito por el propio E. Galois, como el grupo de permutaciones de las raíces del polinomio. Como consecuencia del teorema, se tiene el siguiente corolario.

Corolario 1.1. *Si* $[L : K]$ *es finito entonces* $\mathrm{Gal}(L/K)$ *es finito.*

Demostración. Como $[L : K]$ es finito, la extensión L/K es finitamente generada; digamos, $L = K(\alpha_1,...,\alpha_n)$. Como los $K-$automorfismos de L están determinados por su acción sobre el conjunto generador $\{\alpha_1,...,\alpha_n\}$, existe una cantidad finita de posibilidades para la imagen de cada α_i; por lo tanto existe una cantidad finita de $K-$automorfismos de L. □

Ejemplo 1.9. Consideremos el cuerpo $L = \mathbb{Q}\left(i, \sqrt{3}, \sqrt{5}\right)$. Entonces $L/\mathbb{Q}$ es una extensión de grado finito. Por otro lado, un automorfismo $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$ está completamente determinado por sus valores sobre $\sqrt{3}$, $\sqrt{5}$ e i. Es fácil comprobar que σ deja fijo este valor o lo aplica sobre

su opuesto. Así, hay dos posibilidades para $\sigma\left(\sqrt{3}\right)$, dos para $\sigma\left(\sqrt{5}\right)$ y dos para $\sigma(i)$. Por lo que hay a lo sumo $2 \cdot 2 \cdot 2 = 8$ automorfismos en total. Concluimos que $\mathrm{Gal}(L/\mathbb{Q})$ es de grado finito.

A partir de una colección de automorfismos de L podemos construir subcuerpos de L de la siguiente forma: Sea S una colección de automorfismos de L; el conjunto

$$\mathcal{F}(S) = \{\alpha \in L \mid \sigma(\alpha) = \alpha, \text{ para todo } \sigma \in S\},$$

de los elementos de L que quedan fijos por todos elementos de S es un subcuerpo de L. A este cuerpo lo llamamos *cuerpo fijo* de S.

Teorema 1.9. *Sea L/K una extensión de cuerpos.*

(1) *Si E es un subcuerpo de L entonces* $\mathrm{Gal}(L/E)$ *es un subgrupo de* $\mathrm{Gal}(L/K)$.

(2) $\mathcal{F}(\mathrm{Gal}(L/E))$ *es una extensión de E.*

(3) *Si E_1, E_2 son subcuerpos de L, con $E_1 \subseteq E_2$, entonces* $\mathrm{Gal}(L/E_2) \subseteq \mathrm{Gal}(L/E_1)$.

(4) *Si S_1 y S_2 son subconjuntos de* $\mathrm{Aut}(L)$*, con $S_1 \subseteq S_2$, entonces $\mathcal{F}(S_2) \subseteq \mathcal{F}(S_1)$.*

Demostración. (1) Sean $\sigma, \tau \in \mathrm{Gal}(L/E)$. Para cualquier $\alpha \in L$, $\sigma\tau(\alpha) = \sigma(\alpha) = \alpha$; además, $\sigma(\alpha) = \alpha$ implica $\sigma^{-1}\sigma(\alpha) = \sigma^{-1}(\alpha)$, luego, $\alpha = \sigma^{-1}(\alpha)$. En consecuencia, tanto $\sigma\tau$ como σ^{-1} están en $\mathrm{Gal}(L/E)$, lo que prueba que $\mathrm{Gal}(L/E)$ es un subgrupo de $\mathrm{Gal}(L/K)$.
(2) Los elementos de $\mathcal{F}(\mathrm{Gal}(L/E))$ son los elementos de L que quedan fijos por los automorfismos de $\mathrm{Gal}(L/E)$, y éstos dejan fijos, por definición, los elementos de E.
(3) Sea $\sigma \in \mathrm{Gal}(L/E_2)$. Entonces σ deja fijo los elementos de E_2 y como $E_1 \subseteq E_2$, σ también deja fijo los elementos de E_1; es decir, $\sigma \in \mathrm{Gal}(L/E_1)$, lo que prueba la inclusión.
(4) Sea $\alpha \in \mathcal{F}(S_2)$. Entonces α es fijado por todos los automorfismos de S_2 y como $S_1 \subseteq S_2$, α también es fijado por todos los automorfismos de S_1; esto es, $\alpha \in \mathcal{F}(S_1)$, lo que prueba la inclusión. □

Los dos últimos teoremas de esta sección hacen referencia a propiedades respecto al orden del grupo de Galois y el grado de la extensión. El Teorema 1.10 da una cota superior para el número de $K-$automorfismos de una extensión L de grado finito y el Teorema 1.11 determina cuándo el orden de un grupo de Galois finito es igual al grado de la extensión. La demostración utiliza el Lema de Dedekind, resultado descubierto por Dedekind a finales de siglo XIX e inadvertido por muchos años.

Lema 1.1 (Dedekind)**.** *Sea G un grupo y L un cuerpo. Si $\tau_1, \tau_2, ..., \tau_n$ son homomorfismos distintos de G en el grupo multiplicativo L^*, entonces los τ_i son linealmente independientes sobre L.*

Demostración. Supongamos que el lema es falso. Reordenando los τ_i (si es necesario), sea k el mínimo subíndice para el cual los $\tau_1, ...\tau_k$ son linealmente dependientes sobre L; es decir k es el mínimo subíndice para el cual existen $c_1, c_2, ..., c_k$ en L, no todos nulos, tal que

$$\sum_{i=1}^{k} c_i \tau_i (g) = 0, \quad \text{para todo } g \in G.$$

La elección de k implica que cada uno de los c_i es distinto de 0. Como $\tau_1 \neq \tau_2$, existe algún elemento h en G tal que $\tau_1 (h) \neq \tau_2 (h)$. Se ve fácilmente que

$$\sum_{i=1}^{k} (c_i \tau_1 (h)) \tau_i (g) = 0, \quad \text{para todo } g \in G. \tag{1.2.1}$$

Además,

$$0 = \sum_{i=1}^{k} c_i \tau_i (hg) = \sum_{i=1}^{k} (c_i \tau_i (h)) \tau_i (g), \quad \text{para todo } g \in G. \tag{1.2.2}$$

Restando (1.2.1) y (1.2.2) tenemos,

$$\begin{aligned} 0 &= \sum_{i=1}^{k} \left(c_i \tau_1(h)\right) \tau_i(g) - \sum_{i=1}^{k} \left(c_i \tau_i(h)\right) \tau_i(g) \\ &= \sum_{i=1}^{k} \left(c_i \tau_1(h) - c_i \tau_i(h)\right) \tau_i(g) \\ &= \sum_{i=2}^{k} \left(c_i \tau_1(h) - c_i \tau_i(h)\right) \tau_i(g). \end{aligned}$$

Esta expresión involucra $k-1$ de los τ_i, con no todos los coeficientes nulos ya que al menos $c_2\tau_1(h) - c_2\tau_2(h) \neq 0$. Esto contradice la elección de k y prueba el lema. □

Teorema 1.10. *Si L/K es de grado finito entonces* $|\mathrm{Gal}(L/K)| \leq [L:K]$.

Demostración. Sea $n = [L:K]$. Por reducción al absurdo, supongamos que $|\mathrm{Gal}(L/K)| > n$. Sea $\mathrm{Gal}(L/K) = \{\sigma_1, ..., \sigma_m\}$, con $m > n$, y $\{\alpha_1, ...\alpha_n\}$ una base para L como $K-$espacio vectorial. Considere el sistema

$$\begin{aligned} \sigma_1(\alpha_1)x_1 + \sigma_2(\alpha_1)x_2 + ... + \sigma_n(\alpha_1)x_m &= 0 \\ \sigma_1(\alpha_2)x_1 + \sigma_2(\alpha_2)x_2 + ... + \sigma_n(\alpha_2)x_m &= 0 \\ &\vdots \\ \sigma_1(\alpha_n)x_1 + \sigma_2(\alpha_n)x_2 + ... + \sigma_n(\alpha_n)x_m &= 0 \end{aligned}$$

de n ecuaciones lineales homogéneas en m variables $x_1, x_2, ...x_m$ con coeficientes en L. Como $m > n$, el sistema tiene una solución no trivial $(\beta_1, \beta_2, ..., \beta_m)$, donde cada β_i está en L. Luego, sustituyendo en el sistema anterior, se tiene que para todo j,

$$\sum_{i=1}^{m} \beta_i \sigma_i\left(\alpha_j\right) = 0.$$

Tomemos $G = L^*$ como en el Lema de Dedekind. Entonces $\sigma_1, ..., \sigma_m$ son homomorfismos distintos de G en L^*. Además, todo elemento de G se escribe como combinación lineal de los

α_j; así, para todo g en G tenemos

$$g = \sum_{j=1}^{n} c_j \alpha_j, \text{ donde } c_j \in K.$$

Luego, para todo g en G se cumple

$$\begin{aligned}\sum_{i=1}^{m} \beta_i \sigma_i(g) &= \sum_{i=1}^{m} \beta_i \sigma_i \left(\sum_{j=1}^{n} c_j \alpha_j \right) \\ &= \sum_{i=1}^{m} \beta_i \left(\sum_{j=1}^{n} c_j \sigma_i(\alpha_j) \right) \\ &= \sum_{j=1}^{n} c_j \left(\sum_{j=1}^{n} \beta_i \sigma_i(\alpha_j) \right) \\ &= \sum_{j=1}^{n} c_j(0) = 0,\end{aligned}$$

lo que contradice el Lema de Dedekind ya que no todos los β_i son 0. □

Teorema 1.11 (Artin)**.** *Sea G un grupo finito de automorfismos de L. Entonces $|G| = [L : \mathcal{F}(G)]$ y así $G = \mathrm{Gal}(L/\mathcal{F}(G))$.*

Demostración. Primero probemos que $[L : \mathcal{F}(G)] \leq |G|$. Sea $G = \{\sigma_1 = \mathrm{id}, \sigma_2, ..., \sigma_m\}$. Es suficiente probar que todo conjunto $\{\alpha_1, ...\alpha_n\}$ de elementos de L, con $n > m$, es linealmente dependiente sobre $\mathcal{F}(G)$. Para esos conjuntos, considere el sistema de ecuaciones lineales homogéneas

$$\begin{aligned}\sigma_1(\alpha_1)x_1 + \sigma_1(\alpha_2)x_2 + ... + \sigma_1(\alpha_n)x_n &= 0 \\ \sigma_2(\alpha_1)x_1 + \sigma_2(\alpha_2)x_2 + ... + \sigma_2(\alpha_n)x_n &= 0 \\ &\vdots \\ \sigma_m(\alpha_1)x_1 + \sigma_m(\alpha_2)x_2 + ... + \sigma_m(\alpha_n)x_n &= 0\end{aligned}$$

con coeficientes en L. Como $n > m$, el sistema tiene una solución no trivial en L. Elijamos una

solución $(\beta_1, ..., \beta_m)$ que tenga la menor cantidad posible de elementos distintos de 0.

Reordenando los α_i's (si es necesario), supongamos que $\beta_1 \neq 0$; además, al multiplicar convenientemente por un escalar, podemos suponer que $\beta_1 \in \mathcal{F}(G)$. Mostraremos entonces que todos los β_i están en $\mathcal{F}(G)$. Como $\sigma_1 = \text{id}$, en la primera ecuación se tiene

$$\alpha_1\beta_1 + \alpha_2\beta_2 + ... + \alpha_n\beta_n = 0.$$

Si no todos los β_i están en $\mathcal{F}(G)$, entonces $\sigma_k(\beta_i) \neq \beta_i$ para algún $k \neq 1$ e $i \neq 1$. Aplicando σ_k a las ecuaciones

$$\begin{aligned}
\sigma_1(\alpha_1)\beta_1 + \sigma_1(\alpha_2)\beta_2 + ... + \sigma_1(\alpha_n)\beta_n &= 0 \\
\sigma_2(\alpha_1)\beta_1 + \sigma_2(\alpha_2)\beta_2 + ... + \sigma_2(\alpha_n)\beta_n &= 0 \\
&\vdots \\
\sigma_m(\alpha_1)\beta_1 + \sigma_m(\alpha_2)\beta_2 + ... + \sigma_m(\alpha_n)\beta_n &= 0
\end{aligned}$$

y usando que $\{\sigma_k\sigma_1, ...\sigma_k\sigma_m\}$ es una permutación de $\{\sigma_1, \sigma_2, ..., \sigma_m\}$, tenemos que

$$(\beta_1, \sigma_k(\beta_2), ..., \sigma_k(\beta_i), ...)$$

es también una solución del sistema de ecuaciones. Restando ambas soluciones, obtenemos una solución

$$(0, ..., \beta_i - \sigma_k(\beta_i), ...),$$

la cual es no trivial ya que $\sigma_k(\beta_i) \neq \beta_i$ y distinta de la primera, pero que tiene más ceros que la primera solución (basta observar la primera coordenada). Esto contradice la elección de $(\beta_1, ..., \beta_m)$ como la solución con la menor cantidad posible de elementos distintos de 0. Por lo tanto,

$$[L : \mathcal{F}(G)] \leq m = |G|.$$

Finalmente, como $G \subseteq \mathrm{Gal}\,(L/\mathcal{F}\,(G))$, esta desigualdad y el teorema anterior implican que

$$[L : \mathcal{F}\,(G)] \leq |G| \leq |\mathrm{Gal}\,(L/\mathcal{F}\,(G))| \leq [L : \mathcal{F}\,(G)]\,,$$

lo cual prueba el teorema: $|G| = [L : \mathcal{F}\,(G)]$ y $G = \mathrm{Gal}\,(L/\mathcal{F}\,(G))$. □

1.3. Extensiones de Galois

Definición 1.12. Se dice que la extensión L/K es *normal* si para todo $\alpha \in L$, el polinomio mínimo de α sobre K se descompone en factores lineales sobre L.

Ejemplo 1.10. Por el Teorema Fundamental del Álgebra, la extensión $\mathbb{C}/\mathbb{R}$ es normal.

Definición 1.13. Sea L/K una extensión.

(1) Si $f\,(x) \in K\,[x]$, L es un cuerpo de descomposición de f sobre K si $f\,(x)$ se descompone sobre L y L está generado por las raíces de $f\,(x)$.

(2) Si S es una colección de polinomios no constantes sobre K, entonces L es el cuerpo de descomposición de S sobre K si cada $f \in S$ se descompone sobre L y $L = K\,(X)$, donde X es el conjunto formado por todas las raíces de todos los polinomios en S.

Los siguientes dos teoremas establecen la existencia de cuerpos de descomposición para un polinomio y una famila de polinomios.

Teorema 1.12 (Kronecker)**.** *Sea $f\,(x) \in K\,[x]$ con grado $n \geq 1$. Entonces existe una extensión E de K, con $[E : K] \leq n$, en la que f tiene una raíz. Además, existe un cuerpo L que contiene a E, con $[L : K] \leq n!$, el cual es un cuerpo de descomposición de $f\,(x)$.*

Demostración. Sea $p\,(x)$ un factor irreducible de $f\,(x)$ en $K\,[x]$. Entonces $\langle f\,(x)\rangle = \langle p\,(x)\rangle$, y este ideal es un ideal maximal de $K\,[x]$, lo cual implica que el cociente $L : K\,[x]\,/\langle p\,(x)\rangle$ es un

cuerpo. Considere la aplicación

$$\phi : K \to L$$
$$a \to \overline{a}$$

Esta es un monomorfismo, por lo que L es una extensión de K. Llamemos $\alpha = \overline{x}$ y consideremos el homomorfismo evaluación $\Phi_\alpha : K[x] \to L$. Entonces

$$p(\alpha) = \Phi_\alpha p(x) = \overline{p(x)} = \overline{0},$$

lo que prueba que α es una raíz de $f(x)$. Además, $[E : K] = \deg p(x) \leq n$.

Para la segunda parte procedemos por inducción sobre n:

Si $n = 1$ entonces $K(\alpha)$, donde α la única raíz de $f(x)$, es un cuerpo de descomposición de $f(x)$.

Asumamos como hipótesis inductiva que todo polinomio de grado menor que n tiene un cuerpo de descomposición con las propiedades en cuestión. Para un polinomio $f(x)$ de grado n sabemos que existe una extensión E de K, con $[E : K] \leq n$, en la que f tiene una raíz α. Luego podemos escribir

$$f(x) = (x - \alpha) \cdot g(x), \text{ con } g(x) \in E[x].$$

Ya que el grado de $g(x)$ es $n-1$, por hipótesis inductiva, existe un cuerpo L que contiene a E, con $[L : E] \leq (n-1)!$, el cual es un cuerpo de descomposición de $g(x)$. Luego, L es un cuerpo de descomposición de $f(x)$ y

$$[L : K] = [L : E][E : K] \leq (n-1)! \cdot n = n!,$$

lo que prueba el teorema. □

Utilizando el Lema de Zorn se llega a la existencia de la clausura algebraica de un cuerpo.

Teorema 1.13. *Sea K un cuerpo. Entonces K tiene una clausura algebraica.*

Y como corolario se deduce con facilidad la existencia de un cuerpo de descomposición para una familia de polinomios.

Corolario 1.2. *Sea S una familia de polinomios sobre K. Entonces S tiene un cuerpo de descomposición sobre K. Además, el cuerpo de descomposición de todos los polinomios no constantes sobre K es una clausura algebraica de K.*

El próximo teorema, en cuya demostración se usa el Lema de Zorn, es de utilidad para construir automorfismos de un cuerpo y para calcular el grupo de Galois de una extensión.

Teorema 1.14 (Teorema de Extensión de Isomorfismos)**.** *Sea $\sigma : E \to E'$ un isomorfismo de cuerpos, $S = \{f_i(x)\}_{i\in I}$ una familia de polinomios en $E[x]$ y $S' = \{\sigma(f_i(x))\}_{i\in I} \subseteq E'[x]$ la imagen de S bajo σ. Sea L el cuerpo de descomposición de S sobre E; L' el cuerpo de descomposición de S' sobre E'. Entonces existe un isomorfismo $\tau : L \to L'$ tal que $\tau|_E = \sigma$. Además, si $\alpha \in L$ y β es una raíz de $\sigma(\min(\alpha, E))$ entonces τ se puede elegir de tal forma que $\tau(\alpha) = \beta$.*

Demostración. Para una demostración, se recomienda consultar el Teorema 3.20 en Morandi (1996). □

Observación 1.5. El modo en que se usa el teorema de extensión es el siguiente: tendremos $E = E'$, $L = L'$ y E es una extensión de Galois de otro cuerpo K, $\sigma \in \mathrm{Gal}(E/K)$. Entonces el teorema garantiza que L es una extensión de Galois de K, con $K \subseteq E \subseteq L$ y que existe $\tau \in \mathrm{Gal}(L/K)$ que extiende σ a todo L.

El siguiente teorema proporciona enunciados equivalentes a la definición de extensión normal.

Teorema 1.15. *Sea L/K una extensión algebraica y sea $\overline{K}$ la clausura algebraica de K (luego, $L \subseteq \overline{K}$). Entonces son equivalentes:*

(1) *L/K es una extensión normal;*

(2) *L es el cuerpo de descomposición de una familia de polinomios $\{f_i(x)\}_{i\in I}$, donde I es un conjunto de índices arbitrario y cada $f_i(x) \in K[x]$;*

(3) *Todo K-homomorfismo $\sigma : L \hookrightarrow \overline{K}$ induce un K-automorfismo de L.*

Demostración. Supongamos (1). Considere la familia de polinomios $S = \{\text{mín}(\alpha, K) \mid \alpha \in L\}$ en $K[x]$ y sea X el conjunto formados por las raíces de todos los polinomios de S. La normalidad de L/K implica que cada polinomio de S se descompone en factores lineales sobre L y que $L \subseteq K(X)$. Así, $L = K(X)$. Esto prueba (2).

Supongamos (2). Sea $\sigma : L \hookrightarrow \overline{K}$ un K-homomorfismo. Si $\alpha \in L$ es una raíz de algún $f_i(x)$ entonces $\sigma(\alpha)$ también es una raíz de $f_i(x)$ puesto que σ es inyectiva. Como L está generado por las raíces de los polinomios de la familia $\{f_i(x)\}_{i\in I}$, se tiene que σ aplica L sobre sí mismo; es decir, $\sigma(L) \subseteq L$. Solo falta probar que $L \subseteq \sigma(L)$. Para ello, sea $\alpha \in L$ y E el cuerpo generado por las raíces de $\text{mín}(\alpha, K)$ que están en L. Entonces $E \subseteq L$ y E/K es de grado finito. Además, como σ aplica raíces de $\text{mín}(\alpha, K)$ en raíces de $\text{mín}(\alpha, K)$, se tiene que σ aplica E sobre sí mismo. Ahora, al considerar E como espacio vectorial sobre K, σ es un homomorfismo de espacios vectoriales que deja fijo los elementos de K. Luego, como σ es inyectiva, su imagen $\sigma(E)$ es un subespacio de E que tiene la misma dimensión que E. Al ser E de dimensión finita sobre K, se tiene $\sigma(E) = E$. Como $\alpha \in E \subseteq L$, entonces su imagen, $\sigma(\alpha)$, también está en $E \subseteq L$. Esto prueba (3).

Supongamos finalmente (3). Sea $\alpha \in L$ y $p(x) = \text{mín}(\alpha, K)$. Sea β una raíz de $p(x)$ en $\overline{K}$. Entonces existe un K-isomorfismo de $K(\alpha)$ en $K(\beta)$ que aplica α en β. Extendemos este isomorfismo a un K-homomorfismo $\sigma : L \hookrightarrow \overline{K}$, el cual induce un K-automorfismo de L. Por lo

tanto, $\sigma(\alpha) = \beta \in L$. Así, todas las raíces de $p(x)$ están en L y por tanto, $p(x)$ se descompone en factores lineales sobre L. Esto prueba (1). □

Ejemplo 1.11.

(i) Al cuerpo de descomposición de $x^n - 1$ sobre K se le llama extensión ciclotómica n-ésima del cuerpo K. Si $K = \mathbb{Q}$ entonces $\zeta = \cos\left(\frac{2\pi}{n}\right) + i\sin\left(\frac{2\pi}{n}\right) \in \mathbb{C}$ es raíz de $x^n - 1$ y el cuerpo de descomposición de $x^n - 1$ sobre $\mathbb{Q}$ es $\mathbb{Q}(\zeta)$. Por tanto, $\mathbb{Q}(\zeta)/\mathbb{Q}$ es normal.

(ii) Sea p un número primo. Un cuerpo finito de p^n elementos es (salvo isomorfismos) el cuerpo de descomposición del polinomio $x^{p^n} - 1$ sobre $\mathbb{Z}/p\mathbb{Z}$.

Definición 1.14. Sea K un cuerpo.

(1) Un polinomio irreducible $p(x) \in K[x]$ es *separable* sobre K, si no tiene raíces repetidas en cualquier cuerpo de descomposición.

(2) Un polinomio $f(x) \in K[x]$ es *separable* sobre K, si todos sus factores irreducibles son separables sobre K.

Algunas propiedades que se deducen inmediatamente es que el producto finito de polinomios separables es separable y que un polinomio separable lo es también sobre cualquier extensión de K.

Ejemplo 1.12. Veamos algunos ejemplos de polinomios separables.

(i) El polinomio $f(x) = x^2 - 7$ es irreducible sobre $\mathbb{Q}$ y sus dos raíces son distintas, por lo que es un polinomio separable sobre $\mathbb{Q}$.

(ii) El polinomio $f(x) = \left(x^2 - 3\right)\left(x^2 - 5\right)$ es separable sobre $\mathbb{Q}$ ya que sus factores irreducibles, $x^2 - 3$ y $x^2 - 5$, son separables sobre $\mathbb{Q}$.

(iii) El polinomio $x^2 + x + 1$ es irreducible sobre $\mathbb{F}_2$ ya que no tiene raíces en $\mathbb{F}_2$. Si α es una raíz de este polinomio, es fácil comprobar que $1 + \alpha$ es la otra raíz del polinomio. Por tanto, $x^2 + x + 1$ es separable sobre $\mathbb{F}_2$ ya que sus dos raíces son distintas.

Ejemplo 1.13. Considere $\mathbb{F}_2(t)$, el cuerpo de funciones racionales en una variable. El polinomio $x^2 - t^2$ es irreducible sobre $\mathbb{F}_2(t^2)$. Como $x^2 - t^2 = (x-t)^2$ sobre $\mathbb{F}_2(t)$, el polinomio tiene una única raíz, t, en su cuerpo de descomposición $\mathbb{F}_2(t)$. Por lo tanto, $x^2 - t^2$ no es separable sobre $\mathbb{F}_2(t^2)$.

Definición 1.15. Sea L una extensión de K.

(1) Se dice que $\alpha \in L$ es *separable* sobre K si su polinomio mínimo sobre K es separable sobre K.

(2) La extensión L/K es *separable* si todo $\alpha \in L$ es separable sobre K.

Teorema 1.16. *Si K es un cuerpo de característica 0 o un número primo, todas sus extensiones son separables.*

Ejemplo 1.14. Todas las extensiones de $\mathbb{Q}$ y $\mathbb{F}_p$ son separables.

Definición 1.16. Una extensión L/K es una *extensión de Galois* si es normal y separable.

Observación 1.6. Es decir, que para que una extensión L/K sea de Galois se debe cumplir: para todo $\alpha \in L$, si n es el grado del polinomio mínimo de α sobre K, entonces $\text{mín}(\alpha, K)$ se descompone sobre $L[x]$ en n factores lineales distintos o, equivalentemente, $\text{mín}(\alpha, K)$ tiene n raíces distintas en L.

Son enunciados equivalentes a la definición de extensión de Galois los siguientes.

Teorema 1.17. *Sea L/K una extensión algebraica. Son equivalentes:*

(1) *L/K es una extensión de Galois.*

(2) $\mathcal{F}(\text{Gal}(L/K)) = K$.

Si además L/K es de grado finito, entonces (1) y (2) son equivalentes a

(3) $|\text{Gal}(L/K)| = [L : K]$.

Demostración. Supongamos que L/K es una extensión de Galois. Sea $\alpha \in \mathcal{F}(\mathrm{Gal}(L/K))$. Si $\beta \in L$ es una raíz de $\mathrm{mín}(\alpha, K)$, existe un K-isomorfismo de $K(\alpha)$ en $K(\beta)$ que aplica α en β; éste se puede extender a un K-automorfismo de L, digamos τ, con $\tau(\alpha) = \beta$; pero como $\alpha \in \mathcal{F}(\mathrm{Gal}(L/K))$ se tiene que $\alpha = \beta$ por lo que α es la única raíz de $\mathrm{mín}(\alpha, K)$. Como L/K es de Galois se deduce que $\mathrm{mín}(\alpha, K) = x - \alpha$. Por lo tanto, $\alpha \in K$ y $\mathcal{F}(\mathrm{Gal}(L/K)) \subseteq K$. Así, $\mathcal{F}(\mathrm{Gal}(L/K)) = K$.

Recíprocamente, supongamos que $\mathcal{F}(\mathrm{Gal}(L/K)) = K$. Sea $\alpha \in L$. Como para cada σ en $\mathrm{Gal}(L/K)$, $\sigma(\alpha)$ es una raíz de $\mathrm{mín}(\alpha, K)$, el conjunto

$$\{\sigma(\alpha) \mid \sigma \in \mathrm{Gal}(L/K)\}$$

es finito. Sean $\alpha_1, \alpha_2, ..., \alpha_n$ sus elementos distintos y

$$f(x) = \prod (x - \alpha_i) \in L[x].$$

Entonces $\tau(f) = f$ ya que τ permuta los α_i. Así, los coeficientes de f están en $\mathcal{F}(\mathrm{Gal}(L/K)) = K$, de modo que $f(x) \in K[x]$. Por lo tanto, $\mathrm{mín}(\alpha, K)$ divide a $f(x)$, y así $\mathrm{mín}(\alpha, K)$ se descompone sobre L y no tiene raíces repetidas. Por lo tanto, L/K es normal y separable.

Por lo tanto, (1) y (2) son equivalentes.

Por otro lado, cuando L/K es de grado finito, $\mathrm{Gal}(L/K)$ es finito. Además, $[L : \mathcal{F}(\mathrm{Gal}(L/K))] = |\mathrm{Gal}(L/K)|$.

Si $|\mathrm{Gal}(L/K)| = [L : K]$, por el Teorema de la Torre se tiene

$$\begin{aligned}[L : K] &= [L : \mathcal{F}(\mathrm{Gal}(L/K))]\,[\mathcal{F}(\mathrm{Gal}(L/K)) : K] \\ &= [L : K]\,[\mathcal{F}(\mathrm{Gal}(L/K)) : K],\end{aligned}$$

de donde se tiene que $[\mathcal{F}(\mathrm{Gal}(L/K)) : K] = 1$ y por lo tanto, se obtiene (2): $\mathcal{F}(\mathrm{Gal}(L/K)) = K$.

Recíprocamente, si $\mathcal{F}(\mathrm{Gal}(L/K)) = K$ entonces se obtiene (3):

$$[L : K] = [L : \mathcal{F}(\mathrm{Gal}(L/K))] = |\mathrm{Gal}(L/K)|,$$

lo que muestra la equivalencia entre (2) y (3) para cuando L/K es de grado finito. □

Teorema 1.18. *Una extensión L/K es de Galois si y sólo si es la unión de extensiones de Galois finitas.*

Demostración. Supongamos que L/K es de Galois. Sea $\alpha \in L$ y $p(x) = \mathrm{mín}(\alpha, K)$ de grado n. Entonces $p(x)$ tiene n raíces distintas en L. Denotemos por F_α el subcuerpo de L generado por las raíces de $p(x)$. Entonces:

1) La extensión F_α/F es normal y finita ya que es un cuerpo de descomposición de un polinomio de $K[x]$; y

2) F_α/F es separable ya que L/K lo es. Luego, $L \subseteq \cup F_\alpha$, donde F_α/F es de Galois y finita.

Por otro lado, es claro que $\cup F_\alpha \subseteq L$. Esto prueba que L/K es la unión de extensiones de Galois finitas.

Recíprocamente, si $L = \cup F_i$, con F_i/F finita y de Galois, entonces dado $\alpha \in L$, existe F_{i_0} tal que $p(x) = \mathrm{mín}(\alpha, K)$ se descompone en $F_{i_0}[x]$ en factores lineales distintos, y por lo tanto, también en $L[x]$. Esto implica que L/K es de Galois. □

La importancia de este teorema es que permitirá construir las extensiones de Galois de grado infinito a partir de extensiones de Galois de grado finito, para las cuales se conocen muchas propiedades.

Teorema 1.19. *Si L/K es de Galois y E es un subcuerpo de L que contiene a K entones L/E es de Galois.*

Demostración. El cuerpo L es el cuerpo de descomposicíón de una familia de polinomios separables de $K[x]$; éstos también son una familia de polinomios separables en $E[x]$ cuyo cuerpo de descomposición es L, lo que prueba que L/E es de Galois. □

Teorema 1.20. *Sean E_1, E_2 extensiones de Galois de K. Entonces E_2E_1/K es de Galois. Si además, $E_1/K, E_2/K$ son de grado finito entonces E_2E_1/K también lo es.*

Demostración. Existen dos familias de polinomios separables $\{f_i\}, \{g_j\} \subseteq K[x]$ que son el cuerpo de descomposición de E_1 y E_2, respectivamente. Sean

$$E_1 = K(X) \text{ y } E_2 = K(Y),$$

donde X e Y son el conjunto de raíces de las familias dadas, respectivamente. La familia de polinomios $\{f_i g_j\} \subseteq K[x]$ es separable. El cuerpo E_2E_1 es el cuerpo más pequeño que contiene a E_2 y E_1; luego, es el cuerpo más pequeño que contiene a K y a $X \cup Y$, lo que implica que $E_2E_1 = K(X \cup Y)$ y éste es el cuerpo de descomposición de la familia de polinomios separables $\{f_i g_j\} \subseteq K[x]$. Por lo tanto, E_2E_1/K es de Galois.

Por otro lado, si $E_1/K, E_2/K$ son de grado finito entonces E_1, E_2 son cuerpos finitamente generados por lo que X, Y y $X \cup Y$ son conjuntos finitos. Por lo tanto, E_2E_1 es finitamente generado, lo que significa que E_2E_1/K es de grado finito. □

1.4. Correspondencia de Galois en grado finito

En esta sección se prueba el Teorema Fundamental de la Teoría de Galois. El resultado establece que cuando L/K es una extensión normal y separable, de grado finito, existe una correspondencia uno a uno entre todos los subgrupos del grupo de Galois $\mathrm{Gal}(L/K)$ y todos los subcuerpos intermedios de la extensión L/K. Tal correspondencia se establece como sigue: A cada subcuerpo intermedio E de L asociamos el subgrupo de $\mathrm{Gal}(L/K)$ formado por todos los automorfismos de L que fijan E. Y recíprocamente, a cada subgrupo H de $\mathrm{Gal}(L/K)$ asociamos el subcuerpo intermedio de elementos de L que quedan fijos por los automorfismos de H.

Teorema 1.21 (Teorema Fundamental de la Teoría de Galois finita)**.** *Sea L/K una extensión de Galois finita y $G = \mathrm{Gal}(L/K)$. Entonces existe una correspondencia uno a uno, que revierte inclusiones, entre los cuerpos intermedios E de L/K y los subgrupos de H de G, dado por*

$$E \overset{*}{\mapsto} \mathrm{Gal}(L/E), \quad H \overset{\star}{\mapsto} \mathcal{F}(H)$$

Se tiene además que si $E \leftrightarrow H$ entonces

(1) $[L : E] = |H|$ *y* $|G : H| = [E : K]$*, donde* $|G : H|$ *denota el índice de* H *en* G*.*

(2) $H \triangleleft G$ *si y solo si* E/K *es de Galois. Cuando esto ocurre,* $\mathrm{Gal}(E/K) \cong G/H$*.*

Demostración. Por el Teorema 1.9, se tiene que ambas correspondencias revierten inclusiones. Vamos a probar que $E \overset{*}{\mapsto} \mathrm{Gal}(L/E)$ es biyectiva.

Para la inyectividad, sean E_1 y E_2 cuerpos intermedios de la extensión L/K, con $\mathrm{Gal}(L/E_1) = \mathrm{Gal}(L/E_2)$. Al ser L/K de Galois, lo son también L/E_1 y L/E_2; luego, por el Teorema 1.17, $E_1 = \mathcal{F}(\mathrm{Gal}(L/E_1))$ y $E_2 = \mathcal{F}(\mathrm{Gal}(L/E_2))$, lo cual implica que $E_1 = E_2$.

Para la suryectividad, sea H un subgrupo de G. Como H es un subgrupo finito, del Teorema de Artin, se tiene $H = \mathrm{Gal}(L/\mathcal{F}(H))$. Entonces $E = \mathcal{F}(H)$ es un cuerpo intermedio de L/K cuya imagen es H:

$$E \overset{*}{\mapsto} \mathrm{Gal}(L/E) = \mathrm{Gal}(L/\mathcal{F}(H)) = H.$$

Así, $E \overset{*}{\mapsto} \mathrm{Gal}(L/E)$ es una correspondencia uno a uno entre los cuerpos intermedios de L/K y los subgrupos de G. Además, su inversa es $H \overset{\star}{\mapsto} \mathcal{F}(H)$ ya que

$$E \overset{*}{\mapsto} \mathrm{Gal}(L/E) \overset{\star}{\mapsto} \mathcal{F}(\mathrm{Gal}(L/E)) = E$$
$$H \overset{\star}{\mapsto} \mathcal{F}(H) \overset{*}{\mapsto} \mathrm{Gal}(L/\mathcal{F}(H)) = H.$$

Supongamos ahora que $E \leftrightarrow H$.

(1) Al ser L/K y L/E extensiones de Galois de grado finito, por el Teorema 1.17, se tiene

$[L:K] = |G|$ y $[L:E] = |\mathrm{Gal}(L/E)| = |H|$. Luego,

$$\begin{aligned} |G:H| &= |G|/|H| \\ &= [L:K]/[L:E] \\ &= [E:K]. \end{aligned}$$

(2) Supongamos que H es un subgrupo normal de G. Denotemos $E = \mathcal{F}(H)$. Sea $\alpha \in L$ y β cualquiera otra raíz de $\mathrm{mín}(\alpha, K)$. Por el Teorema de Extensión de Isomorfismos, existe un $\sigma \in G$ tal que $\sigma(\alpha) = \beta$. Si $\tau \in H$ entonces $\tau(\beta) = \sigma\left(\sigma^{-1}\tau\sigma(\alpha)\right)$. Puesto que $H \triangleleft G$, se tiene $\sigma^{-1}\tau\sigma \in H$, por lo que $\sigma^{-1}\tau\sigma(\alpha) = \alpha$ y $\tau(\beta) = \sigma(\alpha) = \beta$, lo que significa que $\beta \in \mathcal{F}(H) = E$. Como $\mathrm{mín}(\alpha, K)$ se descompone sobre L, esto último muestra que $\mathrm{mín}(\alpha, K)$ se descompone sobre E. Por lo tanto, E es normal sobre K; además E/K es separable ya que L/K lo es. Así, E/K es una extensión de Galois.

Recíprocamente, supongamos que E/K es una extensión de Galois. Como E/K es normal, el Teorema 1.15 implica que $\sigma|_E : E \hookrightarrow \overline{K}$ es un $K-$homomorfismo que induce un $K-$automorfismo de E. Por lo que podemos definir la función

$$\begin{aligned} \theta : G &\to \mathrm{Gal}(E/K) \\ \sigma &\mapsto \sigma|_E \end{aligned}$$

Es claro que θ es un homomorfismo de grupos bien definido y su núcleo es

$$\ker\theta = \{\sigma \in G \mid \sigma|_E = \mathrm{id}\} = \mathrm{Gal}(L/E) = H.$$

Por lo tanto, $H \triangleleft G$. Por otro lado, cada $\tau \in \mathrm{Gal}(E/K)$ se puede extender a un $\sigma \in G$ tal que $\sigma|_E = \tau$; esto implica que θ es suryectiva. Luego, por el Primer Teorema de Isomorfismos, $G/H \cong \mathrm{Gal}(E/K)$. □

Ejemplo 1.15. Sea L el cuerpo de descomposición de x^3-2 sobre $\mathbb{Q}$. Las raíces de x^3-2 son: $\sqrt[3]{2}$ y $\sqrt[3]{2}\left(\frac{-1\pm\sqrt{3}i}{2}\right)$. Denotemos $\omega=\frac{-1+\sqrt{3}i}{2}$; entonces $\omega^2=\frac{-1-\sqrt{3}i}{2}$. Como $\omega^2=-1-\omega$, se tiene que el cuerpo de descomposición de x^3-2 sobre $\mathbb{Q}$ es $L=\mathbb{Q}\left(\sqrt[3]{2},\omega\right)$. Determinemos $[L:\mathbb{Q}]$: Es claro, por el Criterio de Eisentein, que $\left[\mathbb{Q}\left(\sqrt[3]{2}\right):\mathbb{Q}\right]=3$; además, $\left\{1,\sqrt[3]{2},\sqrt[3]{2}^2\right\}$ es una base para $\mathbb{Q}\left(\sqrt[3]{2}\right)$ como espacio vectorial sobre $\mathbb{Q}$. Por otro lado,

$$\begin{aligned}\omega&=\frac{-1+\sqrt{3}i}{2}\\ 2\omega+1&=\sqrt{3}i\\ (2\omega+1)^2&=-3\\ (2\omega+1)^2+3&=0.\end{aligned}$$

Esto significa que ω es raíz de $(2x+1)^2+3\in\mathbb{Q}\left(\sqrt[3]{2}\right)[x]$ y como $\omega\notin\mathbb{Q}\left(\sqrt[3]{2}\right)$, concluimos que $\left[\mathbb{Q}\left(\sqrt[3]{2},\sqrt{3}i\right):\mathbb{Q}\left(\sqrt[3]{2}\right)\right]=2$ y que una base para L como espacio vectorial sobre $\mathbb{Q}\left(\sqrt[3]{2}\right)$ es $\{1,\omega\}$.

Utilizando el Teorema de la Torre, tenemos

$$\begin{aligned}[L:\mathbb{Q}]&=\left[L:\mathbb{Q}\left(\sqrt[3]{2},\omega\right)\right]\left[\mathbb{Q}\left(\sqrt[3]{2}\right):\mathbb{Q}\right]\\ &=2\cdot3\\ &=6,\end{aligned}$$

y una base para L como espacio vectorial sobre $\mathbb{Q}$ es

$$\left\{1,\sqrt[3]{2},\sqrt[3]{2}^2,\omega,\sqrt[3]{2}\omega,\sqrt[3]{2}^2\omega\right\}.$$

Como $L/\mathbb{Q}$ es normal, finita y separable, $|\mathrm{Gal}\,(L/\mathbb{Q})|=[L:\mathbb{Q}]=6$. Ahora determinemos estos seis automorfismos. Como x^3-2 es irreducible sobre $\mathbb{Q}$, los automorfismos de L llevan raíces de x^3-2 en raíces de x^3-2. Luego, los siguientes son elementos de $\mathrm{Gal}\,(L/\mathbb{Q})$:

$$\sigma_0 : \begin{pmatrix} \sqrt[3]{2} & \sqrt[3]{2}\omega & \sqrt[3]{2}\omega^2 \\ \downarrow & \downarrow & \downarrow \\ \sqrt[3]{2} & \sqrt[3]{2}\omega & \sqrt[3]{2}\omega^2 \end{pmatrix} \quad \sigma_1 : \begin{pmatrix} \sqrt[3]{2} & \sqrt[3]{2}\omega & \sqrt[3]{2}\omega^2 \\ \downarrow & \downarrow & \downarrow \\ \sqrt[3]{2} & \sqrt[3]{2}\omega^2 & \sqrt[3]{2}\omega \end{pmatrix}$$

$$\sigma_2 : \begin{pmatrix} \sqrt[3]{2} & \sqrt[3]{2}\omega & \sqrt[3]{2}\omega^2 \\ \downarrow & \downarrow & \downarrow \\ \sqrt[3]{2}\omega & \sqrt[3]{2} & \sqrt[3]{2}\omega^2 \end{pmatrix} \quad \sigma_3 : \begin{pmatrix} \sqrt[3]{2} & \sqrt[3]{2}\omega & \sqrt[3]{2}\omega^2 \\ \downarrow & \downarrow & \downarrow \\ \sqrt[3]{2}\omega & \sqrt[3]{2}\omega^2 & \sqrt[3]{2} \end{pmatrix}$$

$$\sigma_4 : \begin{pmatrix} \sqrt[3]{2} & \sqrt[3]{2}\omega & \sqrt[3]{2}\omega^2 \\ \downarrow & \downarrow & \downarrow \\ \sqrt[3]{2}\omega^2 & \sqrt[3]{2} & \sqrt[3]{2}\omega \end{pmatrix} \quad \sigma_5 : \begin{pmatrix} \sqrt[3]{2} & \sqrt[3]{2}\omega & \sqrt[3]{2}\omega^2 \\ \downarrow & \downarrow & \downarrow \\ \sqrt[3]{2}\omega^2 & \sqrt[3]{2}\omega & \sqrt[3]{2} \end{pmatrix}$$

Como estos seis elementos son distintos entre sí entonces

$$\mathrm{Gal}\,(L/\mathbb{Q}) = \{\sigma_i \mid i = 0, 1, 2, 3, 4, 5\}\,.$$

Veamos el efecto de cada uno de ellos sobre $\sqrt{3}i$:

Como $\sigma_0 = \mathrm{id}$, entonces $\sigma_0\left(\sqrt{3}i\right) = \sqrt{3}i$.

- Para σ_1:

$$\begin{aligned} \sigma_1\left(\sqrt[3]{2}\omega\right) &= \sigma_1\left(\sqrt[3]{2}\right)\sigma_1(\omega) \\ \cancel{\sqrt[3]{2}}\omega^2 &= \cancel{\sqrt[3]{2}}\left(\frac{-1+\sigma_1\left(\sqrt{3}i\right)}{2}\right) \\ \frac{-1-\sqrt{3}i}{2} &= -\frac{1}{2}+\frac{1}{2}\sigma_1\left(\sqrt{3}i\right) \\ -\frac{\sqrt{3}i}{2} &= \frac{1}{2}\sigma_1\left(\sqrt{3}i\right) \\ -\sqrt{3}i &= \sigma_1\left(\sqrt{3}i\right). \end{aligned}$$

- Para σ_2:

$$\begin{aligned}
\sigma_2\left(\sqrt[3]{2}\omega\right) &= \sigma_2\left(\sqrt[3]{2}\right)\sigma_2(\omega)\\
\cancel{\sqrt[3]{2}} &= \cancel{\sqrt[3]{2}}\omega\left(\frac{-1+\sigma_2\left(\sqrt{3}i\right)}{2}\right)\\
1 &= \left(\frac{-1+\sqrt{3}i}{2}\right)\left(-\frac{1}{2}+\frac{1}{2}\sigma_2\left(\sqrt{3}i\right)\right)\\
\frac{2}{-1+\sqrt{3}i}\cdot\frac{-1-\sqrt{3}i}{-1-\sqrt{3}i} &= -\frac{1}{2}+\frac{1}{2}\sigma_2\left(\sqrt{3}i\right)\\
\frac{-2-2\sqrt{3}i}{4} &= -\frac{1}{2}+\frac{1}{2}\sigma_2\left(\sqrt{3}i\right)\\
-\frac{1}{2}-\frac{1}{2}\sqrt{3}i &= -\frac{1}{2}+\frac{1}{2}\sigma_2\left(\sqrt{3}i\right)\\
-\sqrt{3}i &= \sigma_2\left(\sqrt{3}i\right).
\end{aligned}$$

- Para σ_3:

$$\begin{aligned}
\sigma_3\left(\sqrt[3]{2}\omega\right) &= \sigma_3\left(\sqrt[3]{2}\right)\sigma_3(\omega)\\
\cancel{\sqrt[3]{2}}\omega^2 &= \cancel{\sqrt[3]{2}}\omega\left(\frac{-1+\sigma_3\left(\sqrt{3}i\right)}{2}\right)\\
\omega &= -\frac{1}{2}+\frac{1}{2}\sigma_3\left(\sqrt{3}i\right)\\
\frac{-1+\sqrt{3}i}{2} &= -\frac{1}{2}+\frac{1}{2}\sigma_3\left(\sqrt{3}i\right)\\
-\frac{1}{2}+\frac{1}{2}\sqrt{3}i &= -\frac{1}{2}+\frac{1}{2}\sigma_3\left(\sqrt{3}i\right)\\
-\frac{1}{2}+\frac{1}{2}\sqrt{3}i &= -\frac{1}{2}+\frac{1}{2}\sigma_3\left(\sqrt{3}i\right)\\
\sqrt{3}i &= \sigma_3\left(\sqrt{3}i\right).
\end{aligned}$$

- Para σ_4:

$$\begin{aligned}
\sigma_4\left(\sqrt[3]{2}\omega\right) &= \sigma_4\left(\sqrt[3]{2}\right)\sigma_4(\omega)\\
\cancel{\sqrt[3]{2}} &= \cancel{\sqrt[3]{2}}\omega^2\left(\frac{-1+\sigma_4\left(\sqrt{3}i\right)}{2}\right)\\
1 &= \omega\left(-\frac{1}{2}+\frac{1}{2}\sigma_4\left(\sqrt{3}i\right)\right)\\
\frac{1}{\omega} &= -\frac{1}{2}+\frac{1}{2}\sigma_4\left(\sqrt{3}i\right)\\
-\frac{1}{2}-\frac{1}{2}\sqrt{3}i &= -\frac{1}{2}+\frac{1}{2}\sigma_4\left(\sqrt{3}i\right)\\
-\sqrt{3}i &= \sigma_4\left(\sqrt{3}i\right).
\end{aligned}$$

- Para σ_5:

$$\begin{aligned}
\sigma_5\left(\sqrt[3]{2}\omega\right) &= \sigma_5\left(\sqrt[3]{2}\right)\sigma_5(\omega)\\
\cancel{\sqrt[3]{2}}\omega &= \cancel{\sqrt[3]{2}}\omega^2\left(\frac{-1+\sigma_5\left(\sqrt{3}i\right)}{2}\right)\\
1 &= \omega\left(-\frac{1}{2}+\frac{1}{2}\sigma_5\left(\sqrt{3}i\right)\right)\\
\frac{1}{\omega} &= -\frac{1}{2}+\frac{1}{2}\sigma_5\left(\sqrt{3}i\right)\\
-\frac{1}{2}-\frac{1}{2}\sqrt{3}i &= -\frac{1}{2}+\frac{1}{2}\sigma_5\left(\sqrt{3}i\right)\\
-\sqrt{3}i &= \sigma_5\left(\sqrt{3}i\right).
\end{aligned}$$

Así, los valores de estos automorfismos sobre $\sqrt[3]{2}$ y $\sqrt{3}i$ son:

$$\sigma_0:\begin{pmatrix}\sqrt[3]{2} & \sqrt{3}i\\ \downarrow & \downarrow\\ \sqrt[3]{2} & \sqrt{3}i\end{pmatrix}\quad \sigma_1:\begin{pmatrix}\sqrt[3]{2} & \sqrt{3}i\\ \downarrow & \downarrow\\ \sqrt[3]{2} & -\sqrt{3}i\end{pmatrix}\quad \sigma_2:\begin{pmatrix}\sqrt[3]{2} & \sqrt{3}i\\ \downarrow & \downarrow\\ \sqrt[3]{2}\omega & -\sqrt{3}i\end{pmatrix}$$

$$\sigma_3:\begin{pmatrix}\sqrt[3]{2} & \sqrt{3}i\\ \downarrow & \downarrow\\ \sqrt[3]{2}\omega & \sqrt{3}i\end{pmatrix}\quad \sigma_4:\begin{pmatrix}\sqrt[3]{2} & \sqrt{3}i\\ \downarrow & \downarrow\\ \sqrt[3]{2}\omega^2 & -\sqrt{3}i\end{pmatrix}\quad \sigma_5:\begin{pmatrix}\sqrt[3]{2} & \sqrt{3}i\\ \downarrow & \downarrow\\ \sqrt[3]{2}\omega^2 & \sqrt{3}i\end{pmatrix}$$

Ahora, el grupo $\mathrm{Gal}(L/\mathbb{Q})$ es isomorfo a $\mathbb{Z}/6\mathbb{Z}$ o a S_3. Como

$$\sigma_1\sigma_2\left(\sqrt[3]{2}\right) = \sigma_1\left(\sqrt[3]{2}\omega\right) = \sqrt[3]{2}\omega^2$$

y

$$\sigma_2\sigma_1\left(\sqrt[3]{2}\right) = \sigma_2\left(\sqrt[3]{2}\right) = \sqrt[3]{2}\omega$$

entonces $\mathrm{Gal}(L/\mathbb{Q})$ no es abeliano. Por lo tanto, $\mathrm{Gal}(L/\mathbb{Q}) \cong S_3$.

Ahora determinemos cómo se corresponden los subgrupos de $\mathrm{Gal}(L/\mathbb{Q})$ con los subcuerpos intermedios de $L/\mathbb{Q}$. Sabemos que

$$S_3 = \{\mathrm{id}, (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2)\}$$

y los subgrupos de S_3 son

$$H_1 = \{\mathrm{id}\}$$
$$H_2 = \{\mathrm{id}, (1\ 2)\}$$
$$H_3 = \{\mathrm{id}, (1\ 3)\}$$
$$H_4 = \{\mathrm{id}, (2\ 3)\}$$
$$H_5 = \{\mathrm{id}, (1\ 2\ 3), (1\ 3\ 2)\}$$
$$H_6 = S_3.$$

Denotando $r_1 = \sqrt[3]{2}$, $r_2 = \sqrt[3]{2}\omega$ y $r_3 = \sqrt[3]{2}\omega^2$, los correspondientes subgrupos de $\mathrm{Gal}(L/\mathbb{Q})$

son:

$$H_1 = \{\sigma_0\}$$

$$H_2 = \{\sigma_0, \sigma_2\}$$

$$H_3 = \{\sigma_0, \sigma_5\}$$

$$H_4 = \{\mathrm{id}, \sigma_1\}$$

$$H_5 = \{\mathrm{id}, \sigma_3, \sigma_4\}$$

$$H_6 = \mathrm{Gal}\,(L/\mathbb{Q})\,.$$

Ahora determinamos los subcuerpos fijos de cada subgrupo: Es claro que $E_{H_1} = L$ y $E_{H_6} = \mathbb{Q}$. Los elementos de L tienen la forma

$$a + b\sqrt[3]{2} + c\sqrt[3]{2}^2 + d\omega + e\sqrt[3]{2}\omega + f\sqrt[3]{2}^2\omega, \text{ con } a, b, c, d, e, f \in \mathbb{Q}.$$

- Para H_2: Aplicando σ_2 se obtiene

$$\begin{aligned}
&a + b\sqrt[3]{2}\omega + c\sqrt[3]{2}^2\omega^2 + d\omega^2 + e\sqrt[3]{2} + f\sqrt[3]{2}\omega\sqrt[3]{2} \\
&= a + b\sqrt[3]{2}\omega + c\sqrt[3]{2}^2(-1-\omega) + d(-1-\omega) + e\sqrt[3]{2} + f\sqrt[3]{2}\omega\sqrt[3]{2} \\
&= a + b\sqrt[3]{2}\omega - c\sqrt[3]{2}^2 - c\sqrt[3]{2}^2\omega - d - d\omega + e\sqrt[3]{2} + f\sqrt[3]{2}^2\omega \\
&= (a-d) + e\sqrt[3]{2} - c\sqrt[3]{2}^2 - d\omega + b\sqrt[3]{2}\omega + f\sqrt[3]{2}^2\omega,
\end{aligned}$$

de donde $a - d = a$,$b = e$, $c = d = 0$, $b = e$. Entonces

$$E_{H_2} = \left\{a + b\left(\sqrt[3]{2} + \sqrt[3]{2}\omega\right) + f\sqrt[3]{2}^2\omega \mid a, b, f \in \mathbb{Q}\right\}.$$

Note que $\mathbb{Q}\left(\sqrt[3]{2}^2\omega\right) \subseteq E_{H_2}$. Por otro lado,

$$\begin{aligned}\left(\sqrt[3]{2}^2\omega\right)^2 &= 2\sqrt[3]{2}\omega^2 \\ &= 2\sqrt[3]{2}\left(-1-\omega\right) \\ &= -2\left(\sqrt[3]{2}+\sqrt[3]{2}\omega\right).\end{aligned}$$

Luego, $\sqrt[3]{2}+\sqrt[3]{2}\omega \in \mathbb{Q}\left(\sqrt[3]{2}^2\omega\right)$ y por lo tanto, todo elemento de E_{H_2} también está en $\mathbb{Q}\left(\sqrt[3]{2}^2\omega\right)$. Así, $E_{H_2} = \mathbb{Q}\left(\sqrt[3]{2}^2\omega\right)$ y

$$H_2 = \{\sigma_0, \sigma_2\} \longleftrightarrow \mathbb{Q}\left(\sqrt[3]{2}^2\omega\right).$$

- Para H_3: Aplicando σ_5 se obtiene

$$\begin{aligned}&a+b\sqrt[3]{2}\omega^2+c\sqrt[3]{2}^2\omega^4+d\omega^2+e\sqrt[3]{2}\omega+f\sqrt[3]{2}\omega^2\sqrt[3]{2}\omega \\ &= a+b\sqrt[3]{2}\left(-1-\omega\right)+c\sqrt[3]{2}^2\omega+d\left(-1-\omega\right)+e\sqrt[3]{2}\omega+f\sqrt[3]{2}^2 \\ &= a-b\sqrt[3]{2}-b\sqrt[3]{2}\omega+c\sqrt[3]{2}^2\omega-d-d\omega+e\sqrt[3]{2}\omega+f\sqrt[3]{2}^2 \\ &= (a-d)-b\sqrt[3]{2}+f\sqrt[3]{2}^2-d\omega+(-b+e)\sqrt[3]{2}^2\omega+c\sqrt[3]{2}^2\omega,\end{aligned}$$

de donde $a-d=a, b=0$, $c=f$, $d=0$, $-b+e=e$. Entonces

$$E_{H_2} = \left\{a+e\sqrt[3]{2}\omega+c\left(\sqrt[3]{2}+\sqrt[3]{2}^2\omega\right) \mid a,e,c \in \mathbb{Q}\right\}.$$

Note que $\mathbb{Q}\left(\sqrt[3]{2}\omega\right) \subseteq E_{H_2}$. Por otro lado,

$$\left(\sqrt[3]{2}^2\omega\right)^2 = -2\left(\sqrt[3]{2}+\sqrt[3]{2}\omega\right).$$

Entonces,

$$\begin{aligned}\sqrt[3]{2}^2+\sqrt[3]{2}^2\omega &= \sqrt[3]{2}\left(\sqrt[3]{2}+\sqrt[3]{2}\omega\right)\\ &= \sqrt[3]{2}\left(\frac{\left(\sqrt[3]{2}^2\omega\right)^2}{-2}\right)\\ &= \frac{2\sqrt[3]{2}^2\omega^2}{-2}\\ &= -\left(\sqrt[3]{2}\omega\right)^2.\end{aligned}$$

Luego, $\sqrt[3]{2}^2+\sqrt[3]{2}^2\omega \in \mathbb{Q}\left(\sqrt[3]{2}\omega\right)$ y por lo tanto, todo elemento de E_{H_3} también está en $\mathbb{Q}\left(\sqrt[3]{2}\omega\right)$. Así, $E_{H_3}=\mathbb{Q}\left(\sqrt[3]{2}\omega\right)$ y

$$H_3=\{\sigma_0,\sigma_5\} \longleftrightarrow \mathbb{Q}\left(\sqrt[3]{2}\omega\right).$$

- Para H_4: Aplicando σ_1 se obtiene

$$\begin{aligned}&a+b\sqrt[3]{2}+c\sqrt[3]{2}^2+d\omega^2+e\sqrt[3]{2}\omega^2+f\sqrt[3]{2}\sqrt[3]{2}\omega^2\\ &= a+b\sqrt[3]{2}+c\sqrt[3]{2}^2+d(-1-\omega)+e\sqrt[3]{2}(-1-\omega)+f\sqrt[3]{2}^2(-1-\omega)\\ &= a+b\sqrt[3]{2}+c\sqrt[3]{2}^2-d-d\omega-e\sqrt[3]{2}-e\sqrt[3]{2}\omega-f\sqrt[3]{2}^2-f\sqrt[3]{2}^2\omega\\ &= (a-d)+(b-e)\sqrt[3]{2}+(c-f)\sqrt[3]{2}^2-d\omega-e\sqrt[3]{2}^2\omega-f\sqrt[3]{2}^2\omega,\end{aligned}$$

de donde $a-d=a, b-e=b$, $c-f=c$, $d=0$, $e=0$ y $f=0$. Entonces,

$$E_{H_4}=\left\{a+b\sqrt[3]{2}+c\sqrt[3]{2}^2 \mid a,b,c\in\mathbb{Q}\right\}=\mathbb{Q}\left(\sqrt[3]{2}\right).$$

Así,

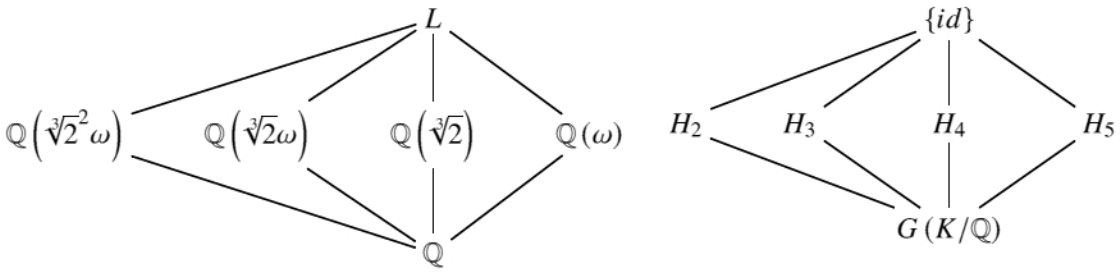
$$H_4=\{\sigma_0,\sigma_1\} \longleftrightarrow \mathbb{Q}\left(\sqrt[3]{2}\right).$$

- Para H_5: $\mathbb{Q}(\omega)$ es un subcuerpo distinto a los anteriores. Como la correspondencia es uno

uno, necesariamente tenemos

$$H_5 = \{\sigma_0, \sigma_3, \sigma_4\} \longleftrightarrow \mathbb{Q}(\omega).$$

Así,



Para finalizar los preliminares algebraicos, veamos una extensión algebraica de grado infinito para el cual no existe tal correspondencia y la cual motiva el desarrollo de este trabajo.

Ejemplo 1.16. Consideremos $S = \left\{\sqrt{p} \mid p \text{ primo}\right\}$ y sea $L = \mathbb{Q}(S)$ el cuerpo generado por los elementos de S sobre $\mathbb{Q}$. La extensión $L/\mathbb{Q}$ es de Galois ya que L es el cuerpo de descomposición de la familia de polinomios separables $\left\{x^2 - p \mid p \text{ primo}\right\} \subseteq \mathbb{Q}[x]$. Además, es de grado infinito (Ejemplo 1.7). Ahora, cualquier $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$ debe enviar $\sqrt{p}$ a uno de sus conjugados sobre $\mathbb{Q}$; esto es, a $\sqrt{p}$ o a $-\sqrt{p}$. Esto implica que σ tiene orden dos y de la teoría de grupos abelianos infinitos, esto significa que $\mathrm{Gal}(L/\mathbb{Q})$ es un 2-grupo abeliano elemental; por lo tanto,

$$\mathrm{Gal}(L/\mathbb{Q}) \cong \prod_{i=1}^{\infty} \mathbb{Z}/2\mathbb{Z}.$$

Este grupo puede considerarse como espacio vectorial V sobre el cuerpo $\mathbb{Z}/2\mathbb{Z}$. Considere el espacio dual $V^* = \{\phi : V \to \mathbb{Z}/2\mathbb{Z} \mid \phi \text{ es una transformación lineal}\}$. Note que $|V^*| = |\mathcal{P}(\mathcal{B})|$, donde $\mathcal{B}$ es una base de V. Como V es de dimensión infinita, $\mathcal{P}(\mathcal{B})$ es no enumerable y, así, V^* es también no enumerable. Esto también implica que el conjunto $\{\ker\phi \mid \phi \in V^*\}$ no es enumerable. Los conjuntos $\ker\phi$ son subgrupos normales de V (ya que V es abeliano), por lo que por el Primer Teorema de Isomorfismos de grupos, $V/\ker\phi \cong \phi(V)$. Pero $\phi(V) \cong \mathbb{F}_2$ ya que $\phi(v)$ solo puede

tomar dos imágenes: 0 o 1 en $\mathbb{Z}/2\mathbb{Z}$. Todo esto implica que $\{\ker\phi \mid \phi \in V^*\}$ es una colección no enumerable de subgrupos de índice dos. Luego, si existiese una correspondencia biyectiva como dice el teorema, debería existir una cantidad no enumerable de subextensiones de grado dos en $L/\mathbb{Q}$; pero esto no es cierto ya que las únicas subextensiones cuadráticas de $L/\mathbb{Q}$ son $\left\{\mathbb{Q}\left(\sqrt{p}\right) \mid p \text{ no es cuadrado perfecto}\right\}$.

1.5. Preliminares de Topología

Para atacar el problema de la correspondencia de Galois en extensiones de grado infinito, nos apoyaremos en una topología que se definirá sobre el grupo de Galois de una extensión de Galois. Así, recopilemos una serie de hechos topológicos que utilizaremos más adelante.

Definición 1.17. Una colección $\mathcal{B}$ de subconjuntos de X es una base para una topología sobre X si:

(1) Para todo $x \in X$ existe $B \in \mathcal{B}$ tal que $x \in B$;

(2) Si $x \in B_1 \cap B_2$, con $B_1, B_2 \in \mathcal{B}$, entonces existe $B_3 \in \mathcal{B}$ tal que $x \in B_3$ y $B_3 \subseteq B_1 \cap B_2$.

Definición 1.18. Un espacio topológico X se denomina espacio de Hausdorff si para cada par x, y de puntos distintos de X, existen abiertos U, V de x, y respectivamente, que son disjuntos.

Definición 1.19. Sea X un espacio topológico. Una separación de X es un par U, V de abiertos disjuntos no triviales de X cuya unión es X. El espacio X se dice que es *conexo* si no existe una separación de X.

Definición 1.20. Un espacio es *totalmente disconexo* si sus únicos subespacios conexos son los conjuntos unipuntuales.

Definición 1.21. (Topología Producto) Sea $\mathcal{J}$ un conjunto de índices, $\{X_j\}_{j\in\mathcal{J}}$ una familia indexada de espacios topológicos y $X = \underset{j\in\mathcal{J}}{\cup} X_j$. El producto cartesiano de esta familia indexada, denotado por

$$\prod_{j\in\mathcal{J}} X_j,$$

se define como el conjunto de todas las $\mathcal{J}-$uplas $\mathbf{x} : \mathcal{J} \to \underset{j\in\mathcal{J}}{\cup} X_j$ de elementos de X tales que $\mathbf{x}(j) \in X_j$, para cada $j \in \mathcal{J}$.

Notación. Las $\mathcal{J}-$uplas las denotaremos por $(x_j)_{j\in\mathcal{J}}$.

Sea $\pi_i : \prod_{j\in\mathcal{J}} X_j \to X_i$ la función que asigna a cada elemento del espacio producto su coordenada $i-$ésima,

$$\pi_i(\mathbf{x}) = \mathbf{x}(i);$$

se denomina aplicación proyección asociada con el índice i.

La *topología producto* sobre $\prod_{j\in\mathcal{J}} X_j$ se define como la topología cuyos abiertos son uniones de intersecciones finitas de elementos de la colección

$$\mathcal{S} = \left\{\pi_i^{-1}(U_i) \mid U_i \text{ es abierto en } X_i\right\}.$$

Teorema 1.22 (Teorema de Tychonoff)**.** *El producto arbitrario de espacios compactos es compacto en la topología producto.*

Demostración. El lector puede consultar la demostración en Munkres (2002, p. 267). □

Capítulo 2

Topología sobre el Grupo de Galois

Al final de la sección 1.4 se estableció que el cuerpo generado al adjuntar a $\mathbb{Q}$ las raíces cuadradas de los números primos, es una extensión de Galois de grado infinito para la cual la correspondencia de Galois no se cumple, ya que hay muchísimos más subgrupos que subcuerpos intermedios de la extensión. Krull fue el primero en considerar cómo reestablecer tal correspondencia, logrando una generalización de la teoría clásica de Galois a extensiones algebraicas de grado infinito al introducir una topología sobre el grupo de Galois. Así, probó que los subgrupos cerrados de $\mathrm{Gal}\,(L/K)$ son los que se corresponden uno a uno con los subcuerpos intermedios de la extensión L/K.

2.1. La Topología de Krull

A lo largo de este capítulo, para una extensión de Galois L/K denotemos:

- $\mathrm{Gal}\,(L/K)$ al grupo de Galois de la extensión L/K.
- $\mathcal{I} = \{E_i \mid i \in I\}$, la colección de cuerpos intermedios $K \subseteq E_i \subseteq L$, tales que E_i/K es una

extensión de Galois de grado finito.

$$\begin{array}{c} L \\ | \\ E_i \\ | \\ K \end{array}$$

- $\mathcal{N} = \{N_i : i \in I\}$, la colección de subgrupos $N_i = \mathrm{Gal}\,(L/E_i)$ del grupo de Galois de la extensión L/K, donde $E_i \in \mathcal{I}$.

Observación 2.1. Ambas colecciones están indexadas por un conjunto de índices I.

Lema 2.1. *Si $\alpha_1, \alpha_2, ..., \alpha_n \in L$ entonces existe E_i en $\mathcal{I}$ tal que $\alpha_1, \alpha_2, ..., \alpha_n \in E_i$.*

Demostración. Basta tomar E_i como el cuerpo de descomposición de la familia de polinomios $\mathrm{mín}\,(\alpha_k, K)$, $k = 1, 2, ..., n$. Entonces la extensión E_i/K es normal (por Teorema 1.15) y finita. Además es separable ya que L/K lo es. Por lo tanto, E_i/K es una extensión de Galois de grado finito que contiene a $\alpha_1, \alpha_2, ..., \alpha_n$. □

Notación. Denotemos por 1 a la identidad de $\mathrm{Gal}\,(L/K)$.

Lema 2.2. *Se tiene:*

(1) $\bigcap\limits_{i \in I} N_i = \{1\}$.

(2) $\bigcap\limits_{i \in I} \sigma N_i = \{\sigma\}$, *para todo* $\sigma \in \mathrm{Gal}\,(L/K)$.

(3) *Para todo i, j en I, $N_i \cap N_j \in \mathcal{N}$.*

Demostración. (1) Sea $\tau \in \bigcap\limits_{i \in I} N_i$ y $\alpha \in L$. Por el Lema 2.1, existe un cuerpo E_i en $\mathcal{I}$ tal que $\alpha \in E_i$; luego, $N_i = \mathrm{Gal}\,(L/E_i)$. Entonces $\tau \in N_i$, por lo que τ fija los elementos de E_i; así, $\tau\,(\alpha) = \alpha$, para todo $\alpha \in L$ y por lo tanto, $\tau = 1$. Así, $\bigcap\limits_{i \in I} N \subseteq \{1\}$, lo que prueba la igualdad.

(2) Sea $\tau \in \bigcap\limits_{i \in I} \sigma N_i$, con $\sigma \in \mathrm{Gal}\,(L/K)$. Entonces, para todo $i \in I$ se tiene que $\tau \in \sigma N_i$; es decir, $\sigma^{-1}\tau \in N_i$. Luego, por la parte 1) se tiene $\sigma^{-1}\tau = 1$, de modo que $\tau = \sigma$. Por lo tanto, $\bigcap\limits_{i \in I} \sigma N_i = \{\sigma\}$, para todo $\sigma \in \mathrm{Gal}\,(L/K)$.

(3) Sean $N_i, N_j \in \mathcal{N}$, donde i, j están en I. Entonces existen subcuerpos E_i, E_j en $\mathcal{I}$ tales que

$$N_i = \text{Gal}\,(L/E_i) \quad \text{y} \quad N_j = \text{Gal}\left(L/E_j\right).$$

Por el Teorema 1.20, E_iE_j está en $\mathcal{I}$. Note que $\sigma \in N_i \cap N_j$ si y solo si $\sigma\,|_{E_i} = 1$ y $\sigma\,|_{E_j} = 1$, si y solo si $E_i \subseteq \mathcal{F}\,(\{\sigma\})$ y $E_j \subseteq \mathcal{F}\,(\{\sigma\})$, si y solo si $E_iE_j \subseteq \mathcal{F}\,(\{\sigma\})$. Esta última condición es cierta si y solo si $\sigma \in \text{Gal}\left(L/E_iE_j\right)$. Por tanto, $\text{Gal}\left(L/E_iE_j\right) = N_i \cap N_j$. Así, $N_i \cap N_j \in \mathcal{N}$. □

Lema 2.3. *Sea $N_i \in \mathcal{N}$, con $N_i = \text{Gal}\,(L/E_i)$ y $E_i \in \mathcal{I}$. Entonces $E_i = \mathcal{F}\,(N_i)$ y $N_i \triangleleft \text{Gal}\,(L/K)$. Además,*

$$\text{Gal}\,(E_i/K) \cong \text{Gal}\,(L/K)\,/N_i.$$

Así,

$$|\text{Gal}\,(L/K)\,/N_i| = |\text{Gal}\,(E_i/K)| = [E_i : K] < \infty.$$

Demostración. Como L es normal y separable sobre K, el cuerpo L también es normal y separable sobre E_i, por lo que L/E_i es una extensión de Galois. Por lo tanto, $E_i = \mathcal{F}\,(N)$.

Considere la aplicación $\theta : \text{Gal}\,(L/K) \to \text{Gal}\,(E_i/K)$ dada por

$$\sigma \mapsto \sigma\,|_E\,.$$

Para cada $\alpha \in E_i$, $\sigma\,(\alpha)$ es raíz de $\text{mín}\,(\alpha, K)$; luego, la normalidad de E_i/K implica que $\sigma\,(\alpha) \in E_i$. Por lo tanto, θ es un homomorfismo de grupos bien definido. Su núcleo es

$$\ker\theta = \left\{\sigma \in G \mid \sigma\,|_{E_i} = 1\right\} = \text{Gal}\,(L/E_i) = N_i.$$

Por lo tanto, $N_i \triangleleft G$. Por otro lado, cada $\tau \in \text{Gal}\,(L/E_i)$ se puede extender a un $\sigma \in G$ tal que $\sigma\,|_E = \tau$; esto implica que θ es suryectiva. Luego, por el Primer Teorema de Isomorfismos de grupos se tiene $\text{Gal}\,(L/K)\,/N_i \cong \text{Gal}\,(E_i/K)$. □

Teorema 2.1. *La colección* $\mathcal{B} = \{\sigma N_i : \sigma \in \mathrm{Gal}\,(L/K)\,,\, N_i \in \mathcal{N}\}$ *es una base para una topología sobre* $\mathrm{Gal}\,(L/K)$.

Demostración. Probaremos las dos condiciones que debe satisfacer $\mathcal{B}$ para que sea base de una topología sobre $\mathrm{Gal}\,(L/K)$:

(1) Sea $\sigma \in \mathrm{Gal}\,(L/K)$. Consideremos un elemento $\alpha \in L$. Por el Lema 2.1, existe un subcuerpo E_i de L que contiene a K tal que E_i/K es finita y de Galois. Por lo tanto, $N_i = \mathrm{Gal}\,(E_i/K) \in \mathcal{N}$ y así, σN_i es un elemento de $\mathcal{B}$ que contiene a σ.

(2) Supongamos que $\sigma \in \sigma_1 N_i \cap \sigma_2 N_j$. Entonces,

$$\sigma_1 N_i \cap \sigma_2 N_j = \sigma N_i \cap \sigma N_j = \sigma\left(N_i \cap N_j\right).$$

Por Lema 2.2, $N_i \cap N_j \in \mathcal{N}$, de modo que $\sigma\left(N_i \cap N_j\right)$ es un elemento de $\mathcal{B}$. Este conjunto está contenido en $\sigma_1 N_i \cap \sigma_2 N_j$ y contiene a σ.

Por lo tanto, $\mathcal{B}$ es una base para una topología sobre el grupo de Galois $\mathrm{Gal}\,(L/K)$. □

Definición 2.1. A la topología generada por $\mathcal{B} = \{\sigma N_i : \sigma \in G, N_i \in \mathcal{N}\}$ sobre $\mathrm{Gal}\,(L/K)$ la llamaremos *Topología de Krull.* En esta topología, un subcojunto $U \subseteq G$ es abierto si y sólo si $U = \emptyset$ o bien U es la unión de elementos de $\mathcal{B}$.

2.2. El Teorema de Krull

El propósito de esta sección es dar la versión del Teorema Fundamental de la Teoría de Galois para extensiones algebraicas de cualquier grado.

Teorema 2.2. *Sea* H *un subgrupo de* $G = \mathrm{Gal}(L/K)$. *Entonces* $\overline{H} = \mathrm{Gal}\,(L/\mathcal{F}\,(H))$, *la clausura de* H *en la topología de* G.

Demostración. Denotemos $H_1 = \mathrm{Gal}\,(L/\mathcal{F}\,(H))$. Es claro que $H \subseteq H_1$; luego, $\overline{H} \subseteq \overline{H_1}$. Probemos que H_1 es cerrado en G y que $H_1 \subseteq \overline{H}$.

Sea $\sigma \in G \setminus H_1$. Entonces $\sigma \notin H_1$, por lo que existe algún $\alpha \in \mathcal{F}(H)$ tal que

$$\sigma(\alpha) \neq \alpha.$$

Por el Lema 2.1, existe $E_i \in \mathcal{I}$ con $\alpha \in E_i$. Sea $N_i = \mathrm{Gal}(L/E_i) \in \mathcal{N}$ y tomemos $U = \sigma N_i$, el cual es abierto en G por definición de $\mathcal{B}$. Veamos que U y H_1 son disjuntos. Si no lo fuese, podríamos tomar τ satisfaciendo $\tau(\alpha) = \alpha$ y

$$\tau = \sigma\phi, \quad \text{para algún } \phi \in N_i,$$

en cuyo caso se tendría

$$\tau(\alpha) = \sigma\phi(\alpha) = \sigma(\alpha) \neq \alpha,$$

lo que es una contradicción. Por lo tanto, U y H_1 son disjuntos. Esto implica que $U \subseteq G \setminus H_1$. Concluimos que $G \setminus H_1$ es abierto en G, y así H_1 es cerrado en G.

Ahora probemos que $H_1 \subseteq \overline{H}$. Denotemos $F = \mathcal{F}(H)$. Sean

$$\sigma \in H_1, \quad N_i \in \mathcal{N}, \quad E_i = \mathcal{F}(N_i)$$

y

$$H_0 = \left\{\rho\,|_{E_i} : \rho \in H\right\}.$$

Entonces H_0 es un subgrupo del grupo finito $\mathrm{Gal}(E_i/K)$. Como

$$\mathcal{F}(H_0) = \mathcal{F}(H) \cap E_i = F \cap E_i,$$

por el Teorema Fundamental de la Teoría de Galois Finita tenemos

$$H_0 = \mathrm{Gal}(E_i/F \cap E_i).$$

Como $\sigma \in H_1$, tenemos $\sigma\,|_F = 1$; por lo que $\sigma\,|_{E_1} \in H_0$. Por lo tanto, existe $\rho \in H$ con $\rho\,|_{E_1} = \sigma\,|_{E_1}$. Así, $\sigma^{-1}\rho \in \mathrm{Gal}\,(E_i/K) = N_i$, por lo que

$$\rho \in \sigma N_i \cap H.$$

Esto significa que todo σN_1 perteneciente a la base $\mathcal{B}$ contiene algún elemento de H, por lo que $\sigma \in \overline{H}$. Esto prueba la inclusión $H_1 \subseteq \overline{H}$. En resumen,

$$\overline{H} \subseteq \overline{H_1} = H_1 \subseteq \overline{H},$$

es decir, $H_1 = \overline{H}$. □

Con la topología de Krull, el Teorema Fundamental de la Teoría de Galois para extensiones de Galois (algebraicas), queda formulado de la siguiente manera.

Teorema 2.3 (Teorema de Krull)**.** *Sea L/K una extensión de Galois y $G = \mathrm{Gal}\,(L/K)$. Con la topología de Krull, existe una correspondencia uno a uno, que revierte inclusiones, entre los cuerpos intermedios E de L/K y los subgrupos cerrados H de G, dado por*

$$E \overset{*}{\mapsto} \mathrm{Gal}\,(L/E), \quad H \overset{\star}{\mapsto} \mathcal{F}\,(H)$$

Además, si $E \leftrightarrow H$ entonces

(1) *$|G : H| < \infty$ si y solo si $[E : K] < \infty$ si y solo si H es abierto. Cuando esto ocurre, $|G : H| = [E : K]$.*

(2) *$H \triangleleft G$ si y sólo si E/K es de Galois. Cuando esto ocurre,* $\mathrm{Gal}\,(E/K) \cong G/H$.

Demostración. Análogamente a la prueba del teorema fundamental para el caso finito, se tiene que ambas correspondencias revierten inclusiones y que $E \overset{*}{\mapsto} \mathrm{Gal}\,(L/E)$ es inyectiva.

Para la suryectividad, sea H un subgrupo cerrado de G. Entonces, por el teorema anterior, $H = \overline{H} = \mathrm{Gal}\,(L/\mathcal{F}\,(H))$. Luego, $E = \mathcal{F}\,(H)$ es un cuerpo intermedio de la extensión L/K cuya

imagen por medio de $*$ es H. Así, $E \overset{*}{\mapsto} \mathrm{Gal}\,(L/E)$ es una correspondencia uno a uno entre los cuerpos intermedios E de L/K y los subgrupos cerrados H de G. Además, su inversa es $H \overset{\star}{\mapsto} \mathcal{F}\,(H)$ ya que

$$E \overset{*}{\mapsto} \mathrm{Gal}\,(L/E) \overset{\star}{\mapsto} \mathcal{F}\,(\mathrm{Gal}\,(L/E)) = E$$
$$H \overset{\star}{\mapsto} \mathcal{F}\,(H) \overset{*}{\mapsto} \mathrm{Gal}\,(L/\mathcal{F}\,(H)) = H.$$

Ahora supongamos que $E \leftrightarrow H$, donde H es un subgrupo cerrado de G. Tengamos presente que $H = \mathrm{Gal}\,(L/E)$ y $E = \mathcal{F}\,(H)$.

(1) Se probará que

$$|G : H| < \infty \Rightarrow H \text{ es abierto } \Rightarrow [E : K] < \infty \Rightarrow |G : H| < \infty.$$

- Supongamos que $|G : H| < \infty$. Entonces $G \setminus H$ es la unión finita de clases laterales de H. Como H es cerrado, cada una de las clases laterales también es cerrada, por lo cual $G \setminus H$ es cerrado. Así, H es abierto.

- Supongamos que H es abierto. Entonces para $1 \in H$ existe un σN_i en $\mathcal{B}$ tal que

$$1 \in \sigma N_i \subseteq H.$$

Luego, $\sigma N_i = 1N_i = N_i$. Es decir, $N_i \subseteq H$ para algún $i \in I$. Sea $F = \mathcal{F}\,(N_i)$; entonces, como la correspondencia revierte inclusiones, se tiene que $E \subseteq F$, donde además, $F \in \mathcal{I}$, por lo que $[F : K]$ es finito. Por el Teorema de la Torre,

$$[F : K] = [F : E]\,[E : K]\,,$$

lo que implica que $[E : K] < \infty$.

- Supongamos que $[E : K] < \infty$. Entonces la extensión E/K es finitamente generada;

digamos, $E = K(\alpha_1, \alpha_2, ..., \alpha_n)$ para ciertos $\alpha_1, \alpha_2, ..., \alpha_n$ en L. Por el Lema 2.1, existe E_i en $\mathcal{I}$ que contiene a estos generadores de E; luego, $E \subseteq E_i$. Sea $N_i = \text{Gal}(L/E_i)$. Entonces, por la reversión de inclusiones, N_i es un subgrupo de H. Por lo tanto,

$$|G : H| \leq |G : N_i| < \infty.$$

Ahora, bajo las condiciones anteriores, E/K es una extensión de Galois de grado finito, por lo que E está en $\mathcal{I}$ y por consiguiente, H está en $\mathcal{N}$. Luego, por el Lema 2.3, $|G : H| = [E : K]$.

(2) Supongamos que $H \triangleleft G$. Sea $\alpha \in E$ y consideremos el polinomio $\text{mín}(\alpha, K)$. Si β es otra raíz de este polinomio entonces el isomorfismo $\psi_{\alpha,\beta}$ se puede extender a un automorfismo $\sigma \in G$ de tal forma que $\sigma(\alpha) = \beta$. Si τ está en H entonces,

$$\tau(\beta) = \sigma^{-1}\left(\sigma\tau\sigma^{-1}(\alpha)\right).$$

Como $\sigma\tau\sigma^{-1}$ está en H y sus automorfismos fijan a E, entonces

$$\begin{aligned}\tau(\beta) &= \sigma^{-1}\left(\sigma\tau\sigma^{-1}(\alpha)\right)\\ &= \sigma^{-1}(\alpha)\\ &= \beta.\end{aligned}$$

Así, β está en el cuerpo fijo de H, el cual es E, por lo que $\text{mín}(\alpha, K)$ se descompone sobre E. Así, el polinomio mínimo de todo $\alpha \in E$ sobre K se descompone sobre E, lo cual implica que E/K es normal. Además, es separable ya que L/K lo es. Por lo tanto, E/K es una extensión de Galois.

Recíprocamente, supongamos que E/K es una extensión de Galois. Sea $\sigma \in G$. Como E/K es normal, el Teorema 1.15 implica que $\sigma|_E : E \hookrightarrow \overline{K}$ es un $K-$homomorfismo que induce un $K-$automorfismo de E. Esto permite definir la función $\theta : G \to \text{Gal}(E/K)$ por $\sigma \mapsto \sigma|_E$, la cual es un homomorfismo. El núcleo de θ está formado por los elementos de G que restringidos a E

son iguales al automorfismo identidad de Gal(E/K); es decir, los elementos de G que dejan fijo a E. Por lo tanto, $\ker\theta = \text{Gal}(L/E) = H$ y por consiguiente, H es normal en G ya que es el núcleo de un homomorfismo. Además, θ es suryectiva: En efecto, cualquier τ en Gal(E/K) se puede extender a un automorfismo σ en G de modo que $\sigma\,|_E = \tau$, lo que implica que $\theta(\sigma) = \sigma\,|_E = \tau$. Así, $\theta : G \to \text{Gal}(E/K)$ es un homomorfismo suryectivo, por lo que por el Primer Teorema de Isomorfismos,

$$\text{Gal}(E/K) \cong G/H.$$

□

Ejemplo 2.1. Sea L/K una extensión de Galois de grado finito. Entonces L está en $\mathcal{I}$. Por consiguiente, Gal$(L/L) = \{1\}$ está en la colección $\mathcal{N}$. Así, todo subconjunto U de Gal(L/K) es abierto en la topología de Krull ya que se puede escribir

$$U = \bigcup_{\sigma\in U} \sigma\{1\}.$$

Esto significa que la topología de Krull coincide con la topología discreta sobre Gal(L/K). Luego, todo subgrupo de Gal(L/K) es cerrado, lo que recupera el teorema fundamental para el caso finito.

2.3. Propiedades topológicas de Gal(L/K)

En esta sección se describe la estructura topológica del grupo de Galois de L/K.

Definición 2.2. En un espacio topológico, un conjunto es *clopen* si es abierto y cerrado.

Así tenemos que,

Teorema 2.4. *$\mathcal{B}$ es una base de conjuntos clopen.*

Demostración. Sea $G = \text{Gal}(L/K)$, $N_i \in \mathcal{N}$ y $\sigma \in G$. Entonces $N_i = \text{Gal}(L/E_i)$ para algún

$E_i \in \mathcal{I}$. Por el Lema 2.1, $[G : N_i]$ es finito, por lo que

$$G/N_i = \{N_i, \sigma_1 N_i, ..., \sigma_n N_i\}, \text{ para algún } n \in \mathbb{N}$$

y

$$\sigma G = \sigma N_i \cup \sigma\sigma_1 N_i \cup ... \cup \sigma\sigma_n N_i.$$

Entonces,

$$G \setminus \sigma N_i = \sigma\sigma_1 N_i \cup ... \cup \sigma\sigma_n N_i,$$

que es un abierto en la topología de Krull. Por lo tanto, σN_i es cerrado. □

Los próximos tres teoremas describen la estructura topológica del grupo de Galois como un espacio topológico Hausdorff, totalmente disconexo y compacto.

Teorema 2.5. $G = \text{Gal}\,(L/K)$ *es un espacio de Hausdorff.*

Demostración. Sean $\sigma, \tau \in G$, con $\sigma \neq \tau$. Por el Lema 2.2, sabemos que

$$\bigcap_{i \in \}I} \sigma N_i = \{\sigma\} \quad \text{y} \quad \bigcap_{i \in I} \tau N_i = \{\tau\}.$$

Como $\sigma \neq \tau$, existe $N_i \in \mathcal{N}$ tal que $\tau \notin \sigma N_i$. Sean $U = \sigma N_i$ y $V = G \setminus \sigma N_i$. Del Teorema 2.4 concluimos que U y V son abiertos en G; además, son disjuntos y satisfacen

$$\sigma \in U, \quad \tau \in V.$$

Por lo tanto, G es un espacio de Hausdorff. □

Teorema 2.6. $G = \text{Gal}\,(L/K)$ *es un espacio totalmente disconexo.*

Demostración. Sea $Y \subseteq G$ con al menos dos elementos σ y τ, con $\sigma \neq \tau$. Tomemos U y V como en el teorema anterior. Entonces el par U, V es una separación de G, por lo que el par $U \cap Y, V \cap Y$

es una separación de Y. Esto implica que Y no es conexo. Así, si Y es conexo entonces Y tiene solo un elemento. □

Para probar la compacidad de Gal (L/K) es necesario hacer uso de la topología producto.

Teorema 2.7. *$G = \text{Gal}\,(L/K)$ con la topología de Krull, es un espacio compacto.*

Demostración. Sea $P = \prod_{i \in I} G/N_i$ el producto directo de los grupos finitos G/N_i. Considere cada G/N_i con la topología discreta y dotemos a P con la topología producto. Note que G/N_i es Hausdorff ya que las clases laterales son disjuntas y compacto ya que G/N_i es un grupo finito. Entonces P es un espacio de Hausdorff y, por el Teorema de Tychonoff, P es compacto.

Sea $\sigma \in G$. Entonces $\sigma N_i \in G/N_i$, para todo $i \in I$. Considere $\mathbf{x}_\sigma = (x_i) \in P$ tal que

$$x_i = \sigma N_i, \text{ para todo } i \in I.$$

Esto nos permite definir una función $f : G \to P$ por

$$\sigma \mapsto \mathbf{x}_\sigma.$$

Afirmación 2.1. f es un homomorfismo de grupos.

En efecto, sean $\sigma, \tau \in G$. Entonces, $f(\sigma\tau) = \mathbf{x}_{\sigma\tau}$. Note que para todo $i \in I$ tenemos,

$$\begin{aligned} \mathbf{x}_{\sigma\tau}(i) &= \sigma\tau N_i \\ &= \sigma N_i \tau N_i \\ &= \mathbf{x}_\sigma(i)\,\mathbf{x}_\tau(i); \end{aligned}$$

es decir, $f(\sigma\tau) = \mathbf{x}_{\sigma\tau} = \mathbf{x}_\sigma \mathbf{x}_\tau = f(\sigma) f(\tau)$ y por lo tanto, f es un homomorfismo de grupos.

Afirmación 2.2. f es inyectiva.

Sea $\sigma \in \ker f$. Entonces $f(\sigma) = \mathbf{e}$ (la identidad de P); es decir, $e_i = N_i$ para todo $i \in I$. Luego, $\mathbf{x}_\sigma = \mathbf{e}$; lo que implica que para todo $i \in I$ se tiene $\sigma N_i = N_i$; o sea, $\sigma \in \bigcap_{i \in I} N_i$. De esta manera,

por el Lema 2.2, se llega a que $\sigma = 1$. Así, $\ker f = \{1\}$, lo que implica que f es inyectiva.

Afirmación 2.3. f es continua.

Sea $\pi_i : P \to G/N_i$ la proyección sobre la componente $i \in I$. Se observa que para todo $\sigma \in G$ se cumple

$$\pi_i(\mathbf{x}_\sigma) = \sigma N_i.$$

La colección $\{\tau N_i\}_{\tau \in G}$ es una base para la topología discreta sobre G/N_i; así que por definición de topología producto, todo conjunto abierto de P es la unión de intersecciones finitas de conjuntos de la forma $\pi_i^{-1}(\tau N_i)$, para ciertos $\tau \in G, i \in I$. Entonces, para probar que f es continua, es suficiente probar que $f^{-1}\left(\pi_i^{-1}(\tau N_i)\right)$ es abierto en G, para toda clase lateral τN_i. Observe que

$$\begin{aligned}
\sigma \in f^{-1}\left(\pi_i^{-1}(\tau N_i)\right) &\iff f(\sigma) \in \pi_i^{-1}(\tau N_i) \\
&\iff \pi_i(f(\sigma)) = \tau N_i \\
&\iff \pi_i(\mathbf{x}_\sigma) = \tau N_i \\
&\iff \sigma N_i = \tau N_i \\
&\iff \sigma \in \tau N_i,
\end{aligned}$$

por lo que $f^{-1}\left(\pi_i^{-1}(\tau N_i)\right) = \tau N_i$, que es un conjunto abierto en G.

Afirmación 2.4. $f^{-1} : \mathrm{Im} f \to G$ es continua.

Primero observe que $f(\tau N_i) = \pi_i^{-1}(\{\tau N_i\}) \cap \mathrm{Im} f$. En efecto,

$$\begin{aligned}
\mathbf{x} \in f(\tau N_i) &\Rightarrow \mathbf{x} \in \mathrm{Im} f \text{ y } \mathbf{x} = \mathbf{x}_\sigma, \text{ para algún } \sigma \in \tau N_i \\
&\Rightarrow \mathbf{x} \in \mathrm{Im} f \text{ y } \pi_i(\mathbf{x}) = \pi_i(\mathbf{x}_\sigma) = \sigma N_i, \text{ para algún } \sigma \in \tau N_i \\
&\Rightarrow \mathbf{x} \in \mathrm{Im} f \text{ y } \pi_i(\mathbf{x}) = \tau N_i, \quad \text{(ya que } \sigma \in \tau N_i) \\
&\Rightarrow \mathbf{x} \in \pi_i^{-1}(\tau N_i) \cap \mathrm{Im} f.
\end{aligned}$$

Por otro lado,

$$\begin{aligned}\mathbf{x} \in \pi_i^{-1}(\{\tau N_i\}) \cap \mathrm{Im} f &\Rightarrow \pi_i(\mathbf{x}) = \tau N_i \text{ y } \mathbf{x} = f(\sigma) = \mathbf{x}_\sigma, \text{ para algún } \sigma \in G. \\ &\Rightarrow \sigma N_i = \tau N_i \text{ y } \mathbf{x} = f(\sigma) = \mathbf{x}_\sigma, \text{ para algún } \sigma \in G \\ &\Rightarrow \mathbf{x} = f(\sigma) = \mathbf{x}_\sigma, \text{ para algún } \sigma \in \tau N_i \\ &\Rightarrow \mathbf{x} \in f(\tau N_i).\end{aligned}$$

Así, $f(\tau N_i) = \pi_N^{-1}(\{\tau N_i\}) \cap \mathrm{Im} f$, que es abierto en $\mathrm{Im} f$, por lo que f^{-1} es continua.

De las afirmaciones 2.2, 2.3 y 2.4 se deduce que de G y $\mathrm{Im} f$ son homeomorfos. El siguiente paso es probar que $\mathrm{Im} f$ es cerrado en P, de modo que $\mathrm{Im} f$, y por consiguiente G, heredan la compacidad que goza P.

En vista del Lema 2.3, existe un isomorfismo de G/N_i en Gal(E_i/K), donde $E_i = \mathcal{F}(N_i)$. Esto equivale a identificar τN_i con $\tau|_{E_i}$. Con esta identificación, para cada $\mathbf{x} \in P$ el elemento $\pi_i(\mathbf{x})$ es un $K-$automorfismo de E_i y para cada $\tau \in G$ tenemos que

$$\pi_i(f(\tau)) = \pi_i(\mathbf{x}_\tau) = \tau|_{E_i}.$$

Sea

$$C = \left\{\mathbf{x} \in P : \text{para } i, j \in I, \pi_i(\mathbf{x})|_{E_i \cap E_j} = \pi_j(\mathbf{x})|_{E_i \cap E_j}\right\}.$$

Afirmación 2.5. $C = \mathrm{Im} f$.

Sea $\mathbf{x} \in \mathrm{Im} f$. Entonces

$$\mathbf{x} = \mathbf{x}_\tau = f(\tau), \text{ para algún } \tau \in G.$$

Observe entonces que $\pi_i(\mathbf{x})$ es $\tau|_{E_i}$ y $\pi_j(\mathbf{x})$ es $\tau|_{E_j}$; luego, restringidos a $E_i \cap E_j$ los automorfismos $\pi_i(\mathbf{x})$ y $\pi_j(\mathbf{x})$ son iguales. Por lo tanto, $\mathbf{x} \in C$.

Sea ahora $\mathbf{x} \in C$. Definamos $\tau : L \to L$ como sigue: Sea $\alpha \in L$. Por el Lema 2.1, existe $E_i \in \mathcal{I}$

tal que $\alpha \in E_i$, donde $E_i = \mathcal{F}(N_i)$. Hemos identificado $\pi_i(\mathbf{x})$ con un $K-$automorfismo de E_i, por lo que se puede definir

$$\tau(\alpha) = \pi_i(\mathbf{x})(\alpha).$$

Esto define una función, pues no depende de E_i. En efecto, si $E_j \in \mathcal{I}$ tal que $\alpha \in E_j$ entonces $\alpha \in E_i \cap E_j$; luego, por la condición sobre C, se tiene

$$\pi_i(\mathbf{x})(\alpha) = \pi_i(\mathbf{x})(\alpha).$$

- Probemos que τ es un homomorfismo de anillos. Para ello, sean $\alpha, \beta \in L$. Por el Lema 2.1, existe $E_i \in \mathcal{I}$ tal que $\alpha, \beta \in E_i$. Como hemos identificado $\pi_i(\mathbf{x})$ con un $K-$automorfismo de E_i se tiene

$$\pi_i(\mathbf{x})(\alpha+\beta) = \pi_i(\mathbf{x})(\alpha) + \pi_i(\mathbf{x})(\beta) \quad \text{y} \quad \pi_i(\mathbf{x})(\alpha\beta) = \pi_i(\mathbf{x})(\alpha)\,\pi_i(\mathbf{x})(\alpha\beta),$$

es decir,

$$\tau(\alpha+\beta) = \tau(\alpha) + \tau(\beta) \quad \text{y} \quad \tau(\alpha\beta) = \tau(\alpha)\,\tau(\beta).$$

- Probemos que τ es biyectiva. Sea $\alpha \in L$. Como $\pi_i(\mathbf{x})$ es un $K-$automorfismo de E_i podemos definir $\sigma : L \to L$ por

$$\sigma(\alpha) = \pi_i^{-1}(\mathbf{x})(\alpha).$$

Entonces $\sigma = \tau^{-1}$, por lo que τ es biyectiva.

Por otro lado, es claro que τ fija los elementos de K, así $\tau \in G$. Además, como $\tau|_{E_i} = \pi_i(\mathbf{x})$, se tiene que $f(\tau) = \mathbf{x}$. Por lo tanto, $\mathbf{x} \in \operatorname{Im} f$.

Finalmente, probemos que C es cerrado en P, probando que $P \setminus C$ es abierto en P.

Sea $\mathbf{x} \in P \setminus C$. Entonces existen $i, j \in I$ tales que

$$\pi_i(\mathbf{x})|_{E_i \cap E_j} \neq \pi_j(\mathbf{x})|_{E_i \cap E_j}. \tag{2.3.1}$$

Considere el conjunto $U = \pi_i^{-1}(\pi_i(\mathbf{x})) \cap \pi_j^{-1}\left(\pi_j(\mathbf{x})\right) \subseteq P$. De inmediato se tiene que $\mathbf{x} \in U$.

Como $\pi_i(\mathbf{x})$ es abierto en la topología discreta de G/N_i, se tiene, por definición de topología producto, que $\pi_i^{-1}(\pi_i(\mathbf{x}))$ es abierto en P; lo mismo es válido para $\pi_j^{-1}\left(\pi_j(\mathbf{x})\right)$. Por lo tanto, U es abierto en P. Finalmente, U y C son disjuntos, pues de lo contrario existiría $\mathbf{y} \in P$ satisfaciendo

$$\pi_i(\mathbf{y}) = \pi_i(\mathbf{x}), \ \pi_j(\mathbf{y}) = \pi_j(\mathbf{x})$$

y

$$\pi_i(\mathbf{y}) \mid_{E_i \cap E_j} = \pi_j(\mathbf{y}) \mid_{E_i \cap E_j},$$

lo que es contrario a (2.3.1). Así, U y C son disjuntos y por lo tanto, $U \subseteq P \setminus C$.

En resumen, U es un conjunto abierto en P contenido en $P \setminus C$ y que contiene a $\mathbf{x}$. Esto significa que $P \setminus C$ es un conjunto abierto en P. Por lo tanto, C es cerrado.

Así, la compacidad de P implica que el conjunto cerrado C es compacto. □

Finalizamos el capítulo haciendo notar al lector que la demostración de la compacidad del grupo de Galois muestra que este puede ser visto como un subgrupo del producto directo de grupos finitos. Este hecho se generaliza con la estructura de límite inverso que se estudia en el siguiente capítulo.

Capítulo 3

Caracterización del grupo de Galois

El propósito de este capítulo es la caracterización del grupo de Galois, lo que proporcionará un lenguaje apropiado para el estudio de las extensiones algebraicas. Para ello, se explora la noción de sistema inverso, límite inverso y grupo profinito. La construcción del límite inverso es propia de la teoría de Categorías, la cual el lector puede consultar en Lang (2002).

Se mantiene la notación introducida a inicios del capítulo anterior:

- $\mathcal{I} = \{E_i \mid i \in I\}$ es la colección de cuerpos intermedios $K \subseteq E_i \subseteq L$, tales que E_i/K es una extensión de Galois de grado finito.
- $\mathcal{N} = \{N_i : i \in I\}$ es la colección de subgrupos $N_i = \mathrm{Gal}\,(L/E_i)$ del grupo de Galois de la extensión L/K, donde $E_i \in \mathcal{I}$.

Donde ambas colecciones están indexadas por el conjunto I.

3.1. Sistemas inversos

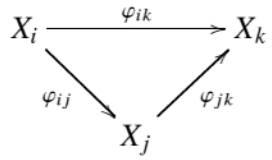
Definición 3.1. Sea $(I, \leq)$ un conjunto parcialmente ordenado. Se dice que $(I, \leq)$ es un *conjunto dirigido* si para todo $i, j \in I$ existe $k \in I$ tal que $i \leq k$ y $j \leq k$.

Es decir, en I siempre existirá un elemento "más grande" que dos elementos dados.

Definición 3.2. Sea $(I, \preceq)$ un conjunto dirigido y C una categoría. Un *sistema inverso* en C indexado por I es una familia de objetos $\{X_i : i \in I\}$ de C, junto con una familia de morfismos $\varphi_{ij} : X_i \to X_j$, con $j \preceq i$, que satisfacen las siguientes propiedades:

i) $\varphi_{ii} = \mathrm{id}_{X_i}$, donde id_{X_i} es el morfismo identidad sobre X_i.

ii) Si $k \preceq j \preceq i$ entonces $\varphi_{jk}\varphi_{ij} = \varphi_{ik}$; es decir, el diagrama conmuta



Notación. Al sistema inverso lo denotamos por $\{X_i, \varphi_{ij}, I\}$ o bien $\{X_i, \varphi_{ij}\}$, si es claro I.

Ejemplo 3.1. Sea L/K una extensión de Galois y consideremos la colección $\mathcal{I} = \{E_i \mid i \in I\}$, de subcuerpos E_i de L tales que E_i/K es una extensión de Galois finita. Definamos un sistema inverso indexado por I de la siguiente forma: sobre I considere la relación:

$$i \preceq j \text{ si y sólo si } E_i \subseteq E_j.$$

Entonces $(I, \preceq)$ es un conjunto parcialmente ordenado. Además, dados i, j en I, el subcuerpo $E_k = E_iE_j$ de L pertenece a $\mathcal{I}$ y contiene tanto a E_i como a E_j; es decir, existe $k \in I$ tal que $i \preceq k$ y $j \preceq k$. Esto prueba que $(I, \preceq)$ es un conjunto dirigido.

Para cada i en I, definamos el objeto

$$X_i = \mathrm{Gal}\,(E_i/K)\,.$$

Ahora, sean $i, j \in I$ tales que $E_j \subseteq E_i$; es decir, $j \preceq i$. Si $\sigma \in \mathrm{Gal}\,(E_i/K)$ entonces σ es un $K-$automorfismo de E_i; luego, $\sigma|_{E_j}$ es un $K-$automorfismo de E_j. Por lo cual, cuando $j \preceq i$ podemos definir la familia de morfismos

$$\varphi_{ij} : \mathrm{Gal}\,(E_i/K) \to \mathrm{Gal}\left(E_j/K\right)$$

por

$$\sigma \mapsto \sigma|_{E_j}$$

Observe que:

1) Puesto que para cada $\sigma \in \mathrm{Gal}\,(E_i/K)$ se tiene $\sigma = \sigma|_i$ entonces $\varphi_{ii} = \mathrm{id}_{X_i}$.

2) Si $k \preceq j \preceq i$ entonces, dado $\sigma \in \mathrm{Gal}\,(E_i/K)$ se tiene

$$\sigma \overset{\varphi_{ij}}{\longmapsto} \sigma|_{E_j} \overset{\varphi_{jk}}{\longmapsto} \sigma|_{E_k} = \varphi_{ik}\,(\sigma)\,;$$

es decir,

$$\varphi_{jk}\varphi_{ij} = \varphi_{ik}.$$

Así, $\left\{X_i, \varphi_{ij}, I\right\}$ es un sistema inverso en la categoría de grupos.

Podemos definir otro sistema inverso relacionado a la extensión de Galois L/K como sigue:

Ejemplo 3.2. Sea L/K una extensión de Galois y consideremos la colección de subgrupos $\mathcal{N} = \{N_i : i \in I\}$ de $\mathrm{Gal}\,(L/K)$, donde $N_i = \mathrm{Gal}\,(L/E_i)$ y $E_i \in \mathcal{I}$. Dados $i, j \in I$ tal que $E_i \subseteq E_j$, sabemos que $N_j = \mathrm{Gal}\left(L/E_j\right) \subseteq \mathrm{Gal}\,(E_i/K) = N_i$, por lo que sobre I podemos definir la relación

$$i \preceq j \text{ si y sólo si } N_j \subseteq N_i.$$

Esta es una relación de orden parcial sobre I. Además, dados $i, j \in I$ tales que $N_i = \mathrm{Gal}\,(L/E_i)$ y $N_j = \mathrm{Gal}\left(L/E_j\right)$, el subcuerpo $E_k = E_iE_j$ pertenece a $\mathcal{I}$ y contiene tanto a E_i como a E_j, por lo que $N_k = \mathrm{Gal}\,(L/E_k)$ está en $\mathcal{N}$ y está contenido tanto en N_i como en N_j; es decir, existe $k \in I$ tal que $i \preceq k$ y $j \preceq k$. Esto implica que $(I, \preceq)$ es un conjunto dirigido.

Ahora bien, con base en el Lema 2.3, para cada $i \in I$ definamos

$$X_i = \mathrm{Gal}\,(L/K)\,/N_i.$$

Y para cada $i, j \in I$, con $j \preceq i$, definamos los morfismos

$$\varphi_{ij} : \mathrm{Gal}\,(L/K)\,/N_i \to \mathrm{Gal}\,(L/K)\,/N_j$$

por

$$\sigma N_i \longmapsto \sigma N_j.$$

Se observa que:

1) $\varphi_{ii} = \mathrm{id}_{X_i}$, para todo $i \in I$.

2) Si $k \preceq j \preceq i$ entonces, dado $\sigma N_i \in \mathrm{Gal}\,(L/K)\,/N_i$ se tiene

$$\sigma N_i \overset{\varphi_{ij}}{\longmapsto} \sigma N_j \overset{\varphi_{jk}}{\longmapsto} \sigma N_k = \varphi_{ik}\,(\sigma N_i)\,;$$

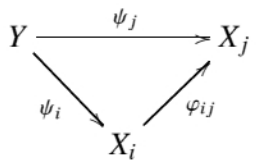
es decir,

$$\varphi_{jk}\varphi_{ij} = \varphi_{ik}.$$

Así, $\{X_i, \varphi_{ij}, I\}$ es un sistema inverso en la categoría de grupos.

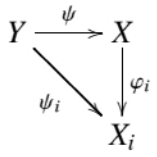
Observación 3.1. Por el Lema 2.3, si $N_i = \mathrm{Gal}\,(L/E_i)$ está en $\mathcal{N}$, entonces $\mathrm{Gal}\,(L/K)\,/N_i \cong \mathrm{Gal}\,(E_i/K)$. Esto significa que ambos sistemas inversos son equivalentes.

Definición 3.3. Si $\{X_i, \varphi_{ij}, I\}$ es un sistema inverso y Y es un objeto de C, una familia de aplicaciones $\psi_i : Y \to X_i$ $(i \in I)$ es compatible si $\varphi_{ij}\psi_i = \psi_j$ cuando $j \preceq i$.



Definición 3.4. Sea $\{X_i, \varphi_{ij}, I\}$ un sistema inverso. Se dice que un objeto X de C junto con una familia de morfismos compatibles $\varphi_i : X \to X_i$ $(i \in I)$ de C es un *límite inverso* del sistema inverso $\{X_i, \varphi_{ij}, I\}$, si satisface la siguiente propiedad universal: Para cualquier otro objeto Y de

C y cualquier familia $\psi_i : Y \to X_i$ $(i \in I)$ de morfismos compatibles, existe un único morfismo $\psi : Y \to X$ tal que $\varphi_i\psi = \psi_i$ para todo i; es decir, el siguiente diagrama conmuta

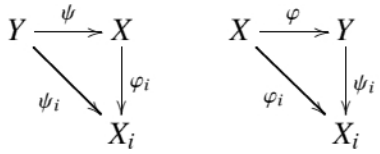


Notación. Si $\{X_i, \varphi_{ij}, I\}$ es un sistema inverso, denotemos su límite inverso por $\varprojlim_{i\in I} X_i$ o por $\varprojlim X_i$.

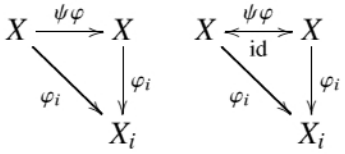
El límite inverso (si existe) está determinado de forma única por la propiedad universal.

Teorema 3.1. *El límite inverso (si existe) es único.*

Demostración. Si X con $\varphi_i : X \to X_i$ y Y con $\psi_i : X \to X_i$ son dos límites inversos del sistema inverso $\{X_i, \varphi_{ij}, I\}$, entonces, por la propiedad universal, existen únicos morfismos $\psi : Y \to X$ y $\varphi : X \to Y$ tales que los siguientes diagramas conmutan



Ahora considere los diagramas



Estos conmutan, para todo $i \in I$. Como, por definición, existe solo un morfismo que hace que cada este diagrama conmute, se tiene que $\psi\varphi = \mathrm{id}_X$. Similarmente, $\varphi\psi = \mathrm{id}_Y$. Por lo tanto, ψ es un isomorfismo. □

En el caso de un sistema inverso de grupos, el límite inverso existe, como lo muestra el siguiente teorema.

Teorema 3.2. *Para un sistema inverso de grupos* $\{G_i, \varphi_{ij}, I\}$*, el límite inverso* $\varprojlim_{i\in I} G_i$ *existe.*

Demostración. Considere $\prod_{i\in I} G_i$ y sea

$$G = \left\{ \mathbf{x} \in \prod_{i\in I} G_i \mid \varphi_{ij}(\mathbf{x}(i)) = \mathbf{x}(j), \text{ para todo } j \preceq i \right\}.$$

Claramente, $G \neq \phi$, ya que contiene a la túpla $\mathbf{x} \in \prod_{i\in I} G_i$ cuyas componentes son $\mathbf{x}(i) = e$ (la identidad de G_i).

Para cada $i \in I$, sea $\pi_i : G \to G_i$ el homomorfismo proyección restringido a G. Entonces,

$$\begin{aligned} \varphi_{ij}\pi_i(\mathbf{x}) &= \varphi_{ij}(\mathbf{x}(i)) \\ &= \mathbf{x}(j) \\ &= \pi_j(\mathbf{x}), \end{aligned}$$

lo que implica que la familia de homomorfismo π_i $(i \in I)$ es compatible. Probemos que G junto con la familia π_i $(i \in I)$ es el límite inverso del sistema $\{G_i, \varphi_{ij}, I\}$.

Supongamos que H es cualquier otro grupo y $\psi_i : H \to G_i$ $(i \in I)$ cualquier otra familia de homomorfismos compatibles con el sistema inverso (esto es, $\varphi_{ij}\psi_i = \psi_j$ para $j \preceq i$). Definamos la aplicación $\psi : H \to \prod_{i\in I} G_i$ por

$$h \to \mathbf{x}, \text{ donde } \mathbf{x}(i) = \psi_i(h), \text{ para todo } i \in I.$$

La aplicación ψ es un homomorfismo ya que si $h_1, h_2 \in H$ entonces $\psi(h_1 h_2)$ es la túpla $\mathbf{x}$ cuya i-ésima componente es $\psi_i(h_1 h_2) = \psi_i(h_1)\psi_i(h_2)$. Ésta es la i-ésima componente del producto de las tuplas cuyas i-ésimas componentes son $\psi_i(h_1)$ y $\psi_i(h_2)$, respectivamente. Por lo tanto, ψ es un homomorfismo.

Ahora, si $\mathbf{x} \in \psi(H)$. Entonces existe h en H tal que

$$\mathbf{x}(i) = \psi_i(h);$$

luego, para todo $j \preceq i$,

$$\begin{aligned}\varphi_{ij}(\mathbf{x}(i)) &= \varphi_{ij}(\psi_i(h)) \\ &= \psi_j(h) \\ &= \mathbf{x}(j),\end{aligned}$$

lo cual implica que $\mathbf{x} \in G$. Así, ψ es una función de H en G.

Por otro lado, para todo h en H,

$$\begin{aligned}\pi_i\psi(h) &= \pi_i(\mathbf{x}), \text{ donde } \mathbf{x}(i) = \psi_i(h) \\ &= \psi_i(h);\end{aligned}$$

esto es, $\pi_i\psi = \psi_i$ para todo i.

Finalmente, para la unicidad de ψ, si $\psi' : H \to G$ es otro homomorfismo que satisface $\pi_i\psi' = \psi_i$, entonces para cada h en H, $\mathbf{x}(i) = \psi_i(h) = \pi_i\psi'(h)$, lo cual implica que para cada $i \in I$, la i-ésima coordenada de $\psi'(h) \in G$ es precisamente, $\mathbf{x}(i)$. Por lo tanto, $\psi(h) = \psi'(h)$, para todo h en H.

Por lo tanto,

$$G = \varprojlim G_i.$$

□

Ejemplo 3.3. Sea L/K una extensión de Galois y consideremos el sistema inverso $\{X_i, \varphi_{ij}, I\}$ del Ejemplo 3.1. Aquí, $X_i = \mathrm{Gal}(E_i/K)$, donde E_i/K es una extensión de Galois finita. Entonces, el teorema anterior implica que G junto con la familia de proyecciones π_i $(i \in I)$ es el límte inverso de este sistema:

$$G = \varprojlim X_i = \varprojlim \mathrm{Gal}(E_i/K),$$

Es decir, el límite inverso del sistema inverso de subgrupos de Galois $\mathrm{Gal}(E_i/K)$ es

$$G = \left\{ \mathbf{x} \in \prod_{i \in I} \mathrm{Gal}(E_i/K) \mid \varphi_{ij}(\mathbf{x}(i)) = \mathbf{x}(j), \text{ para todo } j \preceq i \right\}.$$

Así, el límite inverso es el subgrupo de $\prod_{i \in I} \mathrm{Gal}(E_i/K)$ para el cual cuando $j \preceq i$, la componente $j-$ésima es un automorfismo $\sigma \in \mathrm{Gal}(E_i/K)$ restringido a E_j.

3.2. Grupos profinitos

En esta sección se probará el isomomorfismo entre los grupos G y $\mathrm{Gal}(L/K)$, lo cual caracterizará al grupo de Galois de la extensión L/K.

Teorema 3.3. *Sea L/K una extensión de Galois y $\{X_i, \varphi_{ij}, I\}$ el sistema inverso para el cual $X_i = \mathrm{Gal}(E_i/K)$, con E_i/K es una extensión de Galois finita. Entonces la función*

$$\chi : \mathrm{Gal}(L/K) \to \varprojlim \mathrm{Gal}(E_i/K)$$

definida por

$$\sigma \mapsto \mathbf{x}, \text{ tal que } \mathbf{x}(i) = \sigma|_{E_i} \quad (i \in I)$$

es un isomorfismo de grupos.

Demostración. Sean $\sigma, \tau \in \mathrm{Gal}(L/K)$. Entonces, la i-ésima componente de $\chi(\sigma\tau)$ es $\sigma\tau|_{E_i}$, de $\chi(\sigma)$ es $\sigma|_{E_i}$ y de $\chi(\tau)$, es $\tau|_{E_i}$. Luego, la i-ésima componente de $\chi(\sigma)\chi(\tau)$ es precisamente, $\chi(\sigma\tau)$. Por lo tanto χ es un homomorfismo de grupos.

Para la inyectividad de χ, si $\chi(\sigma) = \mathbf{e}$, donde $\mathbf{e}(i) = 1|_{E_i}$ para todo $i \in I$ entonces $\sigma|_{E_i} = 1_{E_i}$. Como $L = \bigcup_{i \in I} E_i$, se tiene $\sigma = 1$. Por tanto, $\ker\chi = \{1\}$, lo que implica que χ es inyectiva.

Para la suryectividad, sea $\mathbf{x} \in \varprojlim \mathrm{Gal}(E_i/K)$. Definamos $\sigma : L \to L$ como sigue: Por el Lema 2.1, para cada $\alpha \in L$, existe E_i en $\mathcal{I}$ tal que $\alpha \in E_i$. Sea $\sigma(\alpha) = x_i(\alpha)$, donde recordemos que x_i es un automorfismo en $\mathrm{Gal}(E_i/K)$. De esta forma, definimos σ sobre todo L. Se debe probar

que $\sigma \in \mathrm{Gal}(L/K)$. En primer lugar, note que σ fija los elementos de K puesto que cada x_i lo hace. Sean α, β en L. Entonces existe E_i en $\mathcal{I}$ conteniendo a α, β y además,

$$\begin{aligned}\sigma(\alpha\beta) &= x_i(\alpha\beta)\\ &= x_i(\alpha)\, x_i(\beta)\\ &= \sigma(\alpha)\,\sigma(\beta),\end{aligned}$$

lo que muestra que σ es un homomorfismo. Como $0 = \sigma(\alpha) = x_i(\alpha)$ implica que $\alpha = 0$, se tiene que σ es inyectiva. Y si $\beta \in L$ entonces existe E_i en $\mathcal{I}$ tal que $\alpha \in E_i$; luego, si tomamos $\alpha = x_i^{-1}(\beta) \in L$ entonces $\sigma(\alpha) = \beta$, lo que prueba que σ es suryectiva. Así, $\sigma \in \mathrm{Gal}(L/K)$.

Finalmente, por la forma en que se ha definido σ, se tiene que la componente i-ésima de $\chi(\sigma)$ coincide con la i-ésima de $\mathbf{x}$; esto es, $\chi(\sigma) = \mathbf{x}$, lo que prueba la suryectividad de χ.

Por lo tanto, $\chi : \mathrm{Gal}(L/K) \to \varprojlim \mathrm{Gal}(E_i/K)$ es un isomorfismo. □

Definición 3.5. Un *grupo profinito* es un grupo isomorfo a un sistema inverso de grupos finitos.

Por tanto, el grupo de Galois de una extensión de Galois es un grupo profinito. Ahora consideremos una topología sobre un grupo profinito de la siguiente manera:

Definición 3.6. Sea $G = \varprojlim G_i$ un grupo profinito; dotemos a cada G_i con la topología discreta y a $\prod_{i\in I} G_i$ con la topología producto. A la topología del subespacio sobre $G \subseteq \prod_{i\in I} G_i$ la llamaremos *topología profinita.*

Teorema 3.4. *Sea L/K una extensión de Galois y $\{X_i, \varphi_{ij}, I\}$ el sistema inverso para el cual $X_i = \mathrm{Gal}(E_i/K)$, con E_i/K una extensión de Galois finita. Entonces $\mathrm{Gal}(L/K)$ con la topología de Krull y $\varprojlim \mathrm{Gal}(E_i/K)$ con la topología profinita son homeomorfos. Este homeomorfismo viene dado por la función*

$$\chi : \mathrm{Gal}(L/K) \to \varprojlim \mathrm{Gal}(E_i/K)$$

definida por

$$\sigma \mapsto \mathbf{x}, \text{ tal que } \mathbf{x}(i) = \sigma|_{E_i} \quad (i \in I).$$

Demostración. Por el Teorema 3.3, la función χ es un isomomorfismo de grupos, por lo que es biyectiva. Así, solo falta probar que χ y χ^{-1} son continuas. Recordemos que los abiertos de la topología de Krull sobre $G = \mathrm{Gal}(L/K)$ son generados por la base $\mathcal{B} = \{\sigma N_i \mid \sigma \in \mathrm{Gal}(L/K), N_i \in \mathcal{N}\}$ y los abiertos de $\varprojlim \mathrm{Gal}(E_i/K)$ están generados por la subbase $\bigcup_{i\in I}\left\{\pi_i^{-1}(\{\sigma\}) \mid \sigma \in \mathrm{Gal}(E_i/K)\right\}$, donde π_i son las aplicaciones proyecciones restringidas a $\varprojlim \mathrm{Gal}(E_i/K)$.

Para probar que χ es continua, note que si $\sigma \in \mathrm{Gal}\left(E_j/K\right)$ entonces

$$\begin{aligned}
\chi^{-1}\left(\pi_j^{-1}(\{\sigma\})\right) &= \left\{\tau \in \mathrm{Gal}(L/K) \mid \chi(\tau) \in \pi_i^{-1}(\{\sigma\})\right\} \\
&= \{\tau \in \mathrm{Gal}(L/K) \mid \pi_i(\chi(\tau)) = \sigma\} \\
&= \left\{\tau \in \mathrm{Gal}(L/K) \mid \tau|_{E_i} = \sigma\right\} \\
&= \bigcup_{\tau\in G} \tau\mathrm{Gal}(L/E_i), \text{ donde } \tau|_{E_i} = \sigma.
\end{aligned}$$

Este último conjunto es un abierto en G con la topología de Krull. Así, χ es continua.

Para probar la continuidad de χ^{-1}, se probará que χ es una aplicación abierta. Sea σN_j en $\mathcal{B}$; luego, $\sigma \in G$ y $N_j = \mathrm{Gal}\left(L/E_j\right)$, para algún $j \in I$. Entonces,

$$\begin{aligned}
\chi\left(\sigma N_j\right) &= \left\{\mathbf{x} \in \varprojlim \mathrm{Gal}(E_i/K) \mid \mathbf{x}(i) = (\sigma\tau)|_{E_i}, \text{ para algún } \tau \in N_j\right\} \\
&\subseteq \left\{\mathbf{x} \in \varprojlim \mathrm{Gal}(E_i/K) \mid \mathbf{x}(j) = \sigma|_{E_j}\right\}, \text{ ya que } \tau \in N_j \\
&= \pi_j^{-1}\left(\left\{\sigma|_{E_j}\right\}\right).
\end{aligned}$$

Ahora, si $\mathbf{x} \in \pi_j^{-1}\left(\left\{\sigma|_{E_j}\right\}\right)$ entonces $\pi_j(\mathbf{x}) = \sigma|_{E_j}$. Como χ es suryectiva, existe ρ en G tal que $\chi(\rho) = \mathbf{x}$; o sea, $\mathbf{x}(i) = \rho|_{E_i}$. Además, como $\pi_j(\mathbf{x}) = \sigma|_{E_j}$, se tiene $\rho|_{E_j} = \sigma|_{E_j}$, por lo que $\left(\sigma^{-1}\rho\right)|_{E_j} = 1|_{E_j}$ (la identidad restringida a E_j). Esto que implica que $\tau = \sigma^{-1}\rho$ está en N_j y que $\mathbf{x}(i) = \rho|_{E_i} = (\sigma\tau)|_{E_i}$. Así, $\mathbf{x} \in \chi\left(\sigma N_j\right)$ y por tanto,

$$\pi_j^{-1}\left(\left\{\sigma|_{E_j}\right\}\right) \subseteq \chi\left(\sigma N_j\right).$$

De este modo, $\chi\left(\sigma N_j\right) = \pi_j^{-1}\left(\left\{\sigma\mid_{E_j}\right\}\right)$, el cual es abierto en la topología de $\varprojlim \operatorname{Gal}(E_i/K)$. Por lo tanto, χ es un homeomorfismo y

$$\operatorname{Gal}(L/K) \approx \varprojlim \operatorname{Gal}(E_i/K).$$

□

Es decir, el grupo de Galois de una extensión L/K es, a la vez, isomorfo y homeomorfo a un grupo profinito.

Para finalizar este trabajo, utilizaremos la caracterización del grupo de Galois como grupo profinito para calcular el grupo de Galois de algunas extensiones algebraicas de grado infinito.

Ejemplo 3.4. Sea p un número primo. Para cada $n \in \mathbb{N}$, denotemos ζ_{p^n} a una raíz primitiva p^n−ésima de la unidad sobre $\mathbb{Q}$. Sea $S = \left\{\zeta_{p^n} \mid n \in \mathbb{N}\right\}$ y denotemos $\mathbb{Q}(\zeta_\infty) = \mathbb{Q}(S)$, el cuerpo generado por los elementos de S sobre $\mathbb{Q}$. La extensión $\mathbb{Q}(\zeta_\infty)/\mathbb{Q}$ es de Galois ya que $\mathbb{Q}(\zeta_\infty)$ es el cuerpo de descomposición de la familia de polinomios separables $\left\{x^{p^n} - 1 \mid n \in \mathbb{N}\right\} \subseteq \mathbb{Q}[x]$. Los subcuerpos intermedios de $\mathbb{Q}(\zeta_\infty)/\mathbb{Q}$ que son extensiones de Galois finitas de $\mathbb{Q}$ son de la forma $\mathbb{Q}\left(\zeta_{p^n}\right)/\mathbb{Q}$. Así,

$$\mathcal{I} = \left\{\mathbb{Q}\left(\zeta_{p^n}\right) \mid n \in \mathbb{N}\right\}.$$

Además, $\operatorname{Gal}\left(\mathbb{Q}\left(\zeta_{p^n}\right)/\mathbb{Q}\right) \cong \left(\mathbb{Z}/p^n\mathbb{Z}\right)^*$ (unidades del anillo $\mathbb{Z}/p^n\mathbb{Z}$). Ahora, sobre $\mathbb{N}$ consideramos la relación de orden parcial $n \preceq m$ si $\mathbb{Q}\left(\zeta_{p^n}\right) \subseteq \mathbb{Q}\left(\zeta_{p^m}\right)$. Es claro que $(\mathbb{N}, \preceq)$ es un conjunto dirigido. Finalmente, sea

$$\varphi_{mn} : \operatorname{Gal}\left(\mathbb{Q}\left(\zeta_{p^m}\right)/\mathbb{Q}\right) \to \operatorname{Gal}\left(\mathbb{Q}\left(\zeta_{p^n}\right)/\mathbb{Q}\right),$$

con $n \preceq m$, la reestricción. Entonces,

$$\left\{\operatorname{Gal}\left(\mathbb{Q}\left(\zeta_{p^n}\right)/\mathbb{Q}\right), \varphi_{mn}, \mathbb{N}\right\}$$

es un sistema inverso de grupos cuyo límite inverso es $\mathrm{Gal}\left(\mathbb{Q}\left(\zeta_\infty\right)/\mathbb{Q}\right)$. Por lo tanto,

$$\mathrm{Gal}\left(\mathbb{Q}\left(\zeta_\infty\right)/\mathbb{Q}\right) \cong \varprojlim \mathrm{Gal}\left(\mathbb{Q}\left(\zeta_{p^n}\right)/\mathbb{Q}\right) \cong \varprojlim \left(\mathbb{Z}/p^n\mathbb{Z}\right)^\times.$$

Observación 3.2. El anillo de enteros $p-$ádicos, denotado por $\mathbb{Z}_p$, se define como el límite inverso $\varprojlim \left(\mathbb{Z}/p^n\mathbb{Z}\right)$ (Fried y Jarden, 2008, p. 13). Además, $\varprojlim \left(\mathbb{Z}/p^n\mathbb{Z}\right)^\times = \mathbb{Z}_p^\times$. Por tanto, $\mathrm{Gal}\left(\mathbb{Q}\left(\zeta_\infty\right)/\mathbb{Q}\right)$ es el grupo de unidades del anillo $\mathbb{Z}_p$.

Ejemplo 3.5. Sea $\overline{\mathbb{F}_p}$ una clausura algebraica del cuerpo finito $\mathbb{F}_p$ (p primo). De la teoría de cuerpos finitos, sabemos que para cada $n \in \mathbb{N}$, $\mathbb{F}_p$ tiene una única extensión de Galois de grado n, la cual se denota por $\mathbb{F}_{p^n}$; y que $\mathrm{Gal}\left(\mathbb{F}_{p^n}/\mathbb{F}_p\right) \cong \mathbb{Z}/n\mathbb{Z}$. Luego, la unicidad antes mencionada significa que colección de subcuerpos intermedios de la extensión $\overline{\mathbb{F}_p}/\mathbb{F}_p$ que son extensiones de galois finitas de $\mathbb{F}_p$, es

$$\mathcal{I} = \left\{\mathbb{F}_{p^n} \mid n \in \mathbb{N}\right\}.$$

Ahora, de la teoría de cuerpos finitos también sabemos que $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n}$ si y solo si m divide a n. Luego, $\mathrm{Gal}\left(\mathbb{F}_{p^n}/\mathbb{F}_p\right) \subseteq \mathrm{Gal}\left(\mathbb{F}_{p^m}/\mathbb{F}_p\right)$ si y solo si m divide a n. Considere entonces sobre $\mathbb{N}$ la relación de orden parcial $m \preceq n$ si m divide a n. Es claro que $(\mathbb{N}, \preceq)$ es un conjunto dirigido. Finalmente, sea

$$\varphi_{mn} : \mathrm{Gal}\left(\mathbb{F}_{p^m}/\mathbb{F}_p\right) \to \mathrm{Gal}\left(\mathbb{F}_{p^n}/\mathbb{F}_p\right),$$

con $n \preceq m$, la reestricción. Entonces,

$$\left\{\mathrm{Gal}\left(\mathbb{F}_{p^n}/\mathbb{F}_p\right), \varphi_{mn}, \mathbb{N}\right\}$$

es un sistema inverso de grupos cuyo límite inverso es $\mathrm{Gal}\left(\overline{\mathbb{F}_p}/\mathbb{F}_p\right)$. Así,

$$\mathrm{Gal}\left(\overline{\mathbb{F}_p}/\mathbb{F}_p\right) \cong \varprojlim \mathrm{Gal}\left(\mathbb{F}_{p^n}/\mathbb{F}_p\right) \cong \varprojlim \mathbb{Z}/n\mathbb{Z}.$$

Observación 3.3. El grupo de Prüfer, denotado por $\hat{\mathbb{Z}}$, se define como el límite inverso $\varprojlim \mathbb{Z}/n\mathbb{Z}$.

Además, $\hat{\mathbb{Z}} \cong \prod_{p \text{ primo}} \mathbb{Z}_p$, donde $\mathbb{Z}_p$ es el anillo de enteros p-ádicos (Fried y Jarden, 2008, pp. 14-15).

Ejemplo 3.6. Consideremos la extensión $L/\mathbb{Q}$, donde L es el cuerpo generado al adjuntar a $\mathbb{Q}$ las raíces cuadradas de los números primos (Ejemplo 1.16). Como $L/\mathbb{Q}$ es algebraica, las extensiones de grado finito son finitamente generadas por una cantidad finita de raíces cuadradas de números primos distintos. Así, para cada $n \in \mathbb{N}$, hay un subcuerpo E_n de L de la forma $E_n = \mathbb{Q}\left(\sqrt{p_1}, \sqrt{p_2}, ..., \sqrt{p_n}\right)$, para ciertos números primos distintos $p_1, p_2, ..., p_n$. Note que cada $E_n/\mathbb{Q}$ es una extensión de Galois de grado finito. Por tanto, la colección de subcuerpos intermedios de la extensión $L/\mathbb{Q}$ que son extensiones de Galois finitas de $\mathbb{Q}$ es

$$\mathcal{I} = \left\{E_n = \mathbb{Q}\left(\sqrt{p_1}, \sqrt{p_2}, ..., \sqrt{p_n}\right) \mid n \in \mathbb{N}\right\}.$$

Además, como cualquier $\sigma \in \mathrm{Gal}\,(E_n/\mathbb{Q})$ envía $\sqrt{p}$ a uno de sus conjugados sobre $\mathbb{Q}$ (a $\sqrt{p}$ o a $-\sqrt{p}$), se tiene que σ tiene orden dos y de la teoría de grupos abelianos finitos, esto significa que $\mathrm{Gal}\,(E_i/\mathbb{Q})$ es un 2-grupo abeliano elemental; por lo tanto,

$$\mathrm{Gal}\,(E_n/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^n.$$

Ahora, sobre $\mathbb{N}$ consideramos la relación de orden parcial $n \preceq m$ si $E_n \subseteq E_m$ (Entonces, $E_n = \mathbb{Q}\left(\sqrt{p_1}, \sqrt{p_2}, ..., \sqrt{p_n}\right)$ y $E_m = \mathbb{Q}\left(\sqrt{p_1}, \sqrt{p_2}, ..., \sqrt{p_n}, \sqrt{p_{n+1}}, \sqrt{p_{n+2}}, ..., \sqrt{p_m}\right)$. Es claro que $(\mathbb{N}, \preceq)$ es un conjunto dirigido. Finalmente, sea $\varphi_{mn} : \mathrm{Gal}\,(E_m/\mathbb{Q}) \to \mathrm{Gal}\,(E_n/\mathbb{Q})$, con $n \preceq m$, la reestricción. Entonces,

$$\{\mathrm{Gal}\,(E_n/\mathbb{Q}), \varphi_{mn}, \mathbb{N}\}$$

es un sistema inverso de grupos cuyo límite inverso es $\mathrm{Gal}\,(L/\mathbb{Q})$. Por lo tanto,

$$\mathrm{Gal}\,(L/\mathbb{Q}) \cong \varprojlim \mathrm{Gal}\,(E_n/\mathbb{Q}) \cong \varprojlim (\mathbb{Z}/2\mathbb{Z})^n.$$

Observación 3.4. Lo anterior, junto con lo que determinamos en el Ejemplo 1.16, implican

$$\mathrm{Gal}\,(L/\mathbb{Q}) \cong \varprojlim (\mathbb{Z}/2\mathbb{Z})^n \cong \prod_{i=1}^{\infty} \mathbb{Z}/2\mathbb{Z}.$$

Ejemplo 3.7. Sea $K = \mathbb{C}(t)$ y $S = \left\{\sqrt[n]{t} \mid n \in \mathbb{N}\right\}$. Consideremos $L = K(S)$, el cuerpo que se obtiene adjuntando a K los elementos de S. Entonces L es el cuerpo de descomposición de la familia de polinomios $\{x^n - t \mid n \in \mathbb{N}\} \subseteq K[x]$ y, por lo tanto, L/K es normal. Además, es separable ya que K tiene característica cero. Así, L/K es una extensión de Galois. Para cada subextensión finita E_n/K contenida en L, donde $E_n = K\left(\sqrt[n]{t}\right)$, se tiene que $\mathrm{Gal}\,(E_n/K) \cong \mathbb{Z}/n\mathbb{Z}$. Sea

$$\mathcal{I} = \left\{E_n = K\left(\sqrt[n]{t}\right) \mid n \in \mathbb{N}\right\}.$$

Consideremos el conjunto dirigido $(\mathbb{N}, \preceq)$, donde $\preceq$ es la relación de orden parcial: $m \preceq n$ si m divide a n. Si $n \preceq m$ definamos $\varphi_{mn} : \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ por

$$\varphi_{mn}(a \bmod m) = a \bmod n.$$

Entonces $\{\mathbb{Z}/n\mathbb{Z}, \varphi_{mn}, \mathbb{N}\}$ es un sistema inverso de grupos cuyo límite inverso es

$$\mathrm{Gal}\,(L/K) = \varprojlim \mathbb{Z}/n\mathbb{Z} = \hat{\mathbb{Z}}.$$

Comentarios Finales

La correspondencia uno a uno que establece el Teorema Fundamental de la Teoría de Galois clásica solo es cierta cuando la extensión en cuestión es de grado finito. Para el caso de extensiones algebraicas de grado infinito fue necesario el uso de una topología, lo que evidencia algo muy común en Matemática. Por otro lado, las técnicas necesarias para calcular el grupo de Galois de extensiones de grado infinito las proporciona la teoría de Categorías por medio de la construcción del límite inverso de un sistema inverso de grupos.

Tomando como punto de partida lo expuesto en este trabajo, el lector puede avanzar en el conocimiento de otros tópicos como, por ejemplo,

- Una teoría de Galois donde se reemplace el cuerpo base por cualquiera otra estructura algebraica (anillo, álgebra, etc.).
- Las propiedades de los grupos profinitos y cómo éstos ayudan a entender la estructura del grupo de Galois.
- La aplicación de la teoría de Galois en la teoría de números y la ciencia, en general.
- Una teoría de Galois para ecuaciones en otros contextos de la Matemática, como lo pueden ser los sistemas de ecuaciones diferenciales.

Bibliografía

[1] Artin, E. (1998). *Galois Theory*. Dover Publications, Inc.

[2] Arsenault, J. (2015). *On Dedekind's "Über die Permutationen des Körpers aller algebraischen Zahlen"* [tesis de maestría, The University of Maine]. Electronic Theses and Dissertations. http://digitalcommons.library.umaine.edu/etd/2258

[3] Barrera, F. (2011). Una visiónn breve sobre la teoría de Galois y cogalois. *Miscelánea Matemática 53*, 139–151.

[4] Brzezinski, J. (2011). Galois groups and number theory. *Nordisk Matematisk Tidskrift, 59*(3-4), 144-177.

[5] Borceux, F. & Janelidze G. (2001). *Galois Theories*. Cambridge University Press.

[6] Chamizo, F. (2004). ¡Qué bonita es la teoría de Galois! [notas de clase]. http://matematicas.uam.es/~fernando.chamizo/libreria/fich/APalgebraII04.pdf

[7] Conrad, K. (2020). *Infinite Galois Theory* [minicurso]. Connecticut Summer School in Number Theory, Connecticut, Estados Unidos de América. https://ctnt-summer.math.uconn.edu/wp-content/uploads/sites/1632/2020/06/CTNT-InfGaloisTheory.pdf

[8] Dean, E. (2009). *Dedekind's treatment of Galois theory in the Vorlesungen*. Technical Report No. CMU-PHIL-184. https://www.cmu.edu/dietrich/philosophy/docs/tech-reports/184_Dean.pdf

[9] Edwards, H. (1984). *Galois Theory*. Springer-Verlag.

[10] Fenrick, M. (1998). *Introduction to Galois Correspondence*. Springer Science+Business Media New York.

[11] Fried, M. & Jarden, M. (2008). *Field Arithmetic*. Springer-Verlag.

[12] Gray, J. (2018). *A History of Abstract Algebra From Algebraic Equations to Modern Algebra.* Springer.

[13] Kiernan, B. M. (1971). The Development of Galois Theory from Lagrange to Artin. *Archive for History of Exact Sciences, 8*, 40-154.https://doi.org/10.1007/BF00327219

[14] Kleiner, I. (2007). *A History of Abstract Algebra*. Birkhäuser Boston.

[15] Koch, H. (2002). *Galois theory of p-extensions*. Springer-Verlag.

[16] Lang, S. (2002). *Algebra*. Springer-Verlag.

[17] Lang, S. (1994). *Algebraic Number Theory*. Springer-Verlag.

[18] McCarthy, P. (1976). *Algebraic Extensions of Fields*. Chelsea Publishing Company.

[19] Morandi, P. (1996). *Field and Galois Theory.* Springer-Verlag.

[20] Munkres, J. (2002). *Topología*. Pearson Educación, S.A.

[21] Neumann, P. (2011). *The mathematical writings of Évariste Galois*. European Mathematical Society.

[22] Ribes, L. & Zalesskii, P. (2010). *Profinite groups*. Springer-Verlag.

[23] Serre, J. (1997). *Galois Cohomolgy*. Springer-Verlag.

[24] Soundararajan, T. (1969). A Note on Classical Galois Theory. *Mathematische Annalen, 182*(4), 275-280.

[25] Stewart, I. (2015). *Galois Theory*. CRC Press.

[26] Venkataraman, M., & Soundararajan, T. (1965). On the completeness of Galois theories. *Journal of the Australian Mathematical Society, 5*(3), 374-379.

[27] Waterhouse, W. (1974). Profinite groups are galois groups. *Proceeding of the American Mathematical Society, 42*(2), 639-640.

[28] Weintraub, S. (2009). *Galois Theory*. Springer Science+Business Media.

[29] Wilson, J. (1997). *Profinite groups*. Clarendon Press.