Teoría de Galois y el Teorema Fundamental del Álgebra

Dellerlin Astrid Cepeda Orozco

Universidad Industrial de Santader
Facultad de Ciencias
Escuela de Matemáticas
Bucaramanga
2018

Teoría de Galois y el Teorema Fundamental del Álgebra

Dellerlin Astrid Cepeda Orozco

Director

Héctor Edonis Pinedo Tapia
Doctor en Matemáticas

Universidad Industrial de Santader
Facultad de Ciencias
Escuela de Matemáticas
Bucaramanga
2018

AGRADECIMIENTOS

Agradezco a Dios; a mi mamá Nancy Astrid Orozco y a mi papá John Fredy Cepeda, por el apoyo y el esfuerzo que han hecho toda la vida para que pueda cumplir todos los logros que he tenido hasta hoy y sé que para los que vendrán de aquí en adelante tendré el mismo apoyo y amor que ellos me han brindado siempre.

Quiero darle las gracias a mi novio Oscar Daniel Salazar por su apoyo emocional y amor, ya que siempre confió en mis capacidades, me dio fuerzas y animo cuando más lo necesitaba. A mi hermano Esteban Felipe Cepeda porque ha sido una motivación esencial en mi vida para cumplir mis metas y con ello poder ayudarlo a que sus sueños se hagan realidad.

Al profesor Héctor Pinedo por ser mi director de proyecto y por enseñarme la magia del álgebra, ya que con su exigencia en los parciales me mostró una nueva forma de aprender y entender el mundo de las matemáticas.

Finalmente quiero agradecer a mis compañeros y profesores, ya que en el trascurso de la carrera me enseñaron sus conocimientos y con ello reí, lloré, sufrí, gocé y aprendí de cada uno lecciones inolvidables.

Índice general

Introducción 9

1. Preliminares **11**
1.1. Preliminares de teoría de conjuntos 11
1.2. Preliminares de teoría de grupos, anillos y cuerpos 13

2. Extensiones de Campos **18**
2.1. Definiciones 18
2.2. Extensiones Normales 22
2.3. Extensiones Separables 24

3. Teoría de Galois **31**
3.1. Grupos de Galois 31
3.2. Teorema Fundamental De La Teoría De Galois 35

4. El Teorema Fundamental del Álgebra **42**
4.1. Consecuencias del Teorema Fundamental del Álgebra 45

5. Aplicación de la Teoría de Galois de dimensión infinita **48**

RESUMEN

TÍTULO: TEORÍA DE GALOIS Y EL TEOREMA FUNDAMENTAL DEL ÁLGEBRA.[1]

AUTOR: DELLERLIN ASTRID CEPEDA OROZCO. [2]

PALABRAS CLAVE: EXTENSIONES DE GALOIS, GRUPOS DE GALOIS, TEOREMA FUNDAMENTAL DE LA TEORÍA DE GALOIS, TEOREMA FUNDAMENTAL DEL ÁLGEBRA.

DESCRIPCIÓN:

El Teorema Fundamental del Álgebra establece que todo polinomio de coeficientes complejos tiene una raíz compleja. En otras palabras, el teorema asegura que el cuerpo de los números complejos ($\mathbb{C}$) *es algebraicamente cerrado.*

Este trabajo consiste dar una prueba detallada del Teorema Fundamental del Álgebra basados en la teoría de Galois. En el primer capítulo se abordarán algunos conceptos básicos de teoría de conjuntos como la definición de retículo y anti-isomorfismos de retículos; también encontraremos el teorema de Sylow para grupos finitos el cual es de mucha ayuda en la prueba del teorema.

En el segundo capítulo se proporcionaran los conceptos de extensiones normales y separables de campos, necesarios para definir que es una extensión de Galois y con ello la construcción del grupo de Galois.

En el tercer capítulo presentaremos la Teoría de Galois donde la idea principal es asociar las extensiones de Galois con el grupo de Galois y mostrar su interacción en los diferentes resultados del Teorema Fundamental de la Teoría de Galois.

En el ultimo capítulo mostramos una aplicación de la teoría de Galois en dimensión infinita con ayuda de lo aprendido en el tercer capítulo y la concepción de sistema inverso de grupos.

[1] Trabajo de grado

[2] Facultad de Ciencias. Escuela de Matemáticas. Director: Dr. Héctor Edonis Pinedo Tapia.

ABSTRACT

TITLE: THEORY OF GALOIS AND THE FUNDAMENTAL THEOREM OF ALGEBRA.[3]

AUTHOR: DELLERLIN ASTRID CEPEDA OROZCO. [4]

KEYWORDS: EXTENSIONS OF GALOIS, GROUPS OF GALOIS, FUNDAMENTAL THEOREM OF THE THEORY OF GALOIS, FUNDAMENTAL THEOREM OF ALGEBRA.

DESCRIPTION:

The Fundamental Theorem of Algebra states that every polynomial of complex coefficients has a complex root. In other words, the theorem ensures that the field of complex numbers ($\mathbb{C}$) *is algebraically closed.*

This work consists of giving a detailed test of the Fundamental Theorem of Algebra based on the theory of Galois. In the first chapter some basic concepts of set theory will be approached, such as the definition of reticulum and anti-isomorphisms of lattices; we will also find Sylow theorem for finite groups which is very helpful in proof of the theorem.

In the second chapter the concepts of normal and separable extensions of fields will be provided, necessary to define that it is an extension of Galois and with it the construction of the Galois group.

In the third chapter we will present the Theory of Galois where the main idea is to associate the Galois extensions with the Galois group and show their interaction in the different results of the Fundamental Theorem of the Theory of Galois.

In the last chapter we show an application of the theory of Galois in infinite dimension with the help of what was learned in the third chapter and the conception of the inverse system of groups.

[3]Bachelor Thesis

[4]Facultad de Ciencias. Escuela de Matemáticas. Director: Dr. Héctor Edonis Pinedo Tapia.

INTRODUCCIÓN

El Teorema Fundamental del Álgebra establece que todo polinomio con coeficientes complejos de grado mayor que cero tiene una raíz compleja. Muchos matemáticos tuvieron inconvenientes para encontrar una respuesta a este problema, el primero en tratar de demostrar el teorema fue D'Alembert en 1746, seguido de Euler (1749), Foncenex (1759), Lagrange (1772), Laplace (1795) pero fue finalmente el príncipe de las matemáticas Carl Friedrich Gauss quien en 1797 dio la primera solución correcta al teorema.

Recordemos que un polinomio con coeficientes complejos es una función compleja de la forma

$$P(z) = a_n z^n + a_{n-1} z^{n-1} + ... + z_0.$$

Donde $\{a_0, a_1, ..., a_n\} \subseteq \mathbb{C}$ y $n \in \mathbb{N}$. Una raíz, o cero del polinomio, es $z_0 \in \mathbb{C}$ tal que $P(z_0) = 0$. Como los polinomios con coeficientes complejos son diferenciables en todo el dominio, en el lenguaje del análisis complejo son parte de la clase de las llamadas funciones enteras. En este contexto el Teorema Fundamental de Álgebra es consecuencia directa de un resultado general llamado el Teorema de Liouville. Este resultado establece que una función entera que está acotada en el plano complejo debe ser una constante.

En este trabajo un polinomio complejo será considerado como un objeto algebraico y en este contexto el Teorema Fundamental del Álgebra se puede enunciar como "el campo de los números complejos es algebraicamente cerrado". Para verificar tal resultado se presentarán nociones relativas a la construcción de extensiones de campos de allí se podrá deducir una prueba de que los polinomios reales de grado impar tienen una raíz real y que dado un polinomio irreducible $f(X) \in \mathbb{F}[X]$ con $\mathbb{F}$ un cuerpo, se puede construir una extensión $\mathbb{K}$ sobre el cuerpo $\mathbb{F}$ tal que $f(X)$ tiene una raíz en $\mathbb{K}$. Esta prueba sugiere la siguiente generalización del Teorema Fundamental del Álgebra. Si $\mathbb{K}$ es un cuerpo donde los polinomios de grado impar tiene raíces e $i = \sqrt{-1}$, entonces $\mathbb{K}(i)$ es algebraicamente cerrado.

La prueba generalizada involucra Teoría de Galois, en la cual la idea principal es asociar unos tipos especiales de extensiones de campos llamados extensiones de Galois y un grupo llamado el grupo de Galois. El libro guía de este trabajo será *The fundamental*

theorem of algebra de B. Fine y G. Rosenberger [2].

Para desarrollar esta idea el proyecto está estructurado de la siguiente manera: en el primer capítulo mostraremos los conceptos preliminares que son necesarios para el desarrollo del proyecto, como lo son el concepto de retículo, anti-isomorfismo, teoremas de Sylow, etc. Para ello nos guiaremos de los libros *Grupos, corpos e teoria de Galois* de Paulo A. Martin [7], *Abstract Algebra* de D.S. Dummit y R.M. Foote [1], *Advanced Modern Algebra* [8] y *An Introduction to Homological Algebra* de Joseph J.Rotman y [9].

En el segundo capítulo proporcionaremos los conceptos, teoremas y proposiciones necesarias de extensiones de campos, ya que la Teoría de Galois depende en parte de la teoría de grupos finitos y de las propiedades de normalidad y separabilidad de extensiones de campos con las cuales definen las extensiones de Galois y con esto construir el grupo de Galois.

En el tercer capítulo estudiaremos la Teoría de Galois y el Teorema Fundamental de la Teoría de Galois, el cual se basa en las propiedades de las extensiones de Galois, donde se ven reflejadas las propiedades del grupo de Galois, ya que son más fáciles de entender y demostrar, con ello mostraremos todos los resultados del Teorema Fundamental de la Teoría de Galois, en el se describe la interacción entre los subgrupos de Galois y cuerpos intermedios de las extensiones de Galois. Para esto nos basamos en los libros *The fundamental theorem of algebra* de B. Fine y G. Rosenberger [2], *Grupos, corpos e teoria de Galois* de Paulo A. Martin [7] y *Advanced Modern Algebra* de Joseph J.Rotman [8].

En el siguiente capítulo probaremos el Teorema Fundamental del Álgebra con ayuda de los conocimientos adquiridos en los capítulos anteriores. La prueba se seguirá por lo propuesto en el libro guía [2] y por algunas consecuencias que se encontraron en *Polinomios y Raíces* de Teresa Krick [5] y *Álgebra lineal* de Stanley I Grossman y Jose Job Flores Godoy [4].

En el último capítulo veremos una aplicación de la Teoría de Galois en dimensión infinita con ayuda de las notas *Direct limits, inverse limits, and profinite groups* basado en *Algebra* de S. Lang [6] en el cual se involucra el Teorema Fundamental de la Teoría de Galois visto en el capítulo 3.

Capítulo 1

Preliminares

En este capítulo presentaremos algunas definiciones, teoremas y ejemplos importantes para nuestro trabajo de teoría de conjuntos y álgebra moderna, que nos facilitarán las pruebas de los siguientes capítulos. Iniciaremos con las definiciones de retículos y anti-isomorfismo de retículos [7], que serán empleados en los capítulos 3 y 4; seguido de los Teoremas de Sylow para grupos finitos y el Teorema del Isomorfismo [10] y [1], utilizados en los capítulos 2, 3 y 4, y la definición de polinomios con coeficientes en un anillo R [10] y [5] que será empleada en el desarrollo del trabajo y para finalizar emplearemos el Teorema de Dedekind [7] para la algunas pruebas del capítulo 2.

1.1. Preliminares de teoría de conjuntos

Retículos

Una relación de orden parcial en un conjunto S es una relación $\leq$ que cumple:

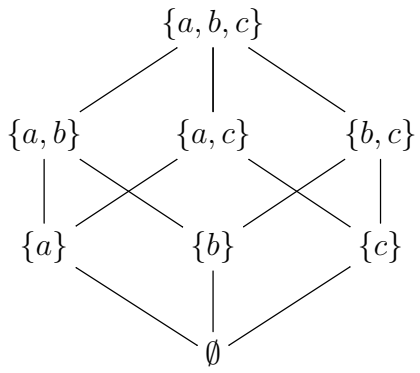
i) $x \leq x$, para todo $x \in S$;

ii) $x \leq y \wedge y \leq z \Longrightarrow x \leq z$, con $x, y, z \in S$;

iii) $x \leq y \wedge y \leq x \Longrightarrow x = y$, con $x, y \in S$.

Un retículo es un conjunto parcialmente ordenado S donde para todo par de elementos x, y de S, el conjunto $\{x, y\}$ posee supremo e ínfimo, denotados, respectivamente por $x \vee y$ y $x \wedge y$. Así mismo, fijando x y y, si $z \in S$ es una cota superior para $\{x, y\}$ entonces $x \vee y \leq z$. Del mismo modo, si $z \in S$ es una cota inferior para $\{x, y\}$, entonces $z \leq x \wedge y$.

Ejemplo 1.1.1. *Sea $S = \{a, b, c\}$, construiremos el retículo de partes de S con la relación $\subseteq$.*
Si $\mathscr{P}(S) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}$, entonces el retículo es:



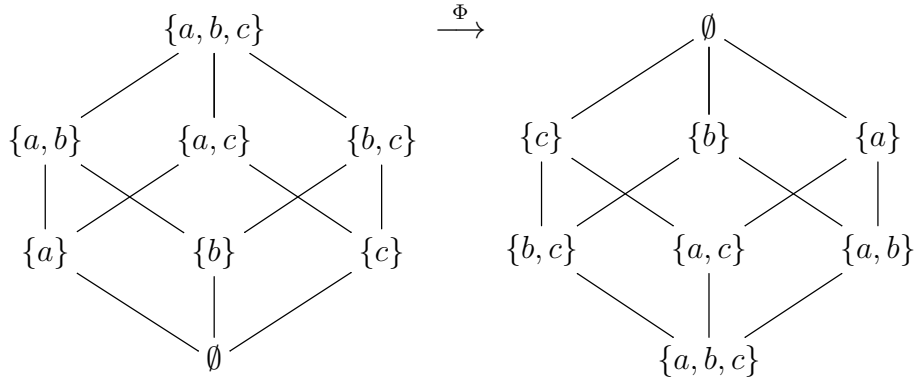
Definición 1.1.1. *Un* **anti-isomorfismo de retículos** $\Phi : S_1 \longrightarrow S_2$ *es una biyección que satisface*

$$\Phi(a \vee b) = \Phi(a) \wedge \Phi(b),$$
$$\Phi(a \wedge b) = \Phi(a) \vee \Phi(b).$$

Ejemplo 1.1.2. *Si $S = \{a, b, c\}$ y $\Phi : \mathscr{P}(S) \longrightarrow \mathscr{P}(S)$ tal que $A \mapsto \Phi(A) = S \backslash A$ entonces Φ es un anti-isomorfismo de retículos.*

Verifiquemos que para todo $x, y \in \mathscr{P}(S)$, $\Phi(x \vee y) = \Phi(x) \wedge \Phi(y)$ y $\Phi(x \wedge y) = \Phi(x) \vee \Phi(y)$.
$\Phi(\{a\}) = \Phi(\{a, b\} \cap \{a, c\}) = \Phi(\{a, b\}) \cup \Phi(\{a, c\}) = \{c\} \cup \{b\} = \{c, b\}$,
$\Phi(\{b\}) = \Phi(\{a, b\} \cap \{b, c\}) = \Phi(\{a, b\}) \cup \Phi(\{b, c\}) = \{c\} \cup \{a\} = \{c, a\}$,
$\Phi(\{c\}) = \Phi(\{c, b\} \cap \{a, c\}) = \Phi(\{c, b\}) \cup \Phi(\{a, c\}) = \{a\} \cup \{b\} = \{a, b\}$,
$\Phi(\{a, b\}) = \Phi(\{a\} \cup \{b\}) = \Phi(\{a\}) \cap \Phi(\{b\}) = \{b, c\} \cap \{a, c\} = \{c\}$,
$\Phi(\{c, b\}) = \Phi(\{c\} \cup \{b\}) = \Phi(\{c\}) \cap \Phi(\{b\}) = \{b, a\} \cap \{a, c\} = \{a\}$,
$\Phi(\{a, c\}) = \Phi(\{a\} \cup \{c\}) = \Phi(\{a\}) \cap \Phi(\{c\}) = \{b, c\} \cap \{a, b\} = \{b\}$,
$\Phi(\{a, b, c\}) = \emptyset$,
$\Phi(\emptyset) = \{a, b, c\}$.

Graficando los retículos correspondientes al anti-isomorfismo de retículos, tenemos:



1.2. Preliminares de teoría de grupos, anillos y cuerpos

Definición 1.2.1. *Sea G un grupo finito tal que $|G| = p^m\alpha$ con p un número primo, α un entero positivo y $mcd(p, \alpha) = 1$. Diremos que un* **p-subgrupo de Sylow** *es un subgrupo de G de orden p^m.*

Ejemplo 1.2.1. *Sea $G = \mathbb{Z}_{p_1^{\alpha_1}} \times \mathbb{Z}_{p_2^{\alpha_2}} \times \ldots \times \mathbb{Z}_{p_n^{\alpha_n}}$, donde p_i es un número primo y $p_i \neq p_j$ para todo $i, j \in \{1, 2..., n\}$. Tenemos que $H = \{0\} \times \{0\} \times ... \times \mathbb{Z}_{p_i^{\alpha_i}} \times ... \times \{0\}$ es un p_i-subgrupo de Sylow de G.*

Ejemplo 1.2.2. *Sea $G = D_n$ el grupo dihedral de n lados, con n par. Si τ es alguna reflexión en G entonces $\{\tau, id\}$ es un 2-subgrupo de Sylow.*

Ahora enunciaremos los **Teoremas de Sylow** para grupos finitos.

Teorema 1.2.1. *a.* **Existencia de p-subgrupos**. *Sea $0 \leq k \leq m$. El número de subgrupos de G de orden p^k es congruente con 1 módulo p. En particular, existen subgrupos de orden p^k.*

b. **p-subgrupos de Sylow son Conjugados**. *Sean Q y P dos p-subgrupo de Sylow, entonces existe $g \in G$ tal que $g^{-1}Qg = P$.*

c. **Número de p-subgrupos de Sylow**. *Sea k el número de p-subgrupos de Sylow de G. Luego k divide $|G|$ y $k - 1$ es divisible por p.*

Ahora escribiremos el **Teorema del Isomorfismo**.

Teorema 1.2.2. *Sea $f : G \longrightarrow H$ un homomorfismo de grupos , entonces $ker f \trianglelefteq G$ y*

$$G/kerf \cong imf.$$

En particular, si f es un epimorfismo

$$G/kerf \cong H.$$

Definición 1.2.2. *Un monoide multiplicativo es un conjunto no vació H con una operación binaria (multiplicativa) asociativa con unidad. Un homomorfismo de un monoide multiplicativo H en un cuerpo $\mathbb{F}$ es una función $f : H \longrightarrow \mathbb{F}$ tal que $f(1) = 1$ y $f(ab) = f(a)f(b)$.*

El siguiente lema será usado en el capítulo 2, la definición y demostración fue tomada de [7].

Lema 1.2.1. El Lema de Dedekind
Si G es un monoide multiplicativo, $\mathbb{K}$ un cuerpo y $\sigma_1, \cdots, \sigma_n : G \longrightarrow \mathbb{K}$ homomorfismos distintos y no nulos, entonces ellos son linealmente independientes sobre $\mathbb{K}$, es decir, si $a_1, \cdots, a_n \in \mathbb{K}$ satisfacen que

$$a_1\sigma_1(t) + a_2\sigma_2(t) + \cdots + a_n\sigma_n(t) = 0 \tag{1.1}$$

para todo $t \in G$, entonces $a_1 = a_2 = \cdots = a_n = 0$.

Demostración. La prueba se hará por inducción sobre el número de homomorfismos que hay de G en $\mathbb{K}$.
Si $n = 1$ el resultado es claro. Supongamos que $n > 1$ y que el resultado es válido para $n - 1$ homomorfismos, entonces por contradicción también podemos suponer que no todos los a_j en (1.1) son nulos. Como $\sigma_1 \neq \sigma_2$ existe $a \in G$ tal que $\sigma_1(a) \neq \sigma_2(a)$, entonces como (1.1) se cumple para todo $t \in G$, en particular como $at \in G$, entonces

$$a_1\sigma_1(at) + a_2\sigma_2(at) + \cdots + a_n\sigma_n(at) = 0,$$

como $\sigma_i(at) = \sigma_i(a)\sigma_i(t)$, tenemos que

$$a_1\sigma_1(a)\sigma_1(t) + a_2\sigma_2(a)\sigma_2(t) + \cdots + a_n\sigma_n(a)\sigma_n(t) = 0 \tag{1.2}$$

luego multiplicando en la ecuación (1.1) por $\sigma_1(a)$ obtenemos

$$\sigma_1(a)(a_1\sigma_1(t) + a_2\sigma_2(t) + \cdots + a_n\sigma_n(t)) = \sigma_1(a) \cdot 0 = 0$$

$$a_1\sigma_1(a)\sigma_1(t) + a_2\sigma_1(a)\sigma_2(t) + \cdots + a_n\sigma_1(a)\sigma_n(t) = 0 \tag{1.3}$$

Sustrayendo (1.2) de (1.3) obtenemos

$$b_2\sigma_2(t) + b_3\sigma_3(t) + \cdots + b_n\sigma_n(t) = 0, \tag{1.4}$$

donde $b_j = a_j(\sigma_j(a) - \sigma_1(a))$. Como $b_2 = a_2(\sigma_2(a) - \sigma_1(a)) \neq 0$ contradecimos la hipótesis de inducción. □

Definición 1.2.3. *Sea R un anillo, una expresión de la forma*

$$f(X) = a_0 + a_1X + \cdots + a_nX^n$$

con $n \in \mathbb{Z}^+, a_i \in R,\ i \in \{1, 2, \cdots, n\}$ es llamado **polinomio con coeficientes en R.** *Si $a_n \neq 0$, decimos que el grado de f es n y escribimos $\partial f(X) = n$.*

El conjunto

$$R[X] = \{f(X) = \sum_{i=1}^{n} a_iX^i : a_i \in R\ \forall i \in \{1, 2, \cdots, n\}\}$$

con la suma y el producto usuales, es llamado anillo de polinomios en la variable X con coeficientes en R.

Propiedades:

1. *Si R es conmutativo, $R[X]$ es conmutativo.*
2. *Si R tiene 1_R, $R[X]$ tiene $1_{R[X]}$ y $1_{R[X]} = 1_R$.*
3. *Dado $r \in R$ identificamos a r con el polinomio $r(X) = r$, es decir, tenemos que $R \subseteq R[X]$.*
4. *Dado R un anillo, tenemos el anillo $R_1 = R[X]$ y de igual forma podemos considerar el anillo de polinomios $R_1[Y] = R[X][Y] = R[X, Y]$ los elementos de este anillo son de la forma*

$$f(X, Y) = \sum_{i,j} a_{ij}X^iY^j$$

donde $(a_{ij})_{i,j}$ es casi nula y así, inductivamente, se construye el anillo de polinomios de n variables $R[X_1, X_2, \cdots, X_n]$.

Definición 1.2.4. *Sea R un anillo e $I \subseteq R$, tal que $(I, +)$ es subgrupo de $(R, +)$, entonces I es llamado*

- **Ideal a izquierda:** *Si dado $a \in R$ y $x \in I$ entonces $ax \in I$.*
- **Ideal a derecha:** *Si dado $a \in R$ y $x \in I$ entonces $xa \in I$.*
- **Ideal bilateral:** *Si es ideal a derecha y a izquierda.*

Definición 1.2.5. *Sea $S \subseteq R$ el ideal a izquierda (derecha o bilateral) más pequeño de R que contiene a S, es llamado ideal generado a izquierda (derecha o bilateral) por S.*

- **Ideal generador a izquierda:** $< S\} = \bigcap_{S \subseteq I \subseteq R} I.$
- **Ideal generador a derecha :** $\{S >= \bigcap_{S \subseteq I \subseteq R} I.$
- **Ideal generador bilateral:** $< S >= \bigcap_{S \subseteq I \subseteq R} I.$

Proposición 1.2.1. *Si R tiene 1_R y $S \neq \emptyset$ tenemos que:*

- $< S\} = \{r_1x_1 + r_2x_2 + \cdots + r_nx_n | r_i \in R, x_n \in S, n \in \mathbb{N}\}.$
- $\{S >= \{x_1r_1 + x_2r_2 + \cdots + x_nr_n | r_i \in R, x_n \in S, n \in \mathbb{N}\}.$
- $< S >= \{r_1x_1r_1^{'} + r_2x_2r_2^{'} + \cdots + r_nx_nr_n^{'} | r_i, r_i^{'} \in R, x_n \in S, n \in \mathbb{N}\}.$

Definición 1.2.6. *El ideal I de R es llamado* **principal**, *si existe $X \in R$ tal que $I =< X >$.*

Dado I un ideal de un anillo R, y dados $x, y \in I$ definamos la relación $\sim$ de la siguiente manera

$$x \sim y \Longleftrightarrow x - y \in I.$$

Esta relación $\sim$ es una relación de equivalencia. La clase de equivalencia de $x \in R$ es

$$\begin{aligned} \overline{x} &= \{y \in I | y \sim x\} \\ &= \{y \in I | y - x \in I\} \\ &= \{y \in I | y \in x + I\}, \end{aligned}$$

luego $\bar{x} = x + I = \{x + i | i \in I\}$.

Definición 1.2.7. *El* **anillo cociente** R/I *se define así:*

$$\begin{aligned} R/I &= \{\overline{x} | x \in R\} \\ &= \{x + I | x \in R\} \end{aligned}$$

Proposición 1.2.2. *Si I es un ideal de R, entonces R/I es un anillo con suma y producto dadas por*

$$\begin{aligned} \overline{x} + \overline{y} &= \overline{x + y} \\ \overline{x} \cdot \overline{y} &= \overline{x \cdot y} \end{aligned}$$

O de manera equivalente

$$\begin{aligned} (x + I) + (y + I) &= (x + y) + I \\ (x + I) \cdot (y + I) &= (x \cdot y) + I \end{aligned}$$

Que cumple las siguientes propiedades:

- *Si R es conmutativo entonces R/I es conmutativo.*
- *Si R tiene 1_R, la identidad de R/I es $1_R + I$ o 1_R.*
- *El cero de R/I es I.*

Capítulo 2

Extensiones de Campos

En este capítulo se proporcionaran los conceptos de extensiones normales y separables de campos, necesarios para definir que es una extensión de Galois y con ello la construcción del grupo de Galois. En las secciones 2.1 y 2.3 se presentaran las definiciones, teoremas y propiedades de extensiones de campos, guiados por los libros de D.S. Dummit y R.M. Foote [1] y K. Spindler [10]. En la sección 2.3 nos orientamos por el orden que impone el libro guía de este trabajo [2], pero en el cual omiten muchas demostraciones, por lo tanto vimos necesario recurrir a la ayuda del libro Advanced Modern Algebra de Rotman [8] para mostrar los detalles omitidos. Todos los resultados expuestos en el capítulo son necesarios para realizar la prueba del Teorema fundamental del álgebra.

2.1. Definiciones

Definición 2.1.1. *Sean* $\mathbb{L}$ *y* $\mathbb{F}$ *campos, si* $\mathbb{L} \subseteq \mathbb{F}$ *decimos que* $\mathbb{F}$ *es una* **extensión** *de* $\mathbb{L}$*. Escribiremos* $\mathbb{F}/\mathbb{L}$ *para decir que* $\mathbb{F}$ *es una extensión de* $\mathbb{L}$*.*

Definición 2.1.2. *Un* **campo intermedio** *de la extensión* $\mathbb{F}/\mathbb{L}$ *es un campo* $\mathbb{K}$ *tal que* $\mathbb{L} \subseteq \mathbb{K} \subseteq \mathbb{F}$*.*

Ejemplo 2.1.1. $\mathbb{R}$ *es un campo intermedio de la extensión* $\mathbb{C}/\mathbb{Q}$*.*

Definición 2.1.3. *Dada* $\mathbb{F}/\mathbb{L}$ *una extensión de campo,* $\alpha \in \mathbb{F}$ *es llamado* **algebraico** *sobre* $\mathbb{L}$ *si existe* $f(X) \in \mathbb{L}[X]$ *no nulo tal que* $f(\alpha) = 0$*. Si* α *no es algebraico entonces* α *es llamado* **trascendente***.*
Si todo elemento de $\mathbb{F}$ *es algebraico sobre* $\mathbb{L}$ *, decimos que* $\mathbb{F}/\mathbb{L}$ *es una* **extensión algebraica***.*

Ejemplo 2.1.2. $\alpha = i \in \mathbb{C}$ *es algebraico sobre* $\mathbb{R}$*, pues es la raíz de* $f(X) = X^2 + 1 \in \mathbb{R}[X]$*.*

Ejemplo 2.1.3. *$\alpha = \sqrt{3} \in \mathbb{R}$ es algebraico sobre $\mathbb{Q}$, pues es la raíz de $f(X) = X^2 - 3 \in \mathbb{Q}[X]$.*

Ejemplo 2.1.4. *$e, \pi \in \mathbb{R}$ son trascendentes sobre $\mathbb{Q}$.*

Definición 2.1.4. *Sea $\mathbb{F}/\mathbb{L}$ es una extensión de campos y $\alpha \in \mathbb{F}$ algebraico sobre $\mathbb{L}$, considere*

$$I_\alpha = \{f(X) \in \mathbb{L}[X] : f(\alpha) = 0\}.$$

Note que I_α es un ideal de $\mathbb{L}[X]$ e $I_\alpha \neq \{f(X) = 0\}$. Como $\mathbb{L}[X]$ es un dominio de ideales principales, ya que, $\mathbb{L}$ es cuerpo, entonces existe un único $P_\alpha(X)$ mónico, tal que

$$I_\alpha = \langle P_\alpha(X) \rangle.$$

$P_\alpha(X)$ es llamado **polinomio minimal** *de α.*

Proposición 2.1.1. *Si $\mathbb{F}/\mathbb{L}$ una extensión de campos, $\alpha \in \mathbb{F}$ algebraico sobre $\mathbb{L}$ tal que $I_\alpha = \langle P_\alpha(X) \rangle$. Las siguientes afirmaciones son equivalentes:*

1. *El grado de $P_\alpha(X)$ es minimal en I_α, es decir, es el polinomio de menor grado en I_α.*
2. *Dado $f(X) \in I_\alpha$, $P_\alpha(X)$ divide a $f(X)$.*
3. *$P_\alpha(X)$ es irreducible.*

Ejemplo 2.1.5. *Si p es un número primo, $n \in \mathbb{N}$ y $\alpha = \sqrt[n]{p}$, entonces $P_\alpha(X) \in \mathbb{Q}[X]$, ya que $P_\alpha(X) = X^n - p \in \mathbb{Q}[X]$.*

Ejemplo 2.1.6. *Si $\alpha = \sqrt{1 + \sqrt{3}}$, entonces $P_\alpha(X) = X^4 - 2X^2 - 2 \in \mathbb{Q}[X]$.*

Definición 2.1.5. *Si $\mathbb{F}/\mathbb{L}$ es una extensión de campos, entonces $\mathbb{F}$ puede considerarse como un espacio vectorial sobre $\mathbb{L}$. La dimensión de $\mathbb{F}$ sobre $\mathbb{L}$ es denotada por $[\mathbb{F} : \mathbb{L}]$ y es llamado el grado de $\mathbb{F}$ sobre $\mathbb{L}$. Decimos que la extensión $\mathbb{F}/\mathbb{L}$ es* **finita** *si $[\mathbb{F} : \mathbb{L}] < +\infty$.*

Ejemplo 2.1.7. *$[\mathbb{C} : \mathbb{R}] = 2$, luego $\mathbb{C}/\mathbb{R}$ es finita y algebraica.*

Ejemplo 2.1.8. *La dimensión de $\mathbb{R}$ como espacio vectorial sobre $\mathbb{Q}$ es infinita, entonces $[\mathbb{R} : \mathbb{Q}] = \infty$*

Ejemplo 2.1.9. *Si p es un número primo, la dimensión $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \cdots, \sqrt{p}, \cdots)$ sobre $\mathbb{Q}$ es infinita y $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \cdots, \sqrt{p}, \cdots)/\mathbb{Q}$ es una extensión algebraica.*

Nota Si $\mathbb{F}/\mathbb{L}$ es finita entonces es algebraica. Suponiendo que $[\mathbb{F} : \mathbb{L}] = n$ tenemos que todo $\alpha \in \mathbb{F}$ es algebraico sobre $\mathbb{L}$, luego $\{1, \alpha, \cdots, \alpha^n\}$ son linealmente dependientes, por lo tanto existen $a_1, a_2, \cdots, a_n$ tales que

$$\sum_{i=0}^{n} a_i \alpha^i = 0$$

con a_i no todos ceros.
Esto quiere decir que el polinomio $f(X) = a_0 + a_1 X + \cdots + a_n X^n \in \mathbb{L}[X]$ es no trivial y α es una raíz.
Ahora enunciaremos el ***Teorema de Kronecker***.

Teorema 2.1.1. *a) Si $f(X) \in \mathbb{L}[X] \backslash \mathbb{L}$ es un polinomio irreducible, entonces la función*

$$\begin{aligned} \iota : \mathbb{L} &\longrightarrow \frac{\mathbb{L}[X]}{\langle f(X) \rangle} \\ l &\longrightarrow l + \langle f(X) \rangle \end{aligned}$$

es monomorfismo. Luego, identificando a $\mathbb{L}$ con $\iota(\mathbb{L})$, tenemos que $f(X)$ tiene una raíz en $\frac{\mathbb{L}[X]}{\langle f(X) \rangle}$.

b) Si $f(X) \in \mathbb{L}[X] \backslash \mathbb{L}$ es un polinomio irreducible y α una raíz de $f(X)$, entonces

$$\Psi_\alpha : \frac{\mathbb{L}[X]}{\langle f(X) \rangle} \longrightarrow \mathbb{L}(\alpha)$$

es un isomorfismo.

c) Si $f(X) \in \mathbb{L}[X] \backslash \mathbb{L}$ es un polinomio irreducible, $\gamma = \mathbb{L} \longrightarrow \mathbb{L}$ un automorfismo con α y α' raíces de $f(X)$ y $\gamma(f(X))$ respectivamente, entonces existe un isomorfismo

$$\lambda : \mathbb{L}(\alpha) \longrightarrow \mathbb{L}(\alpha')$$

tal que,

i) $\lambda(\alpha) = \alpha'$,

ii) $\lambda | \mathbb{L} = \gamma$.

Demostración. a) Veamos que ι es monomorfismo.

Si $l \in ker(\iota)$, es decir, $\iota(l) = l + \langle f(X)\rangle = \langle f(X)\rangle$, entonces $l \in \langle f(X)\rangle$, así existe $g(X) \in \mathbb{L}[X]$ tal que $l = f(X)g(X)$, como $\partial(l) = \partial(f(X)g(X)) = 0$, por tanto $g(X) = 0$ y así $l = 0$.

Si $f(X) = \sum_{i=0}^{n} a_i X^i$, identificando $\mathbb{L}$ con $\iota(\mathbb{L})$ tenemos que

$$f(X) = \sum_{i=0}^{n} \overline{a_i} X^i \in \iota(\mathbb{L})[X],$$

donde $\overline{a_i} = a_i + \langle f(X)\rangle$, vamos a encontrar $\alpha \in \frac{\mathbb{L}[X]}{\langle f(X)\rangle}$ raíz de $f(X)$.
Si $\alpha = \overline{X} = X + < f(X) > \in \frac{\mathbb{L}[X]}{\langle f(X)\rangle}$,
entonces

$$f(\overline{X}) = \sum_{i=0}^{n} \overline{a_i}\,\overline{X^i} = \overline{\sum_{i=0}^{n} a_i X^i} = \overline{f(X)} = \overline{0},$$

por lo tanto $\overline{X}$ es raíz de $f(X)$.

b) Es consecuencia del Teorema del isomorfismo. Como

$$\begin{aligned} \mathbb{L}[X] &\longrightarrow \mathbb{L}(\alpha) \\ f(X) &\longrightarrow f(\alpha) \end{aligned}$$

es un epimorfismo. Y como α es raíz de $f(X)$ entonces $f(\alpha) = 0$, por lo tanto, $ker(\Psi_\alpha) =< f(X) >$.

c) La demostración se hará con base al siguiente diagrama

$$\begin{array}{ccc} \mathbb{L}(\alpha) & \longrightarrow & \mathbb{L}(\alpha') \\ \Psi_\alpha \uparrow & & \uparrow \psi_{\alpha'} \\ \frac{\mathbb{L}[X]}{\langle f(X)\rangle} & \longrightarrow & \frac{\mathbb{L}[X]}{\langle \gamma(f(X))\rangle}. \end{array}$$

Sea

$$\begin{aligned} \hat{\gamma} : \frac{\mathbb{L}[X]}{\langle f(X)\rangle} &\longrightarrow \frac{\mathbb{L}[X]}{\langle \gamma(f(X))\rangle} \\ h(X) + \langle f(X)\rangle &\longrightarrow \gamma(h(X)) + \langle \gamma(f(X))\rangle \end{aligned}$$

Veamos que $\hat{\gamma}$ está bien definida
Si $h(X) - h_1(X) \in \langle f(X)\rangle \Rightarrow \gamma(h(X)) - \gamma(h_1(X)) \in \langle \gamma(f(X))\rangle$, pues γ es un isomorfismo.
$\hat{\gamma}$ es un isomorfismo con inversa $\hat{\gamma}^{-1}$, donde

$$\hat{\gamma}^{-1} : \frac{\mathbb{L}[X]}{\langle f(X)\rangle} \longrightarrow \frac{\mathbb{L}[X]}{\langle \gamma^{-1}(f(X))\rangle}$$
$$h(X) + \langle f(X)\rangle \longrightarrow \gamma^{-1}(h(X)) + \langle \gamma(f(X))\rangle$$

Ahora, definamos $\lambda : \mathbb{L}(\alpha) \longrightarrow \mathbb{L}(\alpha')$, tal que $\lambda = \Psi_{\alpha'}\hat{\gamma}\Psi_{\alpha^{-1}}$, por lo tanto, λ es un isomorfismo.
Finalmente veamos *i*) y *ii*).

i) $\lambda(\alpha) = \Psi_{\alpha'}\hat{\gamma}\Psi_{\alpha^{-1}}(\alpha) = \Psi_{\alpha'}\hat{\gamma}(\alpha + \langle(f(X))\rangle) = \Psi_{\alpha'}(\gamma(\alpha) + \langle\gamma(f(X))\rangle) = \alpha'$.

ii) Si $l \in \mathbb{L}$, entonces
$\lambda(l) = \Psi_{\alpha'}\hat{\gamma}\Psi_{\alpha^{-1}}(l) = \Psi_{\alpha'}\hat{\gamma}(l + \langle(f(X))\rangle) = \Psi_{\alpha'}(\gamma(l)) + \langle\gamma(f(X))\rangle) = \gamma(l)$
Así $\lambda|\mathbb{L} = \gamma$.

□

2.2. Extensiones Normales

Para definir que es una extensión normal primero debemos saber que es un cuerpo de raíces para cualquier familia de polinomios.

Definición 2.2.1. *Sea $\mathbb{L}$ un campo y $\mathscr{F} \subseteq \mathbb{L}[X]\backslash\mathbb{L}$ una familia de polinomios no constantes. Un* **cuerpo de raíces** *de $\mathscr{F}$ sobre $\mathbb{L}$ es un cuerpo $\mathbb{F}$ tal que*
1. *Dado $f(X) \in \mathscr{F}$, $f(X)$ tiene todas las raíces en $\mathbb{F}$.*
2. *$\mathbb{F}$ es minimal respecto a **1.**, es decir, si $\mathbb{K}$ extensión de $\mathbb{L}$ tal que todo $f(X) \in \mathscr{F}$ tiene todas sus raíces en $\mathbb{K}$, entonces $\mathbb{F} \subseteq \mathbb{K}$.*

En este caso decimos que $\mathbb{F}/\mathbb{L}$ es una **extensión normal**.

Proposición 2.2.1. *Si $\mathbb{F}/\mathbb{L}$ es una extensión normal, entonces es algebraica.*

Demostración. Como $\mathbb{F}/\mathbb{L}$ es una extensión normal, el conjunto de los elementos de $\mathbb{F}$ que son algebraicos sobre $\mathbb{L}$, forma un subcuerpo de $\mathbb{F}$ llamado $\mathbb{E}$, el cual contiene a $\mathbb{L}$. Ya que $\mathbb{F} = \mathbb{L}(\mathscr{A})$, donde $\mathscr{A}$ es un conjunto de los elementos algebraicos en $\mathbb{F}$, entonces $\mathbb{F} \subset \mathbb{E}$. Concluimos que $\mathbb{E} = \mathbb{F}$ es algebraico sobre $\mathbb{L}$. □

Definición 2.2.2. *La* **clausura algebraica** *de* $\mathbb{L}$ *se define como el cuerpo de raíces de todos los polinomios no constantes en* $\mathbb{L}[X]$ *y se denota por* $\overline{\mathbb{L}}$.

Ejemplo 2.2.1. *Si* $\mathscr{F} = \{X^2 + 1\} \subseteq \mathbb{R}[X]$, *entonces* $\mathbb{C}$ *es el cuerpo de raíces de* $\mathscr{F}$, *por lo tanto* $\mathbb{C}/\mathbb{R}$ *es una extensión normal.*

Ejemplo 2.2.2. *Si* $\mathscr{F}$ *es la familia de polinomios sobre* $\mathbb{Q}$ *de la forma* $X^2 - p$ *con* p *primo, entonces,* $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}, ..., \sqrt{p}, ...)$ *es el cuerpo de raíces de* $\mathscr{F}$, *concluimos que* $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}, ..., \sqrt{p}, ...)$ *es una extensión normal de* $\mathbb{Q}$.

Ejemplo 2.2.3. $\mathbb{Q}(\sqrt[3]{2})$ *no es normal una extensión normal de* $\mathbb{Q}$, *ya que en* $\mathbb{Q}(\sqrt[3]{2})$ *no están todas las raíces del polinomio minimal* $X^3 - 2$. *Recordemos que si* $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ *es una extensión normal, todas las raíces del polinomio deben estar en* $\mathbb{Q}(\sqrt[3]{2})$.

$$X^3 - 2 = (X - \sqrt[3]{2}) \left(X + \frac{\sqrt[3]{2} - \sqrt{-3\sqrt[3]{4}}}{2} \right) \left(X + \frac{\sqrt[3]{2} + \sqrt{-3\sqrt[3]{4}}}{2} \right),$$

pero $\frac{\sqrt[3]{2} - \sqrt{-3\sqrt[3]{4}}}{2}, \frac{\sqrt[3]{2} + \sqrt{-3\sqrt[3]{4}}}{2} \notin \mathbb{Q}(\sqrt[3]{2})$.

El siguiente teorema nos garantiza la existencia de extensiones normales, también nos será útil, fue tomado del libro *Abstract Algebra with Applications* de K. Spindler [10], allí lo encontramos en la parte a) del Teorema 13.5.

Teorema 2.2.1. *Si* $\mathscr{F} \subseteq \mathbb{L}[X] \backslash \mathbb{L}$ *es una familia de polinomios no constantes en* $\mathbb{L}[X]$, *entonces* $\mathscr{F}$ *tiene cuerpo de raíces.*

Definición 2.2.3. *Un cuerpo* $\mathbb{F}$ *es* **algebraicamente cerrado**, *si dado* $f(X) \in \mathbb{F}[X] \backslash \mathbb{F}$, *existe* $\alpha \in \mathbb{F}$ *tal que* $f(\alpha) = 0$.

Ejemplo 2.2.4. $\mathbb{Q}$ *y* $\mathbb{R}$ *no son algebraicamente cerrados. Pues* $f(X) = X^2 + 1 \in \mathbb{R}[X]$ *no tiene raíces en* $\mathbb{R}$, *del mismo modo,* $f(X)$ *no tiene raíces en* $\mathbb{Q}$.

Ejemplo 2.2.5. *Si* $\mathbb{F}$ *es un cuerpo finito, entonces* $\mathbb{F}$ *no es algebraicamente cerrado, pues si* $\mathbb{F} = \{\alpha_1, ..., \alpha_n\}$, *el polinomio* $p(X) = (X - \alpha_1)...(X - \alpha_n) + 1$ *no tiene raíces en* $\mathbb{F}$.

Ejemplo 2.2.6. *La clausura algebraica denotada por* $\overline{\mathbb{L}}$ *de un cuerpo* $\mathbb{L}$ *es algebraicamente cerrada. Por ejemplo la clausura algebraica de* $\mathbb{Q}$ *es* $\overline{\mathbb{Q}}$ *y en particular* $\overline{\mathbb{Q}} \subset \mathbb{C} = \overline{\mathbb{R}}$ *ya que* e *y* π *son trascendentes sobre* $\mathbb{Q}$.

2.3. Extensiones Separables

Definición 2.3.1. *Si $f(X) \in \mathbb{L}[X]$, entonces existen $\alpha_1, \alpha_2, ..., \alpha_n \in \overline{\mathbb{L}}$ tal que*

$$f(X) = c(X - \alpha_1)^{m_1}(X - \alpha_2)^{m_2}...(X - \alpha_n)^{m_n}.$$

Decimos que m_i es la **multiplicidad** *de α_i.*
Si $m_i > 1$ decimos que α_i es **raíz múltiple**.
Si $m_i = 1$ decimos que α_i es **raíz simple**.

Definición 2.3.2. *$f(X) \in \mathbb{L}[X]$ es* **separable** *si todas sus raíces en $\overline{\mathbb{L}}$ son simples.*

Ejemplo 2.3.1. *$f(X) = X^2 - 2 \in \mathbb{Q}[X]$ es separable, pues $f(X) = (X - \sqrt{2})(X + \sqrt{2}) \in \overline{\mathbb{L}}$ y $\sqrt{2} \neq -\sqrt{2}$.*

Ejemplo 2.3.2. *Sea $f(X) = X^p - t^p \in \mathbb{Z}_p(t)[X]$, donde*

$$\mathbb{Z}_p(t) = \left\{ \frac{f(t)}{g(t)} : f(t), g(t) \in \mathbb{Z}_p, g(t) \neq 0 \right\}$$

y p primo.
Note que $X^p - t^p = (X - t)^p$, entonces t es una raíz con multiplicidad p, por lo tanto $f(X)$ no es separable.

Definición 2.3.3. *Si $\mathbb{L}$ es un campo y α algebraico sobre $\mathbb{L}$, decimos que $\alpha \in \mathbb{F}$ es separable, si $P_\alpha \in \mathbb{L}[X]$ es separable. Diremos que la extensión $\mathbb{F}/\mathbb{L}$ algebraica es separable, si para todo $\alpha \in \mathbb{F}$, α es separable.*

Ejemplo 2.3.3. *Considere $f(X) = X^p - t^p \in \mathbb{Z}_p(t)[X]$. Podemos construir $\mathbb{K}$ el cuerpo de raíces de $f(X)$, por lo tanto, $\mathbb{K}/\mathbb{Z}_p(t)$ es una extensión algebraica pero no es separable, pues t es una raíz de multiplicidad p.*

Definición 2.3.4. *Un cuerpo $\mathbb{F}$ tiene* **característica** *n, si n es el menor entero positivo tal que $n \cdot 1_\mathbb{F} = 0$ en $\mathbb{F}$. Denotaremos la característica por $\lambda(\mathbb{F})$. Si tal n no existe, diremos que $\mathbb{F}$ tiene característica cero.*

Ejemplo 2.3.4. *$\lambda(\mathbb{Q}) = \lambda(\mathbb{R}) = \lambda(\mathbb{C}) = 0$, y cualquier extensión de ellos tiene característica cero.*

Ejemplo 2.3.5. *$\lambda(\mathbb{Z}_p) = p$, y cualquier extensión de $\mathbb{Z}_p$ tiene característica p.*

Ejemplo 2.3.6. *La característica de un cuerpo es cero o cualquier primo. Supongamos que $\lambda(\mathbb{F}) = m$, con $m \in \mathbb{N}$. Por el Teorema Fundamental de la Aritmética tenemos:*

$$m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n},$$

con $\alpha_i, i \in \mathbb{N}$ y p_i primo. Como

$$m \cdot 1_{\mathbb{F}} = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n} \cdot 1_{\mathbb{F}} = 0,$$

entonces $p_1^{\alpha_1} \cdot 1_{\mathbb{F}} = 0$ o $p_2^{\alpha_2} \cdot 1_{\mathbb{F}} = 0$ o $\cdots$ o $p_n^{\alpha_n} \cdot 1_{\mathbb{F}} = 0$. Por lo tanto existe $p_i^{\alpha_i} \cdot 1_{\mathbb{F}} = 0$ y siguiendo el razonamiento anterior $p_i \cdot 1_{\mathbb{F}} = 0$, así $\lambda(\mathbb{F}) = p_i$ con p_i primo.

Proposición 2.3.1. *Si $\mathbb{K}$ es un campo y $f(X) \in \mathbb{K}[X]$ un polinomio irreducible. Entonces las siguientes condiciones son equivalentes:*

1. *$f(X)$ divide a $f'(X)$;*
2. *$f'(X) = 0$;*
3. *$\lambda(\mathbb{K})$ es un número primo, y $f(X) = g(x^p)$ para algún polinomio $g(X) \in \mathbb{K}[X]$;*
4. *$f(X)$ no es separable.*

Demostración.

- (1) $\Longrightarrow$ (2). Como el grado de $f'(X)$ es menor que $f(X)$ entonces $f'(X) = 0$.
- (2) $\Longrightarrow$ (3). Si $f(X) = \sum_{k=0}^{n} a_k X^k$ entonces $f'(X) = \sum_{k=1}^{n} k a_k X^{k-1}$; por lo tanto $f'(X) = 0$ si y solo si $k \cdot 1 = 0$ en $\mathbb{K}$ cuando $a_k \neq 0$. Así $f(X) = g(X^k)$.
- (3) $\Longrightarrow$ (4). Si α es una raíz de $f(X)$ en algún cuerpo de raíces de $f(X)$, entonces α^p es una raíz de $g(X)$ lo que significa que $X - \alpha^p$ divide a $g(X)$. Pero $(X-\alpha)^p = X^p - \alpha^p$ divide $g(X^p) = f(X)$ lo cual prueba que $f(X)$ no es separable.
- (4) $\Longrightarrow$ (2). Si $f(X) = g(X^p) = \sum_{k=0}^{n} a_k X^{pk}$ entonces $f'(X) = \sum_{k=0}^{n} pk a_k X^{pk-1} = 0$.
- (2) $\Longrightarrow$ (1) La implicación es clara.
- (4) $\Longrightarrow$ (1) Como $f(X)$ es separable, existe $\alpha \in \overline{\mathbb{K}}$, tal que, $f(X) = (X-\alpha)^m g(X)$, con $m > 1$ como $f(X)$ es irreducible, el polinomio minimal de α es igual a $f(X)$, ya que $m > 1$, α es raíz de $f'(X)$ pues

$$\begin{aligned} f'(X) =& m(X-\alpha)^{m-1} g(X) + (X-\alpha)^m g'(X) \\ f'(\alpha) =& 0, \end{aligned}$$

por lo tanto, $P_\alpha(X)|f'(X)$, así concluimos que $f(X)|f'(X)$.

□

Teorema 2.3.1. *Cualquier extensión de un cuerpo de característica cero es una extensión separable.*

Demostración. Por la parte 3) ⇔ 4) de la proposición 2.3.1. □

Las siguientes definiciones y demostraciones de los siguientes teoremas fueron tomadas de [8], las cuales fueron necesarias para entender el Corolario 2.3.1. ya que en el libro guía [2] no tenía prueba y es usado en el Teorema Fundamental de la Teoría de Galois.

Definición 2.3.5. *Si $G = \{\sigma_1, \cdots, \sigma_n\}$ es un grupo de automorfismos de $\mathbb{K}$, definimos*

$$\mathbb{K}^G = \{k \in \mathbb{K} : \sigma_i(k) = k \text{ con } 1 \leq i \leq n\}.$$

Teorema 2.3.2. *Si $G = \{\sigma_1, \cdots, \sigma_n\}$ es un grupo de automorfismos de $\mathbb{K}$, entonces $[\mathbb{K} : \mathbb{K}^G] \geq n$.*

Demostración. Supongamos $[\mathbb{K} : \mathbb{K}^G] = r < n$, sea $\{\alpha_1 \cdots, \alpha_r\}$ es una base de la extensión $\mathbb{K}/\mathbb{K}^G$. Consideremos el sistema lineal sobre $\mathbb{K}$ de r ecuaciones con n incógnitas.

$$\begin{aligned}
\sigma_1(\alpha_1)X_1 + \cdots + \sigma_n(\alpha_1)X_n &= 0 \\
\sigma_1(\alpha_2)X_1 + \cdots + \sigma_n(\alpha_2)X_n &= 0 \\
\vdots \qquad\qquad \vdots \qquad\qquad & \vdots \\
\sigma_1(\alpha_r)X_1 + \cdots + \sigma_n(\alpha_r)X_n &= 0.
\end{aligned} \tag{2.1}$$

Como $r < n$, hay una solución no trivial $(X_1, \cdots, X_n)$ del sistema anterior, es decir, $X_i \neq 0$ para algún $i \in \{1, 2, \cdots, n\}$. Para cualquier $\beta \in \mathbb{K}$, tenemos que $\beta = \sum_{i=1}^{r} b_i\alpha_i$ donde $b_i \in \mathbb{K}^G$ y $\alpha_i \in \mathbb{K}$. Multiplicando por b_i en la i-ésima fila en (2.1), obtenemos que

$$\begin{aligned}
b_1\sigma_1(\alpha_1)X_1 + \cdots + b_1\sigma_n(\alpha_1)X_n &= 0 \\
b_2\sigma_1(\alpha_2)X_1 + \cdots + b_2\sigma_n(\alpha_2)X_n &= 0 \\
\vdots \qquad\qquad \vdots \qquad\qquad & \vdots \\
b_r\sigma_1(\alpha_r)X_1 + \cdots + b_r\sigma_n(\alpha_r)X_n &= 0
\end{aligned}$$

como $b_i = \sigma_j(b_i)$ para todo i, j, tenemos

$$\begin{aligned}
\sigma_1(b_1\alpha_1)X_1 + \cdots + \sigma_n(b_1\alpha_1)X_n &= 0 \\
\sigma_1(b_2\alpha_2)X_1 + \cdots + \sigma_n(b_2\alpha_2)X_n &= 0 \\
\vdots \qquad\qquad \vdots \qquad\qquad & \vdots \\
\sigma_1(b_r\alpha_r)X_1 + \cdots + \sigma_n(b_r\alpha_r)X_n &= 0
\end{aligned}$$

Sumando todo el sistema obtenemos

$$\sigma_1(\beta)X_1 \cdots + \sigma_n(\beta)X_n = 0$$

por lo tanto se infringe la independencia de los automorfismos $\{\sigma_1, \cdots, \sigma_n\}$ que garantiza el Lema de Dedekind, pues β es un elemento arbitrario de $\mathbb{K}$. □

Teorema 2.3.3. *Si $G = \{\sigma_1, \cdots, \sigma_n\}$ es un grupo de automorfismos de $\mathbb{K}$, entonces $a[\mathbb{K} : \mathbb{K}^G] = n$.*

Demostración. Es suficiente probar que $[\mathbb{K} : \mathbb{K}^G] \leq n$. Supongamos que $[\mathbb{K} : \mathbb{K}^G] > n$. Sea $\{\omega_1, \cdots, \omega_{n+1}\}$ un conjunto de vectores linealmente independientes de $\mathbb{K}$ sobre $\mathbb{K}^G$. Consideremos el sistema de n ecuaciones con $n+1$ incógnitas.

$$\begin{aligned}
\sigma_1(\omega_1)X_1 + \cdots + \sigma_1(\omega_{n+1})X_{n+1} &= 0 \\
\sigma_2(\omega_1)X_1 + \cdots + \sigma_2(\omega_{n+1})X_{n+1} &= 0 \\
\vdots \qquad\qquad \vdots \qquad\qquad & \vdots \\
\sigma_n(\omega_1)X_1 + \cdots + \sigma_n(\omega_{n+1})X_{n+1} &= 0.
\end{aligned}$$

Hay una solución no trivial $(X_1, \cdots, X_{n+1}) \in \mathbb{K}^{n+1}$. Si escogemos una solución minimal de r componentes diferentes de cero, es decir, $(a_1, \cdots, a_r, 0, \cdots, 0)$. Para reindexar ω_i, consideraremos que la componentes no cero van primero. Note que $r \neq 1$, pues tendríamos que $\sigma_1(\omega_1)a_1 = 0$, entonces $a_1 = 0$.
Multiplicando por el inverso, si es necesario, podemos asumir que $a_r = 1$. Nuestra última suposición es que a_1 no pertenece a $\mathbb{K}^G$, por lo tanto existe σ_k tal que $\sigma_k(a_1) \neq a_1$, tenemos que

$$\begin{aligned}
\sigma_j(\omega_1)a_1 + \cdots + \sigma_j(\omega_r)a_r &= 0 \\
\sigma_j(\omega_1)a_1 + \cdots + \sigma_j(\omega_r)1 &= 0 \\
\sigma_j(\omega_1)a_1 + \cdots + \sigma_j(\omega_r) &= 0 \qquad (2.2)
\end{aligned}$$

aplicando σ_k en (2.2) obtenemos

$$\begin{aligned}\sigma_k\sigma_j(\omega_1)\sigma_k(a_1)+\cdots+\sigma_k\sigma_j(\omega_r)\sigma_k(a_r)&=0\\ \sigma_k\sigma_j(\omega_1)\sigma_k(a_1)+\cdots+\sigma_k\sigma_j(\omega_r)\sigma_k(1)&=0\\ \sigma_k\sigma_j(\omega_1)\sigma_k(a_1)+\cdots+\sigma_k\sigma_j(\omega_r)1&=0\\ \sigma_k\sigma_j(\omega_1)\sigma_k(a_1)+\cdots+\sigma_k\sigma_j(\omega_r)\sigma_k(a_r)&=0.\end{aligned}$$

Como G es un grupo y $\{\sigma_k\sigma_1,\cdots,\sigma_k\sigma_n\}$ es una permutación de $\{\sigma_1,\cdots,\sigma_n\}$, por lo tanto $\sigma_k\sigma_j=\sigma_i$ para la algún $0\leq 1\leq n$, y así tenemos

$$\sigma_i(\omega_1)\sigma_k(a_1)+\cdots+\sigma_i(\omega_r)=0$$

igualando con (2.2) en la fila i- ésima obtenemos que

$$\sigma_i(\omega_1)(a_1-\sigma_k(a_1))+...+\sigma_i(\omega_{r-1})(a_{r-1}-\sigma_k(a_{r-1}))=0$$

Como $a_1-\sigma_k(a_1)\neq 0$, podemos encontrar una solución no trivial de el sistema original teniendo menos de r componentes, lo cual es una contradicción pues r es minimal. □

Corolario 2.3.1. *Si n es el número de automorfismos de $\mathbb{K}$ que fijan $\mathbb{K}^G$ es igual la dimensión de $\mathbb{K}/\mathbb{K}^G$.*

A continuación proporcionaremos la prueba del ***Teorema del elemento primitivo*** que fue tomada del libro de Fraleigh [3].

Teorema 2.3.4. *Si $\mathbb{K}$ es una extensión finita y separable de $\mathbb{F}$, entonces $\mathbb{K}$ es una extensión simple, es decir, $\mathbb{K}=\mathbb{F}(\alpha)$ para algún $\alpha\in\mathbb{K}$.*
Tal α es llamado el elemento primitivo de $\mathbb{K}$ sobre $\mathbb{F}$.

Demostración. Si $\mathbb{F}$ es un cuerpo finito, entonces la extensión $\mathbb{K}$ también es finita. Supongamos que $\mathbb{K}^*$ es el grupo multiplicativo de los elementos no nulos de $\mathbb{K}$ el cual tiene n elementos, es decir, $\mathbb{K}^*=\{k_1,k_2,\cdots,k_n\}$, si r_i el orden de cada k_i, con $1\leq i\leq n$ entonces $k_i^{r_i}=1_{\mathbb{K}}$. Construyendo a $\alpha=(k_1\cdot k_2\cdots k_n)$ donde $\alpha^d=1$ con $d=m.c.m(r_1,r_2,r_3,\cdots,r_n)$, así tenemos que para todo $k_i\in\mathbb{K}^*$, $k_i^d=1_{\mathbb{K}}$, así el polinomio X^d-1 tiene d raíces, entonces, $n\leq d$. Así $1,\alpha,\alpha^2,\cdots,\alpha^{d-1}$ son distintos y pertenecen a $\mathbb{K}^*$. Concluimos que α es un generador de $\mathbb{K}^*$.
Concluimos que $\mathbb{K}=\mathbb{F}(\alpha)$ y α es el elemento primitivo.
Ahora asumamos que $\mathbb{F}$ es infinito y probaremos nuestro teorema en el caso que $\mathbb{K}=\mathbb{F}(\gamma,\beta)$. Ya que este argumento es sencillo para realizar la inducción sobre el número de raíces.
Sea $\{\beta=\beta_1,\beta_2,...,\beta_n\}\in\overline{\mathbb{F}}$ el conjunto de raíces distintas del polinomio $P_\beta(X)\in\mathbb{F}[X]$

y sea $\{\gamma = \gamma_1, \gamma_2, ..., \gamma_m\} \in \overline{\mathbb{F}}$ el conjunto de raíces distintas del polinomio $P_\gamma(X) \in \mathbb{F}[X]$ donde todas las raíces tienen multiplicidad 1, ya que $\mathbb{K}$ es una extensión separable de $\mathbb{F}$. Como $\mathbb{F}$ es infinito, podemos encontrar $a \in \mathbb{F}$ tal que

$$a \neq \frac{(\beta_i - \beta)}{(\gamma - \gamma_j)}$$

Para todo i y j, con $j \neq 1$. Si $\alpha = \beta + a\gamma$, entonces

$$\alpha = \beta + a\gamma \neq \beta_i + a\gamma_j$$

y así

$$\alpha - a\gamma_j \neq \beta_i$$

para todo i y $j \neq 1$.
Considere $h(X) = f(\alpha - aX) \in \mathbb{F}(\alpha)[X]$, por lo tanto obtenemos que

$$\begin{aligned} h(\gamma) =& f(\alpha - a\gamma) \\ h(\gamma) =& f(\beta + a\gamma - a\gamma) \\ h(\gamma) =& f(\beta) \\ h(\gamma) =& 0. \end{aligned}$$

Sin embargo para $j \neq 1$

$$h(\gamma_j) = f(\alpha - a\gamma_j)$$

Como $\alpha - \beta_j \neq a\gamma_j$, entonces

$$\begin{aligned} f(\alpha - a\gamma_j) \neq& f(\alpha - \alpha + \beta_i) \\ h(\alpha_j) \neq& f(\beta_i) \\ h(\alpha_j) \neq& 0. \end{aligned}$$

Por lo tanto, γ es un factor común de $h(X)$ y $P_\gamma(X) \in \mathbb{F}[X]$ en $\mathbb{F}(\alpha)[X]$, p así el polinomio minimal $P_\gamma(X) \in \mathbb{F}(\alpha)[X]$ debe ser lineal, dado que γ es el único cero en común de $P_\gamma(X)$ y $h(X)$. Así $\gamma \in \mathbb{F}(\alpha)$ y por lo tanto $\beta = \alpha - a\gamma$ pertenece a $\mathbb{F}(\alpha)$ ya que es una combinación lineal de α y γ.
Concluimos que $\mathbb{F}(\beta, \gamma) = \mathbb{F}(\alpha)$. □

Ejemplo 2.3.7. *Como $\mathbb{C} = \mathbb{R}(i)$, entonces i es el elemento primitivo de la extensión $\mathbb{C}/\mathbb{R}$.*

Ejemplo 2.3.8. *Veamos que* $\mathbb{Q}(\sqrt{2},\sqrt{3}) = \mathbb{Q}(\sqrt{2}+\sqrt{3})$.
Como $\sqrt{2},\sqrt{3} \in \mathbb{Q}(\sqrt{2},\sqrt{3})$ *y por definición tenemos que* $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}+\sqrt{3})$, *entonces,* $\mathbb{Q}(\sqrt{2}+\sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2},\sqrt{3})$
Ahora probemos que $\sqrt{2},\sqrt{3} \in \mathbb{Q}(\sqrt{2}+\sqrt{3})$, *sea*

$$\begin{aligned}
\alpha &= \sqrt{2}+\sqrt{3} \\
\alpha - \sqrt{2} &= \sqrt{3} \\
(\alpha - \sqrt{2})^2 &= 3 \\
\alpha^2 - 2\sqrt{2}\alpha + 2 &= 3 \\
\alpha^2 - 2\sqrt{2}\alpha &= 1 \\
\frac{\alpha^2 - 1}{2\alpha} &= \sqrt{2}
\end{aligned}$$

así $\sqrt{2} \in \mathbb{Q}(\sqrt{2}+\sqrt{3})$ *y como* $\sqrt{3} = \alpha - \sqrt{2} \in \mathbb{Q}(\sqrt{2}+\sqrt{3})$. *Concluimos que* $\mathbb{Q}(\sqrt{2},\sqrt{3}) = \mathbb{Q}(\sqrt{2}+\sqrt{3})$.

Capítulo 3

Teoría de Galois

En este capítulo presentaremos la Teoría de Galois donde la idea principal es asociar las extensiones de Galois con el grupo de Galois y mostrar su interacción en los diferentes resultados del Teorema Fundamental de la Teoría de Galois. Para poder desarrollar este capítulo fue necesario hacer una complementación del libro guía *The fundamental theorem of algebra* [2], y los libros *Grupos, corpos e teoria de Galois* [7] y *Advanced Modern Algebra* [8]. Ya que había muchas demostraciones que se omitían fue necesario recurrir a otras herramientas para que el capítulo quedara autocontenido.

3.1. Grupos de Galois

Definición 3.1.1. *Una* **extensión de Galois** *de un cuerpo* $\mathbb{F}$ *sobre* $\mathbb{K}$ *es una extensión algebraica, normal y separable.*

Definición 3.1.2. *Sea* $\mathbb{K}$ *una extensión de Galois de un cuerpo* $\mathbb{F}$*. Al grupo de automorfismos de* $\mathbb{K}$ *que fija* $\mathbb{F}$ *es llamado* **grupo de Galois** *de* $\mathbb{K}$ *sobre* $\mathbb{F}$*, denotado por* $Gal(\mathbb{K}/\mathbb{F})$*, es decir*

$$Gal(\mathbb{K}/\mathbb{F}) = \{\varphi \in Aut(\mathbb{K}) : \varphi(x) = x,\ \forall x \in \mathbb{F}\}.$$

Si H *es un subgrupo de* $Gal(\mathbb{K}/\mathbb{F})$ *denotaremos por* $\mathbb{K}^H$ *los elementos de* $\mathbb{K}$ *fijados por los automorfismos de* H*.*

Lema 3.1.1. *Si* $\mathbb{K}/\mathbb{F}$ *es una extensión de Galois con* $[\mathbb{K} : \mathbb{F}] < \infty$*, entonces el número de automorfismos de* $\mathbb{K}$ *que fijan los elementos de* $\mathbb{F}$ *es igual a la dimensión de la extensión de* $\mathbb{K}$ *sobre* $\mathbb{F}$*, es decir:*

$$|Gal(\mathbb{K}/\mathbb{F})| = [\mathbb{K} : \mathbb{F}]$$

Demostración. Es consecuencia del Corolario 2.3.1. □

Lema 3.1.2. *Si $\mathbb{E}$ es un cuerpo intermedio de la extensión de Galois $\mathbb{K} \subseteq /\mathbb{F}$, entonces*

1. *$\mathbb{K}$ es una extensión de Galois sobre $\mathbb{E}$ y $Gal(\mathbb{K}/\mathbb{E})$ es un subgrupo de $Gal(\mathbb{K}/\mathbb{F})$.*
2. *Si H es un subgrupo de $Gal(\mathbb{K}/\mathbb{F})$, entonces $\mathbb{E} = \mathbb{K}^H$ es un cuerpo intermedio de $\mathbb{K}/\mathbb{F}$ y $Gal(\mathbb{K}/\mathbb{E}) = H$.*

Demostración. 1. Probaremos que $\mathbb{K}$ es una extensión de Galois sobre $\mathbb{E}$, es decir, $\mathbb{K}$ es una extensión algebraica, normal y separable sobre $\mathbb{E}$.

- ✓ Veamos que $\mathbb{K}/\mathbb{E}$ es algebraica.
  Si $\alpha \in \mathbb{K}$ y como $\mathbb{K}/\mathbb{F}$ es algebraica, entonces existe $p(X) \in \mathbb{F}[X]$ tal que $p(\alpha) = 0$, como $\mathbb{F} \subset \mathbb{E}$ entonces $p(X) \in \mathbb{E}[X]$, así α es algebraico sobre $\mathbb{E}$.
- ✓ Veamos que $\mathbb{K}/\mathbb{E}$ es separable.
  Ya que $\mathbb{K}/\mathbb{F}$ es una extensión separable entonces para todo $\alpha \in \mathbb{K}$ no nulo, α es separable sobre $\mathbb{F}$. Si $p_\alpha(X)$ es irreducible en $\mathbb{F}[X]$ y $q_\alpha(X)$ el polinomio minimal de α en $\mathbb{E}[X]$, así $q_\alpha(X)|p_\alpha(X)$, es decir, $p_\alpha(X) = q_\alpha(X)h(X)$ con $h(X) \in \mathbb{E}[X]$. Si $q_\alpha(X)$ tuviese una raíz múltiple, entonces $p_\alpha(X)$ también, lo cual es absurdo pues $p_\alpha(X)$ es separable. Concluimos que $q_\alpha(X)$ es separable.
- ✓ Veamos que $\mathbb{K}$ es normal sobre $\mathbb{E}$.
  La extensión $\mathbb{K}/\mathbb{E}$ es normal si $\mathbb{K}$ es cuerpo de raíces de una familia $\mathscr{G} \subseteq \mathbb{E}[X]\backslash\mathbb{E}$. Como $\mathbb{K}/\mathbb{F}$ es normal existe $\mathscr{F} \subseteq \mathbb{F}[X]\backslash\mathbb{F}$ para la cual $\mathbb{K}$ es el cuerpo de raíces, y como $\mathbb{F} \subseteq \mathbb{E}$, entonces $\mathscr{F} \subseteq \mathbb{E}[X]\backslash\mathbb{E}$, así, $\mathbb{K}$ es normal sobre $\mathbb{E}$.
- ✓ Veamos que $Gal(\mathbb{K}/\mathbb{E})$ es un subgrupo de $Gal(\mathbb{K}/\mathbb{F})$.
  Si $\varphi, \phi \in Gal(\mathbb{K}/\mathbb{E})$, entonces $\varphi\phi^{-1} \in Gal(\mathbb{K}/\mathbb{E})$. Como $\phi^{-1}(\alpha) = \alpha$ para todo $\alpha \in \mathbb{E}$, así $\phi^{-1} \in Gal(\mathbb{K}/\mathbb{E})$. Si $\alpha \in \mathbb{F}$, entonces $\varphi\phi^{-1}(\alpha) = \varphi(\alpha) = \alpha$, concluimos que $Gal(\mathbb{K}/\mathbb{E})$ es subgrupo de $Gal(\mathbb{K}/\mathbb{F})$

2. Procederemos a hacer la demostración en tres partes
   a) $\mathbb{F} \subseteq \mathbb{K}^H$,
   b) $\mathbb{K}^H$ es un cuerpo,
   c) $Gal(\mathbb{K}/\mathbb{K}^H) = H$.

   a) Dado que $H \preceq Gal(\mathbb{K}/\mathbb{F})$, todo elemento de $\mathbb{F}$ es fijado por cada automorfismo $\sigma \in H$, luego $\mathbb{F} \subseteq \mathbb{K}^H$.

b) Probemos que $\mathbb{K}^H$ es cuerpo.
Si $k_1, k_2 \in \mathbb{K}^H$ y $\sigma \in H$, tenemos que

$$\sigma(k_1 \pm k_2) = \sigma(k_1) \pm \sigma(k_2) = k_1 \pm k_2.$$

Por lo tanto $k_1 \pm k_2 \in \mathbb{K}^H$.
Del mismo modo, si $k_2 \neq 0$. obtenemos

$$\sigma(k_1 k_2^{-1}) = \sigma(k_1)\sigma(k_2^{-1}) = k_1 k_2^{-1}.$$

y

$$\sigma(k_1 k_2) = \sigma(k_1)\sigma(k_2) = k_1 k_2$$

Entonces $k_1 k_2^{\pm 1} \in \mathbb{K}^H$, por lo tanto $\mathbb{K}^H$ es un campo intermedio de $\mathbb{K}/\mathbb{F}$.

c) Por la forma como definimos $\mathbb{K}^H$ tenemos que $Gal(\mathbb{K}/\mathbb{K}^H) = H$.

□

Ejemplo 3.1.1. *El grupo $Gal(\mathbb{C}/\mathbb{R})$ tiene dos elementos, el automorfismo identidad y el automorfismo de conjugación compleja.*

Ejemplo 3.1.2. *Como $\mathbb{Q}(\sqrt{2})$ es una extensión algebraica, normal y separable sobre $\mathbb{Q}$, entonces $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ es una extensión de Galois y todo automorfismo $\sigma \in Gal(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$ va a permutar las raíces del polinomio irreducible $X^2 - 2$. Es decir, como sabemos que $|Gal(\mathbb{Q}(\sqrt{2})/\mathbb{Q}| = 2$, entonces $Gal(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) = \{1, \sigma\}$, donde σ es el automorfismo que lleva a $\sqrt{2}$ en $-\sqrt{2}$.*

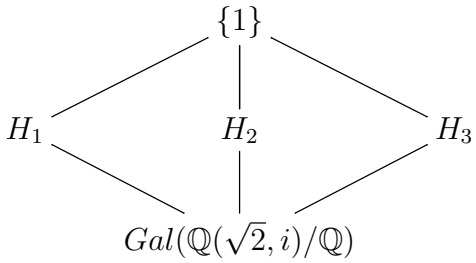
Ejemplo 3.1.3. *El cuerpo $\mathbb{Q}(\sqrt{2}, i)$ es el cuerpo de descomposición de la familia $\mathscr{F} = \{X^2 - 2, X^2 + 1\}$ y por tanto, es normal sobre $\mathbb{Q}$. Como $\mathbb{Q}$ es un cuerpo de característica cero, $\mathbb{Q}(\sqrt{2}, i)$ es una una extensión separable de $\mathbb{Q}$. Además, como $\mathbb{Q}(\sqrt{2}) \subset \mathbb{R}$, entonces el polinomio $x^2 + 1$ es irreducible sobre $\mathbb{Q}(\sqrt{2})$. Así $[\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}] = 4$.*
Los cuatro automorfismos son:

	$\sqrt{2}$	$-\sqrt{2}$	i	$-i$
σ_1	$\sqrt{2}$	$-\sqrt{2}$	i	$-i$
σ_2	$\sqrt{2}$	$-\sqrt{2}$	$-i$	i
σ_3	$-\sqrt{2}$	$\sqrt{2}$	i	$-i$
σ_4	$-\sqrt{2}$	$\sqrt{2}$	$-i$	i

Se identifican los elementos de la primera fila de la tabla anterior con $1, 2, 3, 4$ respectivamente, entonces si $\mathfrak{G}_4$ es el grupo de grupo simétrico de 4 elementos, tenemos una inclusión $Gal(\mathbb{Q}(\sqrt{2}, i)/\mathbb{Q}) \to \mathfrak{G}_4$ dada por

$$\sigma_1 = 1,\ \sigma_2 = (34),\ \sigma_3 = (12),\ \sigma_4 = (12)(34)$$

y, si $H_1 = \langle(12)\rangle$, $H_2 = \langle(34)\rangle$, $H_3 = \langle(12)(34)\rangle$, *el retículo de subgrupos con la relación* $\subseteq$ *es:*



Teorema 3.1.1. *Si* H_1, H_2 *son subgrupos de* $Gal(\mathbb{K}/\mathbb{F})$ *y* $\mathbb{K}^{H_1}, \mathbb{K}^{H_2}$ *los cuerpos intermedios de la extensión* $\mathbb{K}/\mathbb{F}$. *Entonces*

$$H_2 \subseteq H_1 \iff \mathbb{K}^{H_1} \subseteq \mathbb{K}^{H_2}.$$

Demostración. $\implies$ Sea $x \in \mathbb{K}^{H_1}$, por lo tanto, para todo $\sigma \in H_1$ tenemos que $\sigma(x) = x$. Para todo $\gamma \in H_2$, γ también pertenece a H_1, entonces $\gamma(x) = x$ y así $x \in \mathbb{K}^{H_2}$.
$\impliedby$ Si γ pertenece a H_2, γ fija los elementos de $\mathbb{K}^{H_2}$. Por hipótesis tenemos que $\mathbb{K}^{H_1} \subseteq \mathbb{K}^{H_2}$, por tanto, γ fija los elementos de $\mathbb{K}^{H_1}$, así $\gamma \in H_1$. □

Corolario 3.1.1. $H_1 = H_2 \iff \mathbb{K}^{H_1} = \mathbb{K}^{H_2}$.

Teorema 3.1.2. *Si* $\mathbb{K}$ *es un cuerpo y* G *un grupo finito de automorfismos de* $\mathbb{K}$ *con* $|G| = n$, *entonces* $\mathbb{K}$ *es una extensión de Galois finita de* $\mathbb{F} = \mathbb{K}^G$ *y el grupo de Galois es* G.

Demostración. Suponga que $\mathbb{F} = \mathbb{K}^G$, $\alpha \in \mathbb{K}$ no nulo. Si $g_1 = id_{\mathbb{K}}, ..., g_n$ pertencen a G y $S = \{g_1, ..., g_r\}$, con $r \leq n$ el conjunto maximal de elementos tal que $g_1(\alpha), ..., g_r(\alpha)$ todos son distintos. Si $g \in G$, entonces $\{gg_1(\alpha), ..., gg_r(\alpha)\}$ es una permutación del conjunto $\{g_1(\alpha), ..., g_r(\alpha)\}$, dado que g es automorfismo de $\mathbb{K}$ y S es maximal.
Sea

$$f(X) = \prod_{i=1}^{r}(X - g_i(\alpha)).$$

Tenemos que α es raíz de $f(X)$, pues uno de los g_i es la identidad, además $f(X)$ está fijado por todo $g \in G$ pues si

$$g(f(X)) = \prod_{i=1}^{r}(X - gg_i(\alpha))$$

$$g(f(X)) = \prod_{i=1}^{r}(X - g_i(\alpha))$$

$$g(f(X)) = f(X).$$

Por lo tanto, los coeficientes siguen en $\mathbb{F} = \mathbb{K}^G$, dado que $g_i(\alpha)$ son distintos. Así $f(X)$ es separable.
Ya que $\alpha \in \mathbb{K}$ es una raíz de un polinomio de grado menor o igual a n, con coeficientes en $\mathbb{F}$, entonces $\mathbb{K}$ es una extensión separable de $\mathbb{F}$. Además, dado que $f(X)$ se divide en factores lineales, $\mathbb{K}$ es una extensión normal. Concluimos que $\mathbb{K}$ es una extensión de Galois sobre $\mathbb{F}$.
Dado que $\mathbb{K}$ es separable sobre $\mathbb{F}$, entonces es una extensión simple, existe $\gamma \in \mathbb{K}$ tal que $\mathbb{K} = \mathbb{F}(\gamma)$, note que se puede construir como $f(X)$ un polinomio de grado $\leq n$ que tenga a γ como raíz. Así $[\mathbb{K} : \mathbb{F}] \leq n$. Pero como $G \subseteq Gal(\mathbb{K}/\mathbb{F})$ pues G es el grupo de automorfismos de $\mathbb{K}$ que fijan a $\mathbb{F}$. Con esto tenemos que

$$[\mathbb{K} : \mathbb{F}] = |Gal(\mathbb{K}/\mathbb{F})| \geq |G| = n.$$

Concluimos que $[\mathbb{K} : \mathbb{K}^G] = n$ y G debe ser el grupo de Galois de $\mathbb{K}/\mathbb{K}^G$. □

Definición 3.1.3. *Sea $f(X)$ un polinomio irreducible de $\mathbb{F}[X]\backslash\mathbb{F}$ tal que $\mathbb{K}$ es el cuerpo de raíces de $f(X)$ entonces $\mathbb{K}$ es una extensión de Galois sobre $\mathbb{F}$ y el correspondiente grupo de Galois es llamado el* **grupo de Galois del polinomio** *$f(X)$.*

Nota: Supondremos que $\mathbb{F}$ tiene característica cero, entonces todas las extensiones algebraicas de $\mathbb{F}$ son separables por el Teorema 2.3.1.

Ahora examinaremos estos grupos de Galois con más detalle. Si $\mathbb{K}$ es cualquier extensión algebraica de $\mathbb{F}$ y si $\alpha \in \mathbb{K}$ con $P_\alpha(X)$ es el polinomio minimal de α. Cualquier otra raíz $\bar{\alpha}$ de $P_\alpha(X)$, es llamado conjugado de α. Ahora, supongamos que $\mathbb{K}$ es una extensión de Galois sobre $\mathbb{F}$ y $\sigma \in Gal(\mathbb{K}/\mathbb{F})$. Dado que σ fija los elementos de $\mathbb{F}$ también fija a $P_\alpha(X) \in \mathbb{F}[X]$, y por lo tanto $\sigma(\alpha)$ debe ser otra raíz de $P_\alpha(X)$. Así, cualquier $\sigma \in Gal(\mathbb{K}/\mathbb{F})$ envia los elementos en los conjugados.
Si $f(X) \in \mathbb{F}[X]$ un polinomio irreducible, con raíces $\alpha_1, ..., \alpha_n \in \mathbb{K}$ y $\sigma \in Gal(\mathbb{K}/\mathbb{F})$, σ fija a $f(X)$ y envía el conjunto de raíces en si mismo. Tenemos que:

- ✓ Cualquier $\sigma \in Gal(\mathbb{K}/\mathbb{F})$ permuta las raíces del polinomio irreducible.
- ✓ Los conjugados de las raíces del polinomio irreducible son también raíces.

3.2. Teorema Fundamental De La Teoría De Galois

Teorema 3.2.1. *Si $\mathbb{K}$ una extensión de Galois de $\mathbb{F}$ con $G = Gal(\mathbb{K}/\mathbb{F})$ el grupo de Galois.*
Entonces

1. *La función τ definida a continuación es una biyección entre los subgrupos de G y los cuerpos que contienen a $\mathbb{F}$, es decir,*

$$\begin{aligned} \tau : Sub(G) &\longrightarrow \{\mathbb{L} : \mathbb{F} \subseteq \mathbb{L} \subseteq \mathbb{K}\} \\ H &\longrightarrow \mathbb{K}^H \end{aligned}$$

Con inversa

$$\begin{aligned} \delta : \{\mathbb{L} : \mathbb{F} \subseteq \mathbb{L} \subseteq \mathbb{K}\} &\longrightarrow Sub(G) \\ \mathbb{B} &\longrightarrow Gal(\mathbb{K}/\mathbb{B}) \end{aligned}$$

2. *Si H es un subgrupo de G y $\mathbb{E} = \mathbb{K}^H$, entonces $\delta(\mathbb{E}) = H$.*

3. *$\mathbb{K}$ es una extensión Galois sobre $\mathbb{E}$, y $Gal(\mathbb{K}/\mathbb{E}) = \delta(\mathbb{E})$.*

4. *$|G| = |\mathbb{K}/\mathbb{F}|$.*

5. *$\mathbb{E}$ es una extensión de Galois sobre $\mathbb{F}$, si y solo si, $\delta(\mathbb{E}) \lhd G$, en este caso*

$$Gal(\mathbb{E}/\mathbb{F}) \cong \tfrac{G}{\delta(\mathbb{E})}$$

6. *El retículo de subcuerpos de $\mathbb{K}$ que contienen a $\mathbb{F}$ es el retículo inverso de los subgrupos de $Gal(\mathbb{K}/\mathbb{F})$.*

Demostración. 1. Veamos que la función τ es una biyección.

- ✓ Inyectividad.
  Si $\mathbb{K}^{H_1} = \mathbb{K}^{H_2}$, por el Colorario 3.1.1. tenemos que $H_1 = H_2$.
- ✓ Sobreyectividad.
  Considere la composición

$$\tau \circ \delta : \{\mathbb{L} : \mathbb{F} \subseteq \mathbb{L} \subseteq \mathbb{K}\} \xrightarrow{\delta} Sub(G) \xrightarrow{\tau} \{\mathbb{L} : \mathbb{F} \subseteq \mathbb{L} \subseteq \mathbb{K}\}$$

  Donde δ es la función tal que $\delta(\mathbb{E}) = Gal(\mathbb{K}/\mathbb{E})$, luego $\tau\delta(\mathbb{E}) = \mathbb{K}^{Gal(\mathbb{K}/\mathbb{E})}$.
  Por el Teorema 3.1.2. tenemos que

$$\mathbb{K}^{Gal(\mathbb{K}/\mathbb{E})} = \{k \in \mathbb{K} : \sigma(k) = k \quad con \quad \sigma \in Gal(\mathbb{K}/\mathbb{E})\} = \mathbb{E}.$$

  Luego $\tau\delta$ es la identidad, por lo tanto τ es sobreyectiva.

  Nota: A la función δ la llamaremos la función correspondecia de Galois del grupo G.

2. Como $\mathbb{E} = \mathbb{K}^H$, entonces $\delta(\mathbb{K}^H) = Gal(\mathbb{K}/\mathbb{K}^H) = H$.

3. $\delta(\mathbb{E}) = Gal(\mathbb{K}/\mathbb{E}) \subseteq G$ por la parte 1. del Lema 3.1.2. y como

$$\tau\delta(\mathbb{E}) = \mathbb{K}^{Gal(\mathbb{K}/\mathbb{E})} = \mathbb{E} = \mathbb{K}^H$$

Por el corolario 3.1.1. $\delta(\mathbb{E}) = Gal(\mathbb{K}/\mathbb{E}) = H$.

4. Por el Lema 3.1.1.

5. ($\Longrightarrow$) Sea $\mathbb{F} \subseteq \mathbb{E} \subseteq \mathbb{K}$, un cuerpo intermedio. Supongamos que $\mathbb{E}/\mathbb{F}$ es una extensión normal, entonces $\mathbb{E}/\mathbb{F}$ es una extensión de Galois. Sea $Gal(\mathbb{E}/\mathbb{F})$ un grupo de Galois. Es claro que una restricción de $\sigma \in Gal(\mathbb{K}/\mathbb{F})$ a $\mathbb{E}$ forma un homomorfismo de

$$\begin{aligned} res : Gal(\mathbb{K}/\mathbb{F}) &\longrightarrow Gal(\mathbb{E}/\mathbb{F}) \\ \sigma &\longrightarrow res(\sigma) = \sigma|_{\mathbb{E}} \end{aligned}$$

Como $\mathbb{E} = \mathbb{K}^H$ para cierto subgrupo de H de G, tenemos que $H = Ker(res)$, esto implica que

$$Gal(\mathbb{E}/\mathbb{F}) \cong \frac{G}{\delta(\mathbb{E})}.$$

Como $\delta(\mathbb{E}) = ker(res)$ entonces es subgrupo normal de G.

($\Longleftarrow$) Supongamos que H es un subgrupo de G, en principio cualquiera, y $\mathbb{E} = \mathbb{K}^H$. Si $\sigma \in G$ y sea $\tau \in H$ entonces para $u \in \mathbb{E}$,

$$\sigma\tau\sigma^{-1}(\sigma(u)) = \sigma\tau(u) = \sigma(u),$$

es decir, $\sigma H\sigma^{-1} \subseteq Gal(\mathbb{K}/\sigma(\mathbb{E}))$.
Reciprocamente, si $\gamma \in Gal(\mathbb{K}/\sigma(\mathbb{E}))$, entonces

$$\sigma^{-1}\gamma\sigma(u) = \sigma^{-1}\sigma(u) = u,$$

es decir, $\sigma^{-1}Gal(\mathbb{K}/\sigma(\mathbb{E}))\sigma \subseteq H$, entonces,

$$Gal(\mathbb{K}/\sigma(\mathbb{E})) = \sigma Gal(\mathbb{K}/\mathbb{E})\sigma^{-1}.$$

Para cualquier $\sigma \in G$. Como $H \lhd G$, entonces tenemos la siguiente igualdad,

$$H_1 = Gal(\mathbb{K}/\sigma(\mathbb{E})) = Gal(\mathbb{K}/\mathbb{E}) = H$$

para todo $\sigma \in G$ y por el Colorario 3.1.1. $\mathbb{E} = \sigma(\mathbb{E})$, es decir que $\mathbb{E}/\mathbb{F}$ es una extensión normal.

6. Veamos el retículo de subcuerpos de $\mathbb{K}$ que contienen a $\mathbb{F}$ es el retículo inverso de los subgrupos de $Gal(\mathbb{K}/\mathbb{F})$. Para ello primero veamos que:

   ✓ En el conjunto $\mathscr{P}_{\mathbb{K}}$ (el conjunto de los de subcuerpos de $\mathbb{K}$ que contienen a $\mathbb{F}$) tenemos que

   $$\mathbb{K}_1 \vee \mathbb{K}_2 = \mathbb{K}_1\mathbb{K}_2$$
   $$\mathbb{K}_1 \wedge \mathbb{K}_2 = \mathbb{K}_1 \cap \mathbb{K}_2$$

   Donde $\mathbb{K}_1\mathbb{K}_2$ es el menor subcuerpo de $\mathbb{K}/\mathbb{F}$ que contiene a $\mathbb{K}_1$ y $\mathbb{K}_2$.

   Nota: $\mathbb{K}_1\mathbb{K}_2 = \left\{ x \mid x = \sum_{i=1}^{l} a_i b_i \quad con \quad a_i \in \mathbb{K}_1; b_i \in \mathbb{K}_2 \quad y \quad l \in \mathbb{N} \right\}$ es llamado compositium de $\mathbb{K}_1$ y $\mathbb{K}_2$.

   ✓ Sea $\mathscr{P}_G$ el conjunto de los de subgrupos de G tenemos que

   $$H_1 \vee H_2 = \langle H_1, H_2 \rangle$$
   $$H_1 \wedge H_2 = H_1 \cap H_2$$

   Donde $\langle H_1, H_2 \rangle$ es el subgrupo generado por H_1 y H_2.

   Ahora probaremos que

   i. $H_1 \cap H_2$ corresponde a la compositium $\mathbb{K}^{H_1}\mathbb{K}^{H_2}$.
   Sea $\sigma \in H_1 \cap H_2$, entonces σ fija $\mathbb{K}^{H_1}$ y $\mathbb{K}^{H_2}$, es decir, σ fija a los elementos de la compositium $\mathbb{K}^{H_1}\mathbb{K}^{H_2}$. Sea $x \in \mathbb{K}^{H_1}\mathbb{K}^{H_2}$ entonces

   $$x = \sum_{i=1}^{l} a_i b_i$$

   donde $a_i \in \mathbb{K}^{H_1}$, $b_i \in \mathbb{K}^{H_2}$ y $l \in \mathbb{N}$, así tenemos:

   $$\begin{aligned} \sigma(x) &= \sigma(\sum_{i=1}^{l} a_i b_i) \\ &= \sigma(a_1b_1 + a_2b_2 + \cdots + a_lb_l) \\ &= \sigma(a_1b_1) + \sigma(a_2b_2) + \cdots + \sigma(a_lb_l). \end{aligned}$$

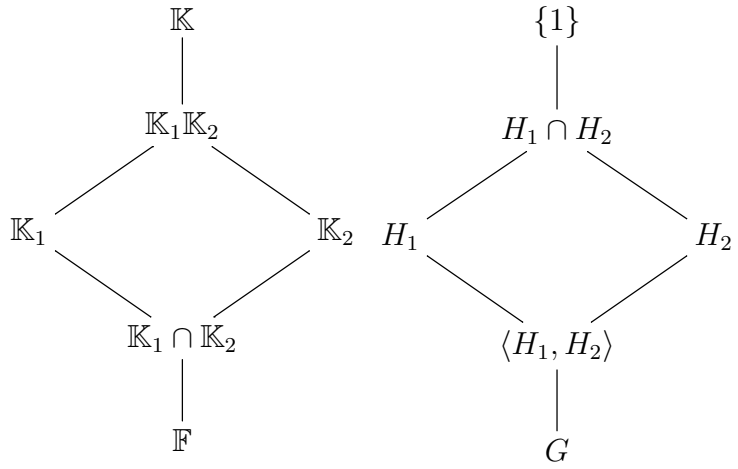
   Como $a_ib_i \in \mathbb{K}^{H_1}\mathbb{K}^{H_2}$ entonces $\sigma(a_ib_i) = \sigma(a_i)\sigma(b_i) = a_ib_i$, por lo tanto, $\sigma(x) = x$.

   ii. $\mathbb{L}_1 \cap \mathbb{L}_2$ corresponde al subgrupo $\langle Gal(\mathbb{K}/\mathbb{L}_1), Gal(\mathbb{K}/\mathbb{L}_2) \rangle$.
   Sea $\mathbb{L}_1$ y $\mathbb{L}_2$ cuerpos intermedios, tal que $\mathbb{L}_1 = \mathbb{K}^{H_1}$ y $\mathbb{L}_2 = \mathbb{K}^{H_2}$. Si $x \in \mathbb{L}_1 \cap \mathbb{L}_2$

, entonces x es fijado por H_1 y por H_2, donde x es fijado por $\langle H_1, H_2\rangle$. Si $y \in \mathbb{K}$ que es fijado por $\langle H_1, H_2\rangle$, entonces, en particular y es fijado por H_1 y por H_2, por tanto $y \in \mathbb{L}_1 \cap \mathbb{L}_2$.

Concluimos que $\delta : \{\mathbb{L} : \mathbb{F} \subseteq \mathbb{L} \subseteq \mathbb{K}\} \longrightarrow Sub(G)$ es un anti-isomorfimo de retículos.

En el próximo diagrama se ilustra algunas de las características expuestas anteriormente.



□

Ejemplo 3.2.1. *Consideremos la extensión de Galois $\mathbb{K}/\mathbb{F}$, donde $\mathbb{K}$ es el cuerpo de descomposición del polinomio irreducible x^4-2 sobre $\mathbb{F} = \mathbb{Q}$. Es claro que $\mathbb{K} = \mathbb{Q}(\sqrt[4]{2}, i)$. Como $\mathbb{Q}(\sqrt[4]{2}) \subset \mathbb{R}$, el polinomio x^2+1 es irreducible sobre $\mathbb{Q}(\sqrt[4]{2})$ así $|\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}| = 8$. Por lo tanto, los automorfismos son:*

	$\sqrt[4]{2}$	$-\sqrt[4]{2}$	$i\sqrt[4]{2}$	$-i\sqrt[4]{2}$
σ_1	$\sqrt[4]{2}$	$-\sqrt[4]{2}$	$i\sqrt[4]{2}$	$-i\sqrt[4]{2}$
σ_2	$\sqrt[4]{2}$	$-\sqrt[4]{2}$	$-i\sqrt[4]{2}$	$i\sqrt[4]{2}$
σ_3	$-\sqrt[4]{2}$	$\sqrt[4]{2}$	$-i\sqrt[4]{2}$	$i\sqrt[4]{2}$
σ_4	$-\sqrt[4]{2}$	$\sqrt[4]{2}$	$i\sqrt[4]{2}$	$-i\sqrt[4]{2}$
σ_5	$i\sqrt[4]{2}$	$-i\sqrt[4]{2}$	$-\sqrt[4]{2}$	$\sqrt[4]{2}$
σ_6	$i\sqrt[4]{2}$	$-i\sqrt[4]{2}$	$\sqrt[4]{2}$	$-\sqrt[4]{2}$
σ_7	$-i\sqrt[4]{2}$	$i\sqrt[4]{2}$	$\sqrt[4]{2}$	$-\sqrt[4]{2}$
σ_8	$-i\sqrt[4]{2}$	$i\sqrt[4]{2}$	$-\sqrt[4]{2}$	$\sqrt[4]{2}$

Si identificamos los elementos de la primera fila de la tabla con $1, 2, 3$ *y* 4*, respectivamente, tenemos la identificación* $Gal(\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q})$ *con su imagen en* $\mathfrak{S}_4$

$$Gal(\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q}) = \{1, (34), (12)(34), (12), (1324), (13)(24), (1423), (14)(23)\}$$

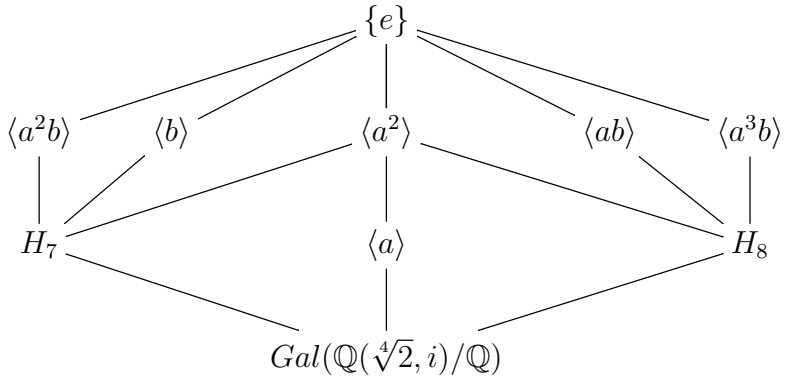
Si suponemos que $a = (1324)$ *y* $b = (12)$*, entonces es facil ver que* $ab \neq ba$ *y que*

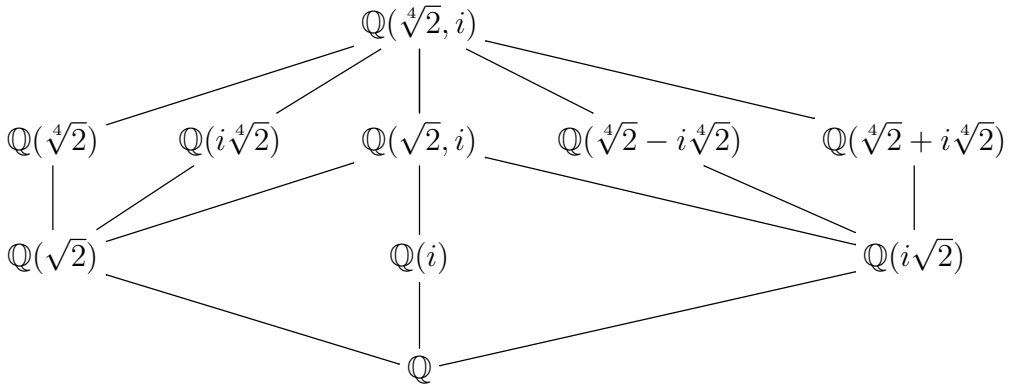
$$Gal(\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q}) = \{e, a, a^2, a^3, b, ab, a^2b, a^3b\}$$

es el grupo diedral $\mathcal{D}_8$*.*
Los subgrupos no triviales de $Gal(\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q})$ *son:*

$$H_1 = \langle a^2 \rangle = \{a^2, e\},\ H_2 = \langle b \rangle = \{b, e\},\ H_3 = \langle ab \rangle = \{ab, e\},\ H_4 = \langle a^2b \rangle = \{a^2, e\},$$
$$H_5 = \langle a^3b \rangle = \{a^3, e\},\ H_6 = \langle a \rangle = \{a, a^2, a^3, e\},\ H_7 = \{e, a^2, b, a^2b\},$$
$$H_8 = \{e, a^2, ab, a^3b\}$$

Como observamos H_j *es de orden* 2 *para* $j = 1, ..., 5$ *y los demás tienen orden* 4*, y* H_6 *es cíclico. Vamos a encontrar los respectivos cuerpos fijos.*
Como $a^2 = \sigma_3$ *en nuestra tabla anterior, vemos que* $\sqrt[4]{2}\sqrt[4]{2} = \sqrt{2}$ *y* $i\sqrt[4]{2}\sqrt[4]{2} = i\sqrt{2}$ *se quedan fino por* a^2 *y* $\mathbb{K}_1 = \mathbb{Q}(i\sqrt{2}, \sqrt{2}) = \mathbb{Q}(i, \sqrt{2})$ *entonces el grado sobre* $\mathbb{Q}$ *es* 4*, de modo que* $\mathbb{K}_1$ *es el cuepo fijo de* H_1*.*
Como $b = (12) = \sigma_4$*, el cuerpo fijo de* H_2 *es* $\mathbb{K}_2 = \mathbb{Q}(i\sqrt[4]{2})$*.*
El elemento que fija $ab = (14)(23) = \sigma_8$ *es* $u = \sqrt[4]{2} - i\sqrt[4]{2}$ *y como*
$u^4 = -8$*,* $[\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}(\sqrt[4]{2} - i\sqrt[4]{2})$ *de donde el cuerpo que fija* H_3 *es* $\mathbb{K}_3 = \mathbb{Q}(\sqrt[4]{2} - i\sqrt[4]{2})$
El elemennto que fija $a^3b = (34) = \sigma_2$*, de modo que el cuerpo que fija* H_4 *es*
$K_4 = \mathbb{Q}(\sqrt[4]{2})$*.*
El elemento $H_5 = a^3b = (13)(24) = \sigma_6$ *fija a* $\mathbb{K}_5 = \mathbb{Q}(\sqrt[4]{2} + i\sqrt[4]{2})$*.*
El elemento $a = (1324) = \sigma_5$ *fija* i*, de modo que* $\mathbb{K}_6 = \mathbb{Q}(i)$*.*
Falta los dos subgrupos que no son cíclicos: $H_7 = \{e, a^2, b, a^2b\}$ *y* $H_8 = \{e, a^2, ab, a^3b\}$*.*
Como $H_7 = H_1H_2$ *el cuerpo* $\mathbb{K}_7$ *fijo por* H_7 *es* $\mathbb{K}_1 \cap \mathbb{K}_2 = \mathbb{Q}(\sqrt{2})$*, y del mismo modo, como* $H_8 = H_1H_3$*, el cuerpo que fija será* $\mathbb{K}_8 = \mathbb{K}_1 \cap \mathbb{K}_3 = \mathbb{Q}(i\sqrt{2})$*.*
Además, podemos representar los retículos de subgrupos y subcuerpos correspondientes:


$\{e\}$
$\langle a^2b\rangle$
$\langle b\rangle$
$\langle a^2\rangle$
$\langle ab\rangle$
$\langle a^3b\rangle$
H_7
$\langle a\rangle$
H_8
$Gal(\mathbb{Q}(\sqrt[4]{2},i)/\mathbb{Q})$


$\mathbb{Q}(\sqrt[4]{2},i)$
$\mathbb{Q}(\sqrt[4]{2})$
$\mathbb{Q}(i\sqrt[4]{2})$
$\mathbb{Q}(\sqrt{2},i)$
$\mathbb{Q}(\sqrt[4]{2}-i\sqrt[4]{2})$
$\mathbb{Q}(\sqrt[4]{2}+i\sqrt[4]{2})$
$\mathbb{Q}(\sqrt{2})$
$\mathbb{Q}(i)$
$\mathbb{Q}(i\sqrt{2})$
$\mathbb{Q}$

Capítulo 4

El Teorema Fundamental del Álgebra

En esta sección mostraremos la prueba del Teorema Fundamental del Álgebra tomando del libro guía [2] y haremos una explicación completa con los resultados de los capítulos anteriores y algunos que expondremos a continuación.

Teorema 4.0.1. Teorema del Valor Intermedio
Si f es una función continua en un intervalo $[a, b]$ entonces para cada u tal que $f(a) < u < f(b)$, existe al menos un c dentro de (a, b) tal que $f(c) = u$.

Lema 4.0.1. *Todo polinomio de coeficientes reales de grado impar tiene una raíz real.*

Demostración. Suponga que $P(X) \in \mathbb{R}[X]$ un polinomio de grado impar n y suponga que $a_n > 0$
(la prueba es idéntica si $a_n < 0$) entonces:

$$P(X) = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0.$$

1.) Hallaremos el límite de $P(X)$ cuando X tiende a infinito.

$$\begin{aligned} \lim_{X\to\infty} P(X) &= \lim_{X\to\infty} (a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0) \\ &= \lim_{X\to\infty} a_n X^n + \lim_{X\to\infty} a_{n-1} X^{n-1} + \cdots + \lim_{X\to\infty} a_1 X + a_0 \\ &= \infty, \end{aligned}$$

donde $a_n > 0$.

2.) Ahora el límite de $P(X)$ cuando X tiende a menos infinito.

$$\begin{aligned}\lim_{X\to-\infty} P(X) &= \lim_{X\to-\infty}(a_nX^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0)\\ &= \lim_{X\to-\infty} a_nX^n + \lim_{X\to-\infty} a_{n-1}X^{n-1} + \cdots + \lim_{X\to-\infty} a_1X + a_0\\ &= -\infty,\end{aligned}$$

donde $a_n > 0$.

Como el $\lim_{X\to\infty} P(X) = \infty$ existe $x_1 \in \mathbb{R}$ tal que, $P(x_1) > 0$, de igual manera, como $\lim_{X\to-\infty} P(X) = -\infty$, por lo tanto, existe $x_2 \in \mathbb{R}$ tal que, $P(x_2) < 0$.
por el Teorema 4.0.1. existe x_3 en (x_2, x_1) tal que $P(x_3) = 0$, y así $P(X)$ no es irredubible en $\mathbb{R}[X]$.

□

Lema 4.0.2. *Todo polimomio complejo de grado 2 tiene una raíz en* $\mathbb{C}$.

Demostración. Si $P(X) = aX^2 + bX + c \in \mathbb{C}[X]$, entonces las fórmulas para hallar las raíces son:

$$\begin{aligned}X_1 &= \tfrac{-b+\sqrt{b^2-4ac}}{2a};\\ X_2 &= \tfrac{-b-\sqrt{b^2-4ac}}{2a}.\end{aligned}$$

Por lo tanto, $X_1, X_2 \in \mathbb{C}$ ya que $\sqrt{b^2-4ac} \in \mathbb{C}$. □

Ahora ya podemos demostrar el objetivo principal de este trabajo.

Teorema 4.0.2. *El cuerpo de los números complejos* $\mathbb{C}$ *es un cuerpo algebraicamente cerrado, esto quiere decir, que cualquier polinomio complejo no constante tiene una raíz en* $\mathbb{C}$.

Demostración. Si $f(x) \in \mathbb{C}[x]$ es un polinomio irreducible, por el Teorema 2.2.1. podemos construir el cuerpo de raíces $\mathbb{K}$ para $f(x)$ sobre $\mathbb{C}$. Esta será una extensión de Galois de $\mathbb{C}$ ya que $\mathbb{C}$ tiene característica cero y por el Teorema 2.3.1 $\mathbb{K}$ es una extensión separable de $\mathbb{C}$. Dado que $\mathbb{C}$ es una extensión finita de $\mathbb{R}$, entonces $\mathbb{K}$ también es extensión de Galois de $\mathbb{R}$. El Teorema Fundamental del Álgebra afirma que $\mathbb{K}$ debe ser $\mathbb{C}$.
La prueba se realizará por casos

1. Si $\mathbb{K}$ es una extensión de grado 2 de $\mathbb{C}$. Por el Teorema del elemento primitivo, $\exists\alpha \in \mathbb{K}$ tal que

$$\mathbb{K} = \mathbb{C}(\alpha)$$

entonces $\partial P_\alpha(x) = 2$. Por el Lema 4.0.2. todo polinomio cuadrático en $\mathbb{C}[x]$ siempre tiene raíces en $\mathbb{C}$. Por lo tanto $\mathbb{C}$ no tiene extensiones de grado 2.

2. Sea $\mathbb{K}$ cualquier extensión finita de $\mathbb{R}$ con $[\mathbb{K} : \mathbb{R}] = 2^m q$ con $(2, q) = 1$. Si $m = 0$, entonces $\mathbb{K}$ es una extensión de grado impar sobre $\mathbb{R}$.
   Por el Teorema 2.3.1 tenemos que $\mathbb{K}$ es separable sobre $\mathbb{R}$, y así es una extensión simple, por el Teorema 2.3.4,

$$\exists \alpha \in \mathbb{K} \quad tal \quad que \quad \mathbb{K} = \mathbb{R}(\alpha),$$

   donde el polinomio minimal $P_\alpha(x) \in \mathbb{R}[X]$ tiene grado impar. Sin embargo, por el Lemma 4.0.1., todo polinomio de coeficientes reales de grado impar siempre tiene una raíz real, y por lo tanto $P_\alpha(x)$ es irreducible solo si su grado es uno. Concluimos que $\alpha \in \mathbb{R}$ y $\mathbb{K} = \mathbb{R}$.

3. Supongamos que $[\mathbb{K} : \mathbb{R}] = 2^m q$ con $(2, q) = 1$, y que $m > 0$.

   Entonces $|Gal(\mathbb{K}/\mathbb{R})| = |G| = 2^m q$ por el Teorema 2.3.3. Por el Teorema 1.2.1 G tiene un 2-subgrupo de Sylow G' de orden 2^m e índice q. Esto corresponde a que existe un cuerpo intermedio $\mathbb{E} = \mathbb{K}^{G'}$ tal que

$$[\mathbb{K} : \mathbb{E}] = 2^m \quad y \quad [\mathbb{E} : \mathbb{R}] = q,$$

   en consecuencia, es una extensión finita de grado impar de $\mathbb{R}$, entonces, $q = 1$ y $\mathbb{E} = \mathbb{R}$.
   Así $[\mathbb{K} : \mathbb{R}] = 2^m$ y $|G| = 2^m$.

   Ahora $[\mathbb{K} : \mathbb{C}] = 2^{m-1}$ y suponga que $G_1 = Gal(\mathbb{K}/\mathbb{C})$, este es un 2-grupo de Sylow. Si no fuera el grupo trivial, por el Teorema 1.2.1, existirá un 2-subgrupo G' de orden 2^{m-2} e índice 2. Por la parte 6 del Teorema Fundamental de la Teoría de Galois, este corresponde a un cuerpo intermedio $\mathbb{E} = \mathbb{K}^{\mathbb{G}'}$ de grado 2 sobre $\mathbb{C}$. Sin embargo, desde el argumento ya visto, $\mathbb{C}$ no tiene una extensión de grado 2 sobre $\mathbb{C}$, por tanto G_1 es trivial, es decir, $|G_1| = 1$, así $[\mathbb{K} : \mathbb{C}] = 1$. Concluimos que $\mathbb{K} = \mathbb{C}$.

□

4.1. Consecuencias del Teorema Fundamental del Álgebra

Teniendo en cuenta el Teorema Fundamental del Álgebra podemos exponer las siguientes consecuencias las cuales fueron tomadas de [5].

1. Los polinomios irreducibles en $\mathbb{R}[X]$ son los de grado 2 con discriminante negativo.

   Demostración. Para encontrar las raíces de un polinomio de la forma

   $$aX^2 + bX + c \in \mathbb{R}[X]$$

   podemos obtenerlas de la siguiente manera

   $$\alpha_1 = \frac{-b + \sqrt{b^2 - 4ac}}{2a};$$

   $$\alpha_2 = \frac{-b - \sqrt{b^2 - 4ac}}{2a}.$$

   Entonces si $b^2 - 4ac < 0$, $\alpha_1, \alpha_2 \neq \mathbb{R}$.
   Recíprocamente, si $f(X)$ tiene grado impar > 1 tiene por lo menos una raíz y por lo tanto es reducible. Como vimos en el Lema 4.0.1.
   Si $f(X)$ es de grado 2, es reducible si y solo si $b^2 - 4ac \leq 0$. Si $f(X)$ tiene grado par ≥ 4, o bien tiene alguna raíz real y en tal caso es reducible, o bien todas sus raíces son complejas no reales, pues como $[\mathbb{K} : \mathbb{R}] = [\mathbb{C} : \mathbb{R}] = 2$ siendo $\mathbb{K}$ el cuerpo de raíces del polinomio $f(X)$, así sus raíces vienen de a pares conjugados, es decir, si z es una de esas raíces, el polinomio real $(X - z)(X - \bar{z})$ divide a $f(X)$ en $\mathbb{R}[X]$ y $f(X)$ resulta reducible tambíen. □

2. La factorización en irreducibles de un polinomio $f(X) \in \mathbb{R}[X]$ es siempre de la forma

   $$f(X) = c(X - a_1)^{k_1} \cdots (X - a_r)^{k_r}(X^2 + b_1X + c_1)^{j_1} \cdots (X^2 + b_sX + c_s)^{j_s},$$

   con r ó s eventualmente nulos, con $k_i, j_l \geq 1$ tal que $1 \leq i \leq r$, $1 \leq l \leq s$, $b_l^2 - 4c_l < 0$ y $\sum_{i=1}^{r} k_i + \sum_{l=1}^{s} j_l = \partial f(X)$.

   También podemos observar que el polinomio se puede reescribir así:

$$f(X) = c(X-a_1)^{k_1}\cdots(X-a_r)^{k_r}(X-z_1)^{j_1}(X-\bar{z_1})^{j_1}\cdots(X-z_s)^{j_s}(X-\bar{z_s})^{j_s}.$$

Con $z_i = \frac{-b+\sqrt{b^2-4c}}{2}$ y $\bar{z}_i = \frac{-b-\sqrt{b^2-4c}}{2}$.

Ejemplo 4.1.1.

$$\begin{aligned} f(X) =& X^4+4X^3+17X^2+70X+208 \\ f(X) =& (X^2+6X+13)(X^2-2X+16) \\ f(X) =& (X-(-3+2i))(X-(-3-2i))(X-(i+4i))(X-(1-4i)) \end{aligned}$$

3.

Teorema 4.1.1. *Si $f(x)$ es un polinomio de grado $n \geq 1$ con coeficientes compejos, entonces existen n números complejos $z_1, z_2, \cdots, z_n$ tales que*

$$f(X) = a(X-z_1)(X-z_2)\cdots(X-z_n)$$

.

4. Para este ejemplo nos basamos en [4].
Sea V un espacio vectorial complejo de dimensión n, sea $T : V \longrightarrow V$ una transformación lineal, B base y $A = [T]_B$ la matriz asociada a la transformación lineal.

Definición 4.1.1. *$\lambda \in \mathbb{C}$ es autovalor de A si existe $v \in V$ tal que $T(v) = \lambda v$.*
Si A la matriz asociada a la transformación lineal de $n \times n$, entonces $p(\lambda) = det(A-\lambda I)$ se denominia el polinomio característico.
Para

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix}$$

entonces,

$$p(\lambda) = det(A-\lambda I) = \begin{vmatrix} a_{11}-\lambda & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22}-\lambda & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn}-\lambda \end{vmatrix}$$

por lo tanto,

$$p(\lambda) = (-1)^n[\lambda^n + b_{n-1}\lambda^{n-1} + \cdots + b_1\lambda + b_0]. \tag{4.1}$$

Teorema 4.1.2. *λ es autovalor de A si y solo si $p(\lambda) = det(A - \lambda I) = 0$.*

$$p(\lambda) = (-1)^n[\lambda^n + b_{n-1}\lambda^{n-1} + \cdots + b_1\lambda + b_0] = 0. \tag{4.2}$$

Por el Teorema Fundamental del Álgebra (4.2) podemos escribir a $p(\lambda)$ como producto de factores lineales.

$$(-1)^n p(\lambda) = (\lambda - \lambda_1)(\lambda - \lambda_2)\cdots(\lambda - \lambda_n)$$

Con $\lambda_1, \lambda_2, \cdots, \lambda_n \in \mathbb{C}$.

Concluimos que los autovalores para una matriz asociada a una trasformación lineal de un espacio vectorial en $\mathbb{C}$ pertenecen a $\mathbb{C}$.

Ejemplo 4.1.2. *Si* $A = \begin{pmatrix} 3 & -5 \\ 1 & -1 \end{pmatrix}$ *entonces el* $det(A - \lambda I) = \begin{vmatrix} 3 & -5 \\ 1 & -1 \end{vmatrix}$

$$\begin{aligned} det(A - \lambda I) =& (3 - \lambda)(-1 - \lambda) - (-5) \\ det(A - \lambda I) =& \lambda^2 - 2\lambda + 2 = 0, \end{aligned}$$

así,

$$\begin{aligned} \lambda =& \frac{-b \pm \sqrt{b^2 - 4ac}}{2a} \\ \lambda =& \frac{2 \pm \sqrt{4 - 8}}{2} \\ \lambda =& \frac{2 \pm \sqrt{-4}}{2} \\ \lambda =& \frac{2 \pm 2i}{2} \\ \lambda =& 1 \pm i. \end{aligned}$$

Los valores característicos de A son $\lambda_1 = 1 + i$ y $\lambda_2 = 1 - i$.

Capítulo 5

Aplicación de la Teoría de Galois de dimensión infinita

En este capítulo expondremos una aplicación de la Teoría de Galois en dimensión infinita. Para ello nos guiaremos por [6] donde encontraremos los términos como sistemas inversos de grupos, límites inversos y propiedades de ellos.

Sistemas Inversos de Grupos.

Definición 5.0.1. *Sea I un conjunto parcialmente ordenado, un* **sistema inverso de grupos** *es un par $\{G_i, \varphi_i^j\}_{j\geq i}$ donde $\{G_i\}_{i\in I}$ es una familia de grupos y $\varphi_i^j : G_j \longrightarrow G_i$ es una familia de homorfismos en $\{G_i\}_{i\in I}$, tal que:*

i. $\varphi_i^i = Id_{G_i}$.

ii. Si $k \geq j \geq i$, entonces

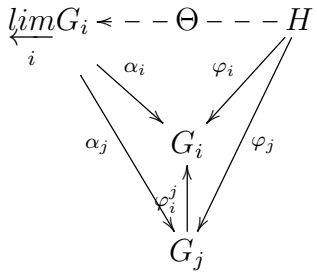
$$\begin{array}{ccc} G_k & \xrightarrow{\varphi_j^k} & G_j \\ \downarrow{\scriptstyle \varphi_i^k} & \swarrow{\scriptstyle \varphi_i^j} & \\ G_i & & \end{array}$$

es conmutativo, es decir, $\varphi_i^j \varphi_j^k = \varphi_i^k$.

Definición 5.0.2. *Sea $\{G_i, \varphi_i^j\}_{j\geq i}$ un sistema inverso de grupos. Un* **límite inverso** *de dicho sistema es un grupo $\varprojlim_i G_i$, que junto con los homomorfismos $\alpha_j : \varprojlim_i G_i \longrightarrow G_j$, cumple las siguientes propiedades:*

(i) $\varphi_i^j \alpha_j = \alpha_i$, *si* $j \geq i$.

(ii) Si existe un grupo H, *junto con los homomorfimos* $\varphi_i : H \longrightarrow G_i$, *tal que para todo* $i \in I$ $\varphi_i^j \varphi_j = \varphi_i$, *entonces existe un único homomorfismo* $\Theta : H \longrightarrow \varprojlim_i G_i$ *que para todo* $i \in I$, $\alpha_i \Theta = \varphi_i$.



Si $\{H, \{\varphi_i\}_{i \in I}\}$ *es un límite inverso, entonces escribimos*

$$H = \varprojlim_i G_i.$$

Proposición 5.0.1. *Si* $\{G_i, \varphi_i^j\}_{j \geq i}$ *es un sistema inverso de un grupo* $\{G_i\}_{i \in I}$, *entonces* $\varprojlim_i G_i$ *siempre existe y es único bajo isomorfismos.*

Demostración. Sea $\prod_{i \in I} G_i = \{(g_i)_{i \in I} : g_i \in G_i\}$ y considere

$$G = \{(g_i)_{i \in I} : g_i = \varphi_i^j g_j, \quad para \quad j \geq i\}.$$

Mostremos que $G = \varprojlim_i G_i$.

Si $j \in I$, consideremos $\alpha_i : G \ni (g_j)_{j \in I} \mapsto g_i \in G_i$, por definición de límite inverso tenemos que $\varphi_i^j \alpha_j = \alpha_i$. Sea H un grupo y $f_i : H \longrightarrow G_i$ homomorfismos tal que $\varphi_i^j f_j = f_i$, para todo $i \in I$. Defina $\Theta : H \ni h \mapsto (g_j(h))_{j \in I} \in G$. Veamos que $(g_j(h))_{j \in I} \in G$. Sea $j \geq i$, entonces $\varphi_i^j(g_j(h)) = g_i(h)$, luego $(g_i(h))_{i \in I} \in G$, finalmente $\alpha_i \Theta(h) = \alpha_i(g_i(h))_{i \in I} = g_i(h) = f_i(h)$.

□

Ejemplo 5.0.1. *So* $\{G_n, \varphi_n^m\}_{m \geq n}$ *un sistema inverso, donde* $m \geq n$ *si* $G_m \subseteq G_n$ *y* $\varphi_n^m : G_m \longrightarrow G_n$ *es la inclusión. Entonces*

$$\begin{aligned} \varprojlim_m G_m &= \{(g_m)_{n \in \mathbb{N}} : g_n = \varphi_n^m(g_m), m \geq n\} \\ &= \{(g_m)_{n \in \mathbb{N}} : g_m = g_n, m \geq n\} \\ &= \{(g)_{n \in \mathbb{N}} : g \in \bigcup_{n \in \mathbb{N}} G_n\}, \end{aligned}$$

y $\varprojlim_m G_m \cong \bigcup_{n\in\mathbb{N}} G_n$, *concluimos que*

$$\varprojlim_m G_m = \bigcup_{n\in\mathbb{N}} G_n.$$

Ejemplo 5.0.2.

Sea p cualquier primo y consideremos el anillo $\mathbb{Z}/p^n\mathbb{Z}$ *para cada* $n \geq 1$. *Luego si* $n \leq m$ *tenemos la proyección natural*

$$\begin{aligned} f_n^m :&\mathbb{Z}/p^m\mathbb{Z} \longrightarrow \mathbb{Z}/p^n\mathbb{Z} \\ &a + \langle p^m\rangle \longrightarrow a + \langle p^n\rangle \end{aligned}$$

Veamos que f_n^m *esta bien definida.*

Si $a + \langle p^m\rangle = b + \langle p^m\rangle \iff a - b + \langle p^m\rangle = \bar{0}_m \iff a - b = p^m d$ *con* $d \in \mathbb{Z}$. *Aplicando* $f_n^m(a-b) = a - b + \langle p^n\rangle = p^m d + \langle p^n\rangle$, *como* $m \geq n$, *entonces* $m = n + r$ *así*

$$p^{n+r}d + \langle p^n\rangle = p^n p^r d + \langle p^n\rangle = p^n d' + \langle p^n\rangle = \bar{0}_n.$$

Por lo tanto, $a + \langle p^n\rangle = b + \langle p^n\rangle$.

Ahora probemos que $\{\{\mathbb{Z}/p^n\mathbb{Z}\}_{n\in\mathbb{N}}, f_n^m\}$ *es un sistema inverso de grupos.*

i. *Como*

$$\begin{aligned} f_n^n :&\mathbb{Z}/p^n\mathbb{Z} \longrightarrow \mathbb{Z}/p^n\mathbb{Z} \\ &a + \langle p^n\rangle \longrightarrow a + \langle p^n\rangle \end{aligned}$$

Concluimos que $f_n^n = id$.

ii. *Si* $q \geq m \geq n$.

$$\begin{aligned} f_n^m f_m^q(a + \langle p^q\rangle) &= f_n^m(a + \langle p^n\rangle) \\ &= a + \langle p^n\rangle \\ &= f_n^q(a + \langle p^q\rangle). \end{aligned}$$

Entonces, $\{\{\mathbb{Z}/p^n\mathbb{Z}\}_{n\in\mathbb{N}}, f_n^m\}$ *es un sistema inverso de grupos.*

Por lo visto en la Proposición 5.1.1. denotemos el $\varprojlim_n \mathbb{Z}/p^n\mathbb{Z} = G$.

Con $G = \{(a_{p^n})_{n\in\mathbb{N}} : a_{p_n} = f_n^m a_{p_m}\}$.

Así tenemos que

$$\begin{aligned} \alpha_n : G &\longrightarrow \mathbb{Z}/p^n\mathbb{Z} \\ (a_{p^r})_{r\in\mathbb{N}} &\longrightarrow a_{p^n} \end{aligned}$$

donde $a_{p^n} = a + \langle p^n \rangle$.
Ahora veamos que $f_n^m \alpha_m = \alpha_n$.

$$\begin{aligned} f_n^m \alpha_m((a_{p^r})_{r\in\mathbb{N}}) &= f_n^m(a_{p^m}) \\ &= f_n^m(a + \langle p^m \rangle) \\ &= a + \langle p^n \rangle \\ &= a_{p^n} \\ &= \alpha_n((a_{p^r})_{r\in\mathbb{N}}). \end{aligned}$$

Este límite inverso lo denotaremos por $\mathbb{Z}_p$. *Es decir*

$$\mathbb{Z}_p = \varprojlim_n \mathbb{Z}/p^n\mathbb{Z}$$

Llamado el grupo de los enteros $p-$*ádicos. En particular* $\mathbb{Z}_p$ *es un grupo aditivo el cual es límite inverso de grupos finitos.*

Proposición 5.0.2. *Si* $\mathbb{K}/\mathbb{F}$ *es una extensión de Galois,* $G = Gal(\mathbb{K}/\mathbb{F})$, *y* $\mathcal{N}$ *la colección de subgrupos normales de índice finito en* G ($\mathcal{N}$ *está ordenado por inclusión revertida, es decir,* $N \leq M$, *sí y solo sí,* $M \subset N$, *para todos* $N, M \in \mathcal{N}$), *entonces existen proyecciones naturales* $p_N^M : G/M \longrightarrow G/N$ *y* $\{\mathcal{N}, p_N^M\}$ *es un sistema inverso de grupos.*

Demostración. Por la parte 5 del Teorema Fundamental de la Teoría de Galois , tenemos que $G/N \cong Gal(\mathbb{K}^N/\mathbb{F})$ y del mismo modo $G/M \cong Gal(\mathbb{K}^M/\mathbb{F})$, como $M \subset N$ por la parte 6 del Teorema Fundamental de la Teoría de Galois tenemos que $\mathbb{K}^N \subset \mathbb{K}^M$. Por lo tanto,

$$\begin{aligned} p_N^M : Gal(\mathbb{K}^M/\mathbb{F}) &\to Gal(\mathbb{K}^N/\mathbb{F}) \\ \sigma_M &\to res(\sigma) = \sigma|_{\mathbb{K}^N} = \sigma_N. \end{aligned}$$

Ahora veamos que $\{\mathcal{N}, p_N^M\}$ es un sistema inverso de grupos.

i. Es claro que $p_N^N = Id$.

ii. Si $Q \supset M \supset N$, entonces

$$\begin{aligned} p_N^M p_M^Q(\sigma_Q) =& p_N^M(\sigma|_{\mathbb{K}^M}) \\ &= \sigma|_{\mathbb{K}^N} \\ &= \sigma_N \\ &= p_N^Q(\sigma_Q). \end{aligned}$$

Es decir, $p_N^M p_M^Q = p_N^Q$.

Concluimos que $\{\mathcal{N}, p_N^M\}$ es un sistema inverso de grupos. □

Proposición 5.0.3. *Sean $\mathbb{K}, \mathbb{F}, G$ y $\mathcal{N}$, como en la Proposición 5.1.2.*
Para $N \in \mathcal{N}$ considere las proyecciones $p_N : G \longrightarrow G/N$, las cuales corresponden a las restricción de los elementos de $Gal(\mathbb{K}/\mathbb{F})$ en $Gal(\mathbb{K}^N/\mathbb{F})$.Entonces tenemos que $M \subset N$, $p_N = p_N^M \circ p_M$, con ellos obtendremos una proyección de G al límite inverso de todos los G/N y $p : G \ni \sigma \longrightarrow (\sigma_N)_{N\in\mathcal{N}} \in \varprojlim_{N\in\mathcal{N}} G/N$ es un isomorfismo de grupos.

Demostración. Primero probaremos que p es inyectiva. Si $\sigma \in G$, tenemos que $p(\sigma)$ es la identidad en el límite inverso, sí y solo sí, $p(\sigma)_N$ es la identidad en G/N para cada $N \in \mathcal{N}$. Ya que

$$\begin{aligned} \varprojlim_{N\in\mathcal{N}} G/N &= \{(\sigma_N)_N \in \mathcal{N} : \sigma_N = p_N^M \sigma_m, M \subset N\} \\ &= \{(\sigma_N)_N \in \mathcal{N} : \sigma_N = \sigma_M|_{\mathbb{K}^N}, M \subset N\} \end{aligned}$$

Por lo tanto, tenemos que

$$Ker(p) = \bigcap_{N\in\mathcal{N}} N.$$

Sea $\sigma \in Ker(p)$. Si $P_\alpha(X) \in \mathbb{F}[X]$ es el polinomio minimal de $\alpha \in \mathbb{K}$ sobre $\mathbb{F}$ entonces podemos encontrar la extensón de Galois finita $\tilde{\mathbb{F}}/\mathbb{F}$, donde $\mathbb{F} \subset \tilde{\mathbb{F}} \subset \mathbb{K}$.
Ahora consideremos la función

$$res_{\tilde{\mathbb{F}}} : G \longrightarrow Gal(\tilde{\mathbb{F}}/\mathbb{F})$$

la cual es la restricción de un elemento en G al actuar en $\tilde{\mathbb{F}}$.

Ya que $res_{\tilde{\mathbb{F}}}$ es un homomorfismos de grupos con kernel igual a $Gal(\mathbb{K}/\tilde{\mathbb{F}})$ como vimos en la parte 5. del Teorema Fundamental de la Teoría de Galois. Ahora como $Gal(\mathbb{K}/\tilde{\mathbb{F}})$

es un subgrupo normal de G el cual tiene índice finito porque $\tilde{\mathbb{F}}/\mathbb{F}$ es una extensión finita. Pero dado que $\sigma \in Ker(p)$, entonces $\sigma \in Gal(\mathbb{K}/\tilde{\mathbb{F}})$ y en particular, $\sigma(\alpha) = \alpha$. Como α es arbitrario, tenemos que $\sigma = Id$ y así p es inyectiva.

Para probar que p es sobreyectiva, sea $(\sigma_N)_{N\in\mathcal{N}}$ un elemento arbitrario del límite inverso de G/N. Si $\alpha \in \mathbb{K}$, entonces podemos encontrar una extensión finita $\tilde{\mathbb{F}}$ de $\mathbb{F}$ que contiene a α, y $\tilde{N} = Gal(\mathbb{K}, \tilde{\mathbb{F}})$ es un subgrupo normal de índice finito en G, y cada elemento de $G/\tilde{N}$ que puede verse como un elemento de $Gal(\tilde{\mathbb{F}}/\mathbb{F})$.

Ahora defina $\sigma(\alpha) = \sigma_{\tilde{N}}(\alpha)$. La afirmación es que esto define un elemento de G. Si $\mathbb{E}$ es cualquier otra extensión finita de Galois de $\mathbb{F}$ que contiene a α, entonces $\mathbb{L} = \mathbb{E}\tilde{\mathbb{F}}$ también lo es, la cual contiene a $\mathbb{E}$ y $\tilde{\mathbb{F}}$, siendo $Gal(\mathbb{K}/\mathbb{E}) = M$, $Gal(\mathbb{K}/\mathbb{L}) = H$, tenemos que $H \subset M, \tilde{N}$.
Por la construcción de límite inverso, tenemos que $p^H_{\tilde{N}}(\sigma_H) = \sigma_{\tilde{N}}$ y $p^H_M(\sigma_H) = \sigma_M$, mientras que las funciones proyección no cambian la acción sobre α, ya que equivalen a las restricciones de los elemenos del grupo de Galois. Así, σ esta bien definida ya que son automorfismos de $\mathbb{K}$. Dado que la proyección p_N es una restricción de los elementos del grupo de Galois, entonces tenemos que $\sigma_N = p_N(\sigma)$ para cada $N \in \mathcal{N}$, concluimos que $p(\sigma) = (\sigma_N)_{N\in\mathcal{N}}$.

□

En conclusión de esta proposición podemos inferir que si $\mathbb{K}/\mathbb{F}$ es una extensión de Galois de dimensión infinita, su grupo de Galois asociado es el límite inverso de grupos de Galois de dimensión finita.

Bibliografía

[1] DUMMIT, David y FOOTE, Richard. *Abstract Algebra*. Third Edition. John Eiley and Sons, Inc. 2004.

[2] FINE, Benjamin y ROSENBERGER, Gerhard. *The fundamental theorem of algebra*. Springer-Verlag New York. Inc. 1997.

[3] FRALEIGH, John B. *A First Course In Abstract Algebra*. seventh edition. 2007.

[4] GROSSMAN, Stanley I. Y FLORES GODOY, José Job. *Álgebra lineal*. Septima edición.McGRAW-HILL. Interamericana Editores, S.A.2012.

[5] KRICK, Teresa. *Polinomios y Raíces*. Departamento de Matemática. Facultad de Ciencias Exactas y Naturales. Universidad de Buenos Aires. -1428- Buenos Aires. ARGENTINA.

[6] LANG, Serge. *Algebra*. Revised third edition. Graduate Texts in Mathematics, 211. Springer-Verlag, New York, 2002.

[7] MARTIN, Paulo A. *Grupos, corpos e teoria de galois*. Editora Livraria da Física.2010.

[8] ROTMAN, Joseph J. *Advanced Modern Algebra*. Second edition. American Mathematical Society Providence, Rhode Islamd. 2010.

[9] ROTMAN, Joseph J. *An Introduction to Homological Algebra*. Second edition. Springer Science+Business Media, LLC.2009.

[10] SPINDLER, Karlheinz. *Abstract Algebra with Applications*. Volume 2: Rings and Fields, Chapman and Hall/CRC Pure and Applied Mathematics, 1993.