UNIVERSIDAD JUÁREZ AUTÓNOMA DE TABASCO

DIVISIÓN ACADÉMICA DE CIENCIAS BÁSICAS

UN TRATAMIENTO ELEMENTAL AL PROBLEMA INVERSO DE GALOIS A TRAVÉS DEL PROBLEMA DE NOETHER

TESIS PARA OBTENER EL TÍTULO DE:

LICENCIADA EN MATEMÁTICAS

PRESENTA

KAREN DE LA CRUZ RAMOS

BAJO LA DIRECCIÓN DE:

DR. CARLOS ARIEL POMPEYO GUTIÉRREZ

CUNDUACÁN, TABASCO, A 05 DE FEBRERO DE 2025

DIRECCIÓN

Cunduacán, Tabasco; a 04 de febrero de 2025.

C. KAREN DE LA CRUZ RAMOS
PASANTE DE LA LICENCIATURA EN MATEMÁTICAS
PRESENTE

Por medio del presente, me dirijo a usted para hacer de su conocimiento que proceda a la impresión del trabajo titulado **"UN TRATAMIENTO ELEMENTAL AL PROBLEMA INVERSO DE GALOIS A TRAVÉS DEL PROBLEMA DE NOETHER"**, dirigido por el Dr. Carlos Ariel Pompeyo Gutiérrez, bajo la modalidad de titulación por **TESIS**. La comisión de revisión conformada por el Dr. Miguel Ángel de la Rosa Castillo, Dr. Víctor Castellanos Vargas, Dr. Jair Remigio Juárez y Dr. Carlos Ariel Pompeyo Gutiérrez, liberó el documento en virtud de que reúne los requisitos para el **EXAMEN PROFESIONAL** correspondiente.

Sin otro particular, reciba usted un cordial saludo.

A T E N T A M E N T E

DIVISIÓN ACADÉMICA DE CIENCIAS BÁSICAS

DRA. HERMICENDA PÉREZ VIDAL
DIRECTORA

C.c.p. Archivo.

DIR´DRA.HPV/kfvg

Declaración de Autoría y Originalidad

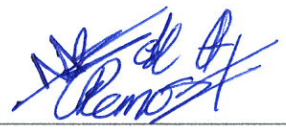
En la Ciudad de Cunduacán, el día 5 del mes febrero del año 2025, la que suscribe Karen De La Cruz Ramos alumna del Programa de Lic. en Matemáticas con número de matrícula 192A31004, adscrita a la División Académica de Ciencias Básicas, de la Universidad Juárez Autónoma de Tabasco, como autora de la Tesis presentada para la obtención del Título de Licenciada en Matemáticas y titulada UN TRATAMIENTO ELEMENTAL AL PROBLEMA INVERSO DE GALOIS A TRAVÉS DEL PROBLEMA DE NOETHER dirigida por Carlos Ariel Pompeyo Gutiérrez.

DECLARO QUE:

La Tesis es una obra original que no infringe los derechos de propiedad intelectual ni los derechos de propiedad industrial u otros, de acuerdo con el ordenamiento jurídico vigente, en particular, la LEY FEDERAL DEL DERECHO DE AUTOR (Decreto por el que se reforman y adicionan diversas disposiciones de la Ley Federal del Derecho de Autor del 01 de Julio de 2020 regularizando y aclarando y armonizando las disposiciones legales vigentes sobre la materia), en particular, las disposiciones referidas al derecho de cita.

Del mismo modo, asumo frente a la Universidad cualquier responsabilidad que pudiera derivarse de la autoría o falta de originalidad o contenido de la Tesis presentada de conformidad con el ordenamiento jurídico vigente.

Villahermosa, Tabasco a 05 de febrero de 2025.



Karen De La Cruz Ramos

Carta de Cesión de Derechos

Villahermosa, Tabasco a 05 de febrero de 2025.

Por medio de la presente manifestamos haber colaborado como AUTORA en la producción, creación y realización de la obra denominada UN TRATAMIENTO ELEMENTAL AL PROBLEMA INVERSO DE GALOIS A TRAVÉS DEL PROBLEMA DE NOETHER.

Con fundamento en el artículo 83 de la Ley Federal del Derecho de Autor y toda vez que, la creación y realización de la obra antes mencionada se realizó bajo la comisión de la Universidad Juárez Autónoma de Tabasco; entendemos y aceptamos el alcance del artículo en mención, de que tenemos el derecho al reconocimiento como autores de la obra, y la Universidad Juárez Autónoma de Tabasco mantendrá en un 100 % la titularidad de los derechos patrimoniales por un período de 20 años sobre la obra en la que colaboramos, por lo anterior, cedemos el derecho patrimonial exclusivo en favor de la Universidad.

COLABORADORES

ALUMNA	DIRECTOR
KAREN DE LA CRUZ RAMOS	DR. CARLOS ARIEL POMPEYO GUTIÉRREZ

TESTIGOS

DRA. ADDY MARGARITA BOLÍVAR CIMÉ	DR. EDILBERTO NÁJERA RANGEL.

LICENCIATURA UN TRATAMIENTO ELEMENTAL AL PROBLEMA INVERSO DE GALOIS A TRAVÉS DEL PROBLEMA DE NOETHER

INFORME DE ORIGINALIDAD

6%
ÍNDICE DE SIMILITUD

FUENTES PRIMARIAS

1	hal.science Internet	287 palabras — 2%
2	hal.archives-ouvertes.fr Internet	220 palabras — 1%
3	matematicas.unex.es Internet	116 palabras — 1%
4	hdl.handle.net Internet	106 palabras — 1%
5	mcc1.mccfl.edu Internet	46 palabras — < 1%
6	repositorio.unesp.br Internet	42 palabras — < 1%
7	idoc.pub Internet	29 palabras — < 1%
8	arxiv.org Internet	27 palabras — < 1%
9	www.joshwalter.net Internet	27 palabras — < 1%

DIVISIÓN ACADÉMICA DE CIENCIAS BÁSICAS
ESTUDIOS TERMINALES

Agradecimientos

A Dios por la continua posibilidad de vivir momentos simples extraordinarios, la fortaleza para afrontar cada experiencia y la sabiduría para desempeñarme en mi carrera, como en este trabajo.

A mi familia, mi inspiración para esforzarme y lograr este título. Mis padres Alicia y Sergio, por su amor, su apoyo y su cuidado continuo. A Sergio Carlos, mi hermanito, por su amor, por estar siempre ahí y por ser un ejemplo para mí.

A mi asesor de tesis y profesor Dr. Carlos Ariel Pompeyo, por dirigir este trabajo, por sus enseñanzas compartidas, por su guía constante y su fe en mis habilidades.

A mis amigos y amigas, por su compañía, soporte y cariño. Son una fuente inagotable de sabiduría y ánimo en mi vida.

A cada uno de mis maestros a lo largo de estos años universitarios, por su dedicación y enseñanzas que me formaron.

A mis compañeros, que compartieron más que solo conocimiento, con los cuales crecí profesional y académicamente, me llevo algo de cada uno de ustedes.

A mis seres especiales de cuatro patas, por un amor especial e incondicional y por la compañía en la noches trabajo.

A Miguel, por traerme felicidad con su radiante existencia y motivarme a dar lo mejor de mí.

Índice general

UN TRATAMIENTO ELEMENTAL AL PROBLEMA INVERSO DE GALOIS A TRAVÉS DEL PROBLEMA DE NOETHER

Resumen y Abstract

Resumen

El problema inverso de Galois, planteado en los primeros años del siglo XIX examina cuándo un grupo finito G surge como grupo de Galois de una extensión de Galois de $\mathbb{Q}$, dicho problema no cuenta con solución completa. En este trabajo se procedió con un un tratamiento y análisis elemental tanto para el problema inverso de Galois como para el enfoque de Noether que permite una solución parcial, como es el caso de los ejemplos presentados. Así mismo, se expone una alternativa para algunos casos donde no es posible aplicar la solución de Noether.

Abstract

The inverse Galois problem, proposed in the early years of 19th century, examines when a finite group G occurs as a Galois group of an extension of $\mathbb{Q}$, this problem doesn't have a complete solution. In this work we provide an elementary treatment for both the inverse Galois problem and Noether's approach which allows us to give a partial solution, such is the case of the presented examples. In addition, we give an alternative for some cases where Noether's solution isn't applicable.

Palabras claves: Problema inverso de Galois, Teorema de irreducibilidad de Hilbert, Teorema de Noether, Polinomios, Extensiones.

Introducción

La Teoría de Galois forma parte del Álgebra abstracta y se concentra en estudiar campos y sus extensiones. Sus inicios se remontan al siglo XIX, desarrollada inicialmente por el matemático francés Évariste Galois y fue empleada para responder algunos de los más famosos cuestionamientos en la historia de la matemática: mediante una construcción con regla y compás, no es posible trisecar un ángulo, duplicar un cubo u obtener la cuadratura de un círculo; así como la prueba de que no existe una fórmula general (con funciones no trascendentes) para encontrar raíces de polinomios de grado 5 o más (Morandi, 2012). Debido a esto, se ha convertido en una herramienta importante para distintas áreas de las matemáticas tales como Teoría de Números y Geometría Algebraica (Stewart, 2022).

El estudio de la Teoría de Galois se centra en cómo se relacionan las extensiones de campo con sus grupos de automorfismos, en razón de esto, es comprensible considerar lo que hoy conocemos como el Problema inverso de Galois, que en su versión clásica examina si un grupo finito puede surgir como el grupo de Galois de una extensión sobre $\mathbb{Q}$.

Por medio de este problema, la Teoría de Galois, con la información obtenida de los grupos de Galois de las extensiones, nos acerca a entender los polinomios y sus raíces. Ahora bien, éste ha sido un problema difícil que aún se encuentra sin solución completa, pero en el que se ha mostrado tal interés que se han involucrado grandes matemáticos como Hilbert y Noether. El Teorema de irreducibilidad de Hilbert y el problema de Noether nos han aproximado a una solución, ya que permiten hallar extensiones sobre los números racionales y de manera más general para los campos numéricos algebraicos bajo ciertas condiciones (Ranjbar y Ranjbar, 2015).

En este trabajo se expondrá un tratamiento más elemental al Problema inverso de Galois, desde la teoría de Campos; haciendo este resultado más comprensible de abordar para la comunidad matemática.

Marco Teórico

La teoría de campos implementada se centra principalmente en las extensiones de campos, que fueron relevantes para solucionar algunos problemas clásicos de construcciones con regla y compás y la solubilidad de ecuaciones polinomiales, (ver por ejemplo, (Morandi, 2012)). Algunos ejemplos de campos son $\mathbb{C}$, $\mathbb{Q}$ y $\mathbb{R}$, con sus operaciones usuales de adición y multiplicación.

Una extensión de un campo es algún otro campo que lo contenga, por lo que podemos encontrar muchas opciones para un campo en particular. Una forma de obtener una extensión, es añadir elementos algebraicos al campo, más explícitamente, al añadir al campo las raíces de algún polinomio irreducible con coeficientes en el campo; dichas extensiones serán de nuestro interés a posteriori.

Al considerar los automorfismos de una extensión, encontramos dos definiciones relevantes: si consideramos los automorfismos que dejen fijos a los elementos del campo base, obtenemos el grupo de Galois de dicha extensión; todos los elementos en la extensión que para un conjunto de automorfismos permanezcan fijos conforman el campo fijo de dicho conjunto. Cuando el campo fijo del grupo de Galois coincide con el campo base, a dicha extensión se le denomina extensión de Galois. Aquí comienza a estrecharse la relación entre extensiones de campos y el grupo de Galois, lo que llegaría a desarrollarse en la Teoría de Galois. De dicha relación podemos destacar dos cosas, la igualdad entre el grado de una extensión de Galois y el orden del Grupo de Galois (para extensiones finitas), y en segundo lugar, la correspondencia entre campos intermedios de una extensión y subgrupos del grupo de Galois, resultado importante plasmado en el Teorema Fundamental de la Teoría de Galois y que incitaría a plantear el Problema inverso de Galois, interés principal de este trabajo.

La Teoría Inversa de Galois trata con la interrogante: ¿Todo grupo finito G puede ser realizable como grupo de Galois de una extensión de Galois de $\mathbb{Q}$?, esto involucra ciertos cuestionamientos más, que se describen en (Ranjbar y Ranjbar, 2015):

a) Problema de existencia general: Determinar cuándo existe una extensión de Galois $L|K$ tal que el grupo de Galois $Gal(L|K)$ es isomorfo a G.

b) Construcción actual: Si a) se cumple, construimos una familia de polinomios sobre K que tengan a G como grupo de Galois.

c) Construcción de polinomios genéricos: Considerando G y K como antes, determinar si existe un polinomio genérico para las extensiones de K que tengan a G como grupo de

Galois, y de ser así, encontrarlo.

d) El número de parámetros: Siguiendo la suposición de que existe, ¿Cuál es el menor número posible de parámetros para un polinomio genérico para una extensión como la descrita antes?

La respuesta a los cuestionamientos, se ha encontrado favorable para ciertos casos, algunos de los cuales se estudiarán en este trabajo.

El caso clásico del problema inverso de Galois es el problema de existencia a) cuando $K = \mathbb{Q}$ el campo de los números racionales. Como consecuencia, de los cuestionamientos descritos anteriormente también se cuenta con el caso regular, es decir, cuando $K = \mathbb{Q}(t)$ el campo de funciones racionales en una indeterminada sobre $\mathbb{Q}$. El problema clásico se tornará el punto central de este proyecto.

El Problema inverso de Galois ha sido un problema difícil que, hasta la fecha, sigue sin resolverse por completo, a pesar de contar con avances desde sus comienzos. Por lo cual, este trabajo contribuye con la divulgación de resultados significativos para la solución al Problema inverso de Galois, así como con un tratamiento elemental de las aproximaciones relevantes y ejemplos ilustrativos favorables.

Capítulo 1

Planteamiento del problema

1.1. Justificación

El Problema inverso de Galois ha sido un problema difícil que, hasta la fecha, sigue sin resolverse por completo, a pesar de contar con avances desde sus comienzos; los primeros resultados que permitieron dar una solución parcial del Problema inverso de Galois recaen en el Teorema de Irreducibilidad de Hilbert y el enfoque del problema de Noether. Por consiguiente, este trabajo contribuye con la divulgación de resultados significativos para la solución al Problema inverso de Galois, así como un tratamiento elemental de las aproximaciones relevantes y ejemplos ilustrativos favorables.

1.2. Preguntas de investigación

- ¿Cuáles son los resultados que sustentan el problema inverso de Galois?
- ¿Cuáles son las condiciones necesarias para que sea factible dar solución al problema inverso de Galois?
- ¿Qué limitantes o alternativas han surgido hasta ahora?

1.3. Hipótesis

Tenemos un grupo finito G actuando sobre el campo de funciones racionales $\mathbb{Q}(X)$, lo cual nos produce el campo $\mathbb{Q}(X)^G$ de funciones racionales invariantes bajo la acción, para el cual la extensión $\mathbb{Q}(X)/\mathbb{Q}(X)^G$ es de Galois con grupo de Galois G y $\mathbb{Q}(X)^G$ es puramente trascendente sobre $\mathbb{Q}$, si esto ocurre, el problema inverso de Galois tiene solución afirmativa, es decir, G es grupo de Galois de alguna extensión de $\mathbb{Q}$.

1.4. Objetivos

1.4.1. Objetivo general

Presentar un tratamiento elemental del Teorema de irreducibilidad de Hilbert y del problema de Noether, los cuales permitieron dar las primeras soluciones afirmativas al problema inverso de Galois.

1.4.2. Objetivos específicos

- Describir el problema inverso de Galois.
- Analizar el enfoque de la solución de Noether al problema inverso de Galois y presentar los resultados que sostienen su solución.
- Enunciar y justificar el Teorema de Irreducibilidad de Hilbert.
- Identificar y establecer las condiciones encontradas en las cuales en enfoque de Noether permite encontrar una solución afirmativa al problema inverso de Galois.
- Mostrar y evidenciar que el enfoque de Noether no permite dar soluciones afirmativas al Problema inverso de Galois en todos los casos.
- Presentar ejemplos concretos en los que el Problema inverso de Galois tiene solución.

1.5. Metodología

Este proyecto siguió una investigación básica (pura), recopilando los hallazgos significativos del Problema inverso de Galois y haciendo un análisis elemental de sus resultados involucrados, principalmente el problema de Noether y el Teorema de Irreducibilidad de Hilbert, teniendo en cuenta, la variable de aquellos grupos de los cuales se pueda obtener una extensión según los requerimientos del problema de Noether; con el fin de incrementar el entendimiento de este problema.

Capítulo 2

Resultados preliminares

El propósito de este capítulo es proporcionar los resultados preliminares de la teoría de campos y Galois necesarios para el desarrollo de los capítulos posteriores de este trabajo.

2.1. Resultados básicos de la Teoría de Campos y Galois

En esta sección se presentan resultados y definiciones que se necesitan en el desarrollo posterior de la tesis. Las demostraciones de dichos resultados pueden consultarse en (Cox, Little, y O'Shea, 2018) y (Morandi, 2012).

2.1.1. Notación y simbología

En lo restante del trabajo consideraremos la siguiente notación:

Símbolo	Significado
F,K	campos
$min(\alpha, K)$	polinomio mínimo de α sobre K
$K\|F$	extensión de campo $F \subseteq K$
$[K : F]$	grado de la extensión $K\|F$
$Aut(K)$	grupo de automorfismos de K
$F[x]$	anillo de polinomios con coeficientes en F en x
$\langle f \rangle$	ideal generado por el polinomio f
$F(\alpha)$	campo generado por F y α
$H \triangleleft G$	H subgrupo normal en G
$char(F)$	característica de F

Definición 2.1.1. Sea $S \neq \emptyset$ y $S \subseteq Aut(K)$. El campo fijo de S es

$$\mathscr{F}(S) = \{a \in K : \tau(a) = a \ \forall \tau \in S \ \}.$$

Definición 2.1.2. Sea $f = a_0 + a_1x + \cdots + a_nx^n \in F[x]$ con raíces $\alpha_1, \ldots, \alpha_n$ en alguna extensión de campo K. El discriminante de f se define como

$$\Delta(f) = \prod_{i \neq j} (\alpha_i - \alpha_j).$$

Es útil notar que $\Delta(f)$ es un polinomio simétrico en $a_1, \ldots, a_n$.

Definición 2.1.3. $K|F$ es normal si K es campo de descomposición de un conjunto de polinomios sobre F.

Definición 2.1.4. Si F es un campo, diremos que un polinomio irreducible $f \in F[x]$ es separable sobre F si no tiene raíces repetidas en ningún campo de descomposición. Un polinomio $g \in F[x]$ es separable sobre F si todos sus factores irreducibles son separables sobre F. Sean $K|F$ una extensión y $\alpha \in K$. Diremos que α es separable sobre F si $min(\alpha, F)$ es separable sobre F. $K|F$ es separable si todo elemento de K es separable sobre F.

Lema 2.1.1. *Sean S un subanillo de $\mathbb{Q}(t)$ y $f, h \in S[x]$, con f mónico. Si $g \in \mathbb{Q}(t)[x]$ y $h = fg$, entonces $g \in S[x]$.*

Demostración. Como f es mónico, (por el algoritmo de la división) existen $q, r \in S[x]$ tales que $h = fq + r$, con $deg(r) < deg(f)$. Tenemos así

$$h = fq + r = fg \Rightarrow r = f(g - q).$$

Como $deg(r) < deg(f)$ y $f \neq 0$,

$$deg(f) + deg(g - q) = deg(r) < \deg(f) \Rightarrow g - q = 0 \ .$$

Por lo tanto, $g = q \in S[x]$. ■

Proposición 2.1.1. *Sean $f \in F[x]$ irreducible y K una extensión de F que contiene una raíz α de f. Entonces, existe un isomorfismo*

$$\Phi : \frac{F[x]}{\langle f \rangle} \longrightarrow F(\alpha)$$

que fija F, i.e., para una constante $g \in F$, $\Phi(g + \langle f \rangle) = g$ y tal que $\Phi(x + \langle f \rangle) = \alpha$.

Proposición 2.1.2. *Sea f un polinomio separable en $F[x]$ de grado n con grupo de Galois $G = Gal(K|F)$. Si $f \in F[x]$ es irreducible, entonces la acción de G en el conjunto de raíces de f es transitiva.*

Teorema 2.1.2 (Extensión de isomorfismo)**.** *Sea $\sigma : F \to F'$ un isomorfismo. Sean $S = \{f_i(x)\}_{i\in I}$ un conjunto de polinomios con coeficientes en F y $S' = \{\sigma(f_i)\}_{i\in I}$ el correspondiente conjunto de polinomios con coeficientes en F'. Sea K un campo de descomposición de S sobre F y K' un campo de descomposición de S' sobre F'. Entonces existe un isomorfismo $\hat{\sigma} : K \to K'$ tal que $\hat{\sigma}|_F = \sigma$. Más aún, si $\alpha \in K$ y α' es raíz de $\sigma(min(\alpha, F))$ en K' entonces podemos elegir $\hat{\sigma}$ de modo que $\hat{\sigma}(\alpha) = \alpha'$.*

Proposición 2.1.3. *Sea $K|F$ una extensión. $K|F$ es de Galois si y sólo si $|Gal(K|F)| = [K : F]$.*

Teorema 2.1.3 (Fundamental de la Teoría de Galois (caso finito))**.** *Sean $K|F$ una extensión finita de Galois y $G = Gal(K|F)$. Existe una biyección que invierte contenciones entre campos intermedios de $K|F$ y subgrupos de G, dada por:*

$$\begin{aligned} \{L : F \subset L \subset K\} &\longrightarrow \{H : H \leq G\} \\ L &\longmapsto Gal(K|L) \end{aligned}$$

con inversa

$$\begin{aligned} \{H : H \leq G\} &\longrightarrow \{L : F \subset L \subset K\} \\ H &\longmapsto \mathscr{F}(H) \quad . \end{aligned}$$

Más aún, si L y H se corresponden entonces

$$[K : L] = |H| \quad y \qquad [L : F] = [G : H]$$

Además, $H \lhd G$ (H es normal en G) si y sólo si $L|F$ es de Galois. Cuando esto ocurre, $Gal(L|F) \cong \dfrac{G}{H}$.

Teorema 2.1.4 (Elemento primitivo)**.** *Si $K|F$ es finita y separable entonces $K = F(\alpha)$ para algún $\alpha \in K$.*

2.2. Extensiones y Automorfismos

En este apartado se encuentran resultados utilizados en el desarrollo del enfoque y Teorema de Noether (capítulo 3).

Lema 2.2.1. *Sea L un campo*

1. *Si K es un subcampo de L entonces $K \subseteq \mathscr{F}(Gal(L|K))$.*
2. *Si $S_1 \subseteq S_2 \subseteq Aut(L)$ entonces $\mathscr{F}(S_2) \subseteq \mathscr{F}(S_1)$.*
3. *Si $S \subseteq Aut(L)$ entonces $S \subseteq Gal(L|\mathscr{F}(S))$.*
4. *Si $K = \mathscr{F}(S)$ para algún $S \in Aut(L)$, entonces $K = \mathscr{F}(Gal(L|K))$.*

Demostración. 1. Sea $a \in K$, si $\sigma \in Gal(L|K) \Rightarrow \sigma|_K = id_K$
$\Rightarrow \sigma(a) = a \quad \forall \sigma \in Gal(L|K) \Rightarrow a \in \mathscr{F}(Gal(L|K))$

$$\therefore K \subseteq \mathscr{F}(Gal(L|K)) \ .$$

2. Sea $a \in \mathscr{F}(S_2) \Rightarrow a \in L$ tal que $\sigma(a) = a \ \forall \sigma \in S_2$ pero $S_1 \subseteq S_2$, en particular $\sigma(a) = a \ \forall \sigma \in S_1 \Rightarrow a \in \mathscr{F}(S_1)$

$$\therefore \mathscr{F}(S_2) \subseteq \mathscr{F}(S_1) \ .$$

3. Si $\sigma \in S$ y $a \in \mathscr{F}(S) \Rightarrow \sigma(a) = a$ y esto $\forall a \in \mathscr{F}(S) \Rightarrow \sigma|_{\mathscr{F}(S)} = id_{\mathscr{F}(S)} \Rightarrow \sigma \in Gal(L|\mathscr{F}(S))$

$$\therefore S \subseteq Gal(L|\mathscr{F}(S)) \ .$$

4. Por 3. $S \subseteq Gal(L|\mathscr{F}(S)) = Gal(L|K)$ y por 2. $K = \mathscr{F}(S) \supseteq \mathscr{F}(Gal(L|K))$. Por 1. $K \subseteq \mathscr{F}(Gal(L|K))$

$$\therefore K = \mathscr{F}(Gal(L|K)) \ .$$

□

Proposición 2.2.1. *Sea G un grupo finito de automorfismos de L con $F = \mathscr{F}(G)$. Entonces $|G| = [L : F]$ y entonces $G = Gal(L|F)$.*

Demostración. Como $G \leq Aut(L) \Rightarrow G \subseteq Gal(L|\mathscr{F}(G)) = Gal(L|F)$.

$$|G| \leq |Gal(L|F)| \leq [L : F].$$

Supongamos $|G| < |Gal(L|F)|$. Sea $n = |G|$ y sea $\{\alpha_1, ..., \alpha_{n+1}\} \subseteq L$ un conjunto linealmente independiente sobre F. Sea $G = \{\tau_1, ..., \tau_n\}$. Considere la matriz

$$A = \begin{bmatrix} \tau_1(\alpha_1) & \cdots & \tau_1(\alpha_{n+1}) \\ \vdots & \ddots & \vdots \\ \tau_n(\alpha_1) & \cdots & \tau_n(\alpha_{n+1}) \end{bmatrix} \in Mat_{n\times(n+1)}(L) \ \cong L$$

es espacio vectorial sobre L. Y rango$(A) \leq min\{n, n+1\} = n$, por lo que las columnas son linealmente dependientes sobre L. Elegimos s mínimo, de modo que las primeras s columnas de A sean linealmente dependientes sobre L (reetiquetando los valores α_i de ser necesario). De este modo existen $c_i \in F$ no todos ceros tales que

$$\sum_{i=1}^{s} c_i \tau_j(\alpha_i) = 0 \ \forall j.$$

Por la minimalidad de s, se sigue que $c_i \neq 0 \ \forall i$.

$$\begin{aligned} c_1\tau_j(\alpha_1) + c_2\tau_j(\alpha_2) + \cdots + c_s\tau_j(\alpha_s) = 0 \\ \Rightarrow \tau_j(\alpha) + \frac{c_2}{c_1}\tau_j(\alpha_2) + \cdots + \frac{c_s}{c_1}\tau_j(\alpha_s) = 0. \end{aligned}$$

Por lo que podemos "renombrar" $c_1 = 1$ y $c_i = \frac{c_i}{c_1}$ para $i > 2$. Si cada c_i pertenece a F, entonces $0 = \tau_j\left(\sum_{i=1}^{s} c_i\alpha_i\right)$ para cada j, entonces $\sum_{i=1}^{s} c_i\alpha_i = 0$. Esto es falso por la independencia de α_i sobre F. Sea $\sigma \in G = \{\tau_1, ..., \tau_n\}$. Dado que σ permuta los elementos de G, es decir

$$\begin{aligned} \sigma : G &\longrightarrow G \\ \tau_i &\longmapsto \tau_m,\ m \in \{1, \ldots, n\}, \end{aligned}$$

la cual no es difícil ver que es biyección, obtenemos que

$$0 = \sigma(0) = \sigma\Big(\sum_{i=1}^{s} c_i\tau_j(\alpha_i)\Big) = \sum_{i=1}^{s} \sigma(\tau_i)\sigma(\tau_j(\alpha_i)) = \sum_{i=1}^{s} \sigma(c_i)\tau_j(\alpha_i) \quad \forall j$$

$$\Rightarrow 0 = \sum_{i=1}^{s}(c_i)\tau_j(\alpha_i) - \sum_{i=1}^{s}\sigma(c_i)\tau_j(\alpha_i) = \sum_{i=2}^{s}\big(c_i - \sigma(c_i)\big)\tau_j(\alpha_i) \quad \forall j\ .$$

Por minimalidad se sigue que $\sigma(c_i) = c_i$ para cada i; ya que esto es cierto para todo $\sigma \in G$, esto implica que $c_i \in \mathscr{F}(G) = F \quad \forall c_i$!
De este modo

$$\begin{aligned} G \subseteq Gal(L|F) \text{ y } |Gal(L|F)| \leq [L : F] = |G| \\ \Rightarrow G = Gal(L|F). \end{aligned}$$

■

Una consecuencia inmediata del resultado previo es que

$$|Gal(L|F)| = [L : F] \ \text{ si } \ F = \mathscr{F}(G) = \mathscr{F}(Gal(L|F)).$$

Proposición 2.2.2. *Supongamos que R es un dominio entero y F su campo de fracciones, adicionalmente sea E una extensión separable de F de grado n. Entonces existe $\alpha \in E$ tal que $E = F(\alpha)$ y $min(\alpha, F) \in R[x]$.*

Demostración. Del Teorema del Elemento Primitivo 2.1.4 sabemos que existe $\beta \in E$ tal que $E = F(\beta)$. Suponga que

$$m(x) = min(\beta, F) = b_0 + b_1x + \cdots + b_{n-1}x^{n-1} + x^n.$$

Como F es el campo de fracciones de R, podemos encontrar una constante distinta de cero $d \in R$ tal que $db_i \in R$ para $i = 0, 1, ..., n-1$, por lo cual $d^{n-i}b_i \in R$. Fijando $\alpha = d\beta$, tenemos $F(\alpha) = F(\beta) = E$, y si

$$f(x) = d^nb_0 + d^{n-1}b_1x + \cdots + db_{n-1}x^{n-1} + x^n,$$

entonces $f \in R[x]$ y

$$f(\alpha) = f(d\beta) = d^nm(\beta) = 0.$$

Si

$$g(x) = a_0 + a_1x + \cdots a_{s-1}x^{s-1} + x^s \in F[x]$$

y $s < n$ entonces

$$n(x) = a_0 + a_1dx + \cdots a_{s-1}d^{s-1}x^{s-1} + x^s \in F[x]$$

y $n(\beta) = 0$, lo cual es absurdo. Por lo tanto f es el polinomio mínimo de α. ■

Comentario. *De ahora en adelante supondremos que los anillos y los campos tienen característica 0 (char$(F) = 0$).*

Lema 2.2.2. *Sean R un dominio entero y F su campo de fracciones, consideremos $E = F(\alpha)$ para $\alpha \in E$, una extensión de Galois de F con $f = min(\alpha, F)$ en $R[x]$ y A un subconjunto finito de E que contiene a α tal que*

$$\forall t \in A \ \forall \sigma \in Gal(E|F), \ \sigma(t) \in A.$$

Entonces existe $u \in R$ tal que, para cualquier campo F' y homomorfismo de anillos $\omega : R \longrightarrow F'$ con $\omega(u) \neq 0$, podemos encontrar una extensión de Galois E' de F' y una extensión del homomorfismo de anillos $\tilde{\omega} : R[A] \longrightarrow E'$ de ω, donde $R[A]$ es el subanillo de E generado por R y A, con las siguientes propiedades:

- *$E' = F'(\alpha')$, donde $\alpha' = \tilde{\omega}(\alpha)$;*
- *Si $f' \in F'[x]$ es el polinomio obtenido de f aplicando ω a los coeficientes de f y f' es irreducible, entonces $G' = Gal(E'|F')$ es isomorfo a $G = Gal(E|F)$.*

Demostración. La demostración se sigue por pasos.

1. Definiendo u : Sea $u = \Delta(f)$, el discriminante de f. Como $char\,(F) = 0$, porque $char\,(R) = 0$ y f es irreducible, entonces f no tiene raíces múltiples. Esto implica que $u \neq 0$. Si F' es un campo y $\omega : R \longrightarrow F'$ un homomorfismo de anillos tal que $\omega(u) \neq 0$, entonces $\Delta(f') = \Delta(\omega(f)) = \omega(\Delta(f)) = \omega(u) \neq 0$, y por tanto f' es separable.

2. Una primera extensión de R y ω: Ahora, construimos un anillo $\tilde{R}$ que contiene a R y extendemos ω a este anillo. Como $E = F(\alpha)$ y $A \subset E$, para cada $t \in A$, existe un $g_t \in F[x]$ tal que $t = g_t(\alpha)$. Además, F es el campo de fracciones de R, por lo que existe $d_t \in R^*$, *i.e.*, un elemento unidad de R, invertible tal que $d_tg_t \in R[x]$, (el producto de los denominadores de los coeficientes de g_t).
Ahora consideramos

$$d = \prod_{t \in A} d_t \ .$$

Entonces $dg_t \in R[x]$, para toda $t \in A$. Establecemos así

$$\tilde{R} = R[d^{-1}] \subset F, \text{ el subanillo de } R \text{ generado por } d^{-1},$$

con $d^{-1} = \prod_{t \in A} d_t^{-1}$ y $d_td_t^{-1} = 1$.
Extendemos así, ω a $\omega_1 : \tilde{R} \longrightarrow F'$, definidas como $\omega_1(d^{-1}) = \omega(u)^{-1}$.

Probaremos que $\tilde{R}[A] = \tilde{R}[\alpha]$. Primero, $\alpha \in A$ implica que $\tilde{R}[\alpha] \subset \tilde{R}[A]$. Por otro lado, si $t \in A$ y $g_t(x) = \sum_{i=0}^{n} a_i x^i$, con $a_0, \ldots, a_n \in F$. Entonces

$$t = g_t(\alpha) = \sum_{i=0}^{n} a_i \alpha^i \Longrightarrow \ dt = \sum_{i=0}^{n} \left(\prod_{y \in A,\ y \neq t} d_y \right) (d_t a_i) \alpha^i,$$

donde $d_t a_i \in R$, para toda i, además $d_y \in R$ para toda y, así $dt \in R[\alpha]$. Sin embargo, $R[\alpha] \subset \tilde{R}[\alpha] \Rightarrow dt \in \tilde{R}[\alpha]$ y $t = d^{-1}(dt) \in \tilde{R}[\alpha]$. Así, $A \in \tilde{R}[\alpha]$ y entonces $\tilde{R}[A] \subset \tilde{R}[\alpha]$.

3. $\tilde{R}[x]/f$ y $\tilde{R}[\alpha]$ son isomorfos: Existe un homomorfismo natural de $\tilde{R}[x]$ en $\tilde{R}[\alpha]$:

$$\begin{aligned} \phi : \tilde{R}[x] &\longrightarrow \tilde{R}[\alpha] \\ g &\longmapsto g(\alpha) \ . \end{aligned}$$

Si $h \in ker(\phi)$, como $ker(\phi)$ es un ideal de $F[x]$, entonces existe $g \in F[x]$ tal que $h = fg$, porque $f = min(\alpha, F)$. Del lema 2.1.1, $g \in \tilde{R}[x]$, porque $\tilde{R}$ es un subanillo de F. Por lo anterior, $h \in \langle f \rangle$, $ker\phi \subset \langle f \rangle$. Por otro lado, si $g \in \langle f \rangle$, entonces $g(\alpha) = f(\alpha)q(\alpha) = 0$, y así, $g \in ker\phi$. Se sigue que $\ker(\phi) = \langle f \rangle$.
Además, $\forall\ h \in \tilde{R}[\alpha]$, $h = g(\alpha) = \phi(g)$, para algún $g \in \tilde{R}[x]$, $Im\phi = \tilde{R}[\alpha]$, *i.e.* ϕ es sobreyectivo. Por el Primer Teorema de Isomorfismo, obtenemos el isomorfismo

$$\bar{\phi} : \frac{\tilde{R}[x]}{\langle f \rangle} \longrightarrow \tilde{R}[\alpha].$$

4. Construcción de una extensión E' de F': El siguiente paso es construir una extensión de Galois E' de F' y un homomorfismo de anillos $\tilde{\omega}$ de $\tilde{R}[A]$ a E', extendiendo ω_1 y por tanto ω. Sea g' un factor irreducible de f' y $\rho : F'[x] \longrightarrow \dfrac{\tilde{F}[x]}{\langle g' \rangle}$ la proyección natural. Del homomorfismo $\omega_1 : \tilde{R} \longrightarrow F'$ construido arriba, obtenemos el homomorfismo natural: $\hat{\omega}_1 : \tilde{R}[x] \longrightarrow \tilde{F}'[x]$. Componiendo, $\hat{\omega}_1$ con ρ obtenemos el homomorfismo

$$\rho \circ \hat{\omega}_1 : \tilde{R}[x] \longrightarrow \frac{\tilde{F}'[x]}{\langle g' \rangle}$$

y luego usamos esto para construir otro homomorfismo:

$$\begin{aligned} \gamma : \frac{\tilde{R}[x]}{\langle f \rangle} &\longrightarrow \frac{F'[x]}{\langle g' \rangle} \\ v + \langle f \rangle &\longmapsto \rho \circ \hat{\omega}_1(v) \ . \end{aligned}$$

(Como $\rho \circ \hat{\omega}_1(f) = f' + \langle g' \rangle$ y $g' | f' (f' = g'q)$, entonces $\rho \circ \hat{\omega}_1(f) = 0 + \langle g' \rangle$, debemos tener $\rho \circ \hat{\omega}_1(v) = 0$, para todo $v \in \langle f \rangle$ y así γ está bien definida.)

Ahora establecemos

$$E' = \frac{F'[x]}{\langle g' \rangle} \qquad \text{y} \qquad \tilde{\omega} = \gamma \circ \bar{\phi}^{-1} \ .$$

Como g' es irreducible, E' es un campo, que claramente es una extensión de F'. También, $\tilde{R}[A] = \tilde{R}[\alpha]$ y entonces $\tilde{\omega}$ es un homomorfismo de $\tilde{R}[A]$ a E'. Necesitamos comprobar que $\tilde{\omega}$ extiende ω. Si $r \in R \subset \tilde{R}[A]$, entonces

$$\begin{aligned}\tilde{\omega}(r) &= \gamma \circ \bar{\phi}^{-1}(r) = \gamma(r + \langle f \rangle) = \rho \circ \hat{\omega}_1(r) \\ &= \rho(\omega_1(r)) = \rho(\omega(r)) = \omega(r) + \langle g' \rangle,\end{aligned}$$

por lo tanto, $\tilde{\omega}$ extiende ω a $\tilde{R}[A]$. Si restringimos $\tilde{\omega}$ a $R[A]$, entonces tenemos el homomorfismo que estamos buscando, a continuación probaremos las condiciones $E' = F'(\alpha')$ y que E' es una extensión de Galois de F'.

5. $E' = F'(\alpha')$: Como

$$\bar{\phi}^{-1}(\alpha) = x + \langle f \rangle$$

y

$$\gamma(x + \langle f \rangle) = \rho(\hat{\omega}_1(x)) = \rho(x) = x + \langle g' \rangle,$$

tenemos

$$\alpha' = \tilde{\omega}(\alpha) = x + \langle g' \rangle$$

y por la proposición 2.1.1,

$$\alpha' = \tilde{\omega}(x + \langle g' \rangle) = x + \langle g' \rangle = \rho(x)$$

$$\Rightarrow F'(\alpha') = F'(x + \langle g' \rangle) = \frac{F'[x]}{\langle g' \rangle} = E' \ .$$

6. E' es una extensión de Galois de F': Sea $\alpha' \in F'(\alpha') = E'$, consideremos $min(\alpha', F')$ que es irreducible sobre F', como $char(F') = 0$, $min(\alpha', F')$ es separable, en consecuencia $E'|F'$ es separable, así sólo necesitamos demostrar que E' es una extensión normal de F'. Sean $\alpha_1, \ldots, \alpha_n$ las raíces de f. Como f es irreducible sobre F, f se escinde en $E = F(\alpha)$, campo de descomposición de f, la proposición 2.1.2 nos asegura que el grupo de Galois $G = Gal(E|F)$ actúa transitivamente en las raíces de f, esto es, para algunas α_i, α_j raíces de f, $\alpha_i = \sigma(\alpha_j)$, para $\sigma \in G$. Consideremos $\alpha \in A$ raíz de f. Entonces las raíces α_i de f son de la forma $\sigma(\alpha) = \alpha_i$ para algún $\sigma \in G$, pero como $\alpha \in A \Rightarrow \sigma(\alpha) = \alpha_i \in A$; esto implica que las raíces de f pertenecen a A. Además, las raíces de f' son $\tilde{\omega}(\alpha_1), \ldots, \tilde{\omega}(\alpha_n)$, ya que, por las relaciones entre las raíces de un polinomio y sus coeficientes (todo polinomio simétrico en las raíces puede ser expresado como un polinomio en los coeficientes de f' y, además los coeficientes de f', fueron obtenidos al aplicara ω a los coeficientes de f y $\tilde{\omega}$ extiende a ω),

$$f'(x) = (x - \tilde{\omega}(\alpha_1)) \cdots (x - \tilde{\omega}(\alpha_n)).$$

Como consecuencia,

$$E' = F'(\alpha') = F'\left(\tilde{\omega}(\alpha_1), \ldots, \tilde{\omega}(\alpha_n)\right)$$

es un campo de descomposición de f', se sigue de la definición 2.1.3, E' es una extensión normal de F'.

7. El caso especial $g' = f'$. En este caso, f' es irreducible, como antes, sean $\alpha_1, \ldots, \alpha_n$ los

conjugados de α. Como $E = F(\alpha)$, del Teorema de Extensión de Isomorfismo (2.1.2) existe un único $\sigma_i \in G$ tal que $\sigma_i(\alpha) = \alpha_i$. Similarmente, $\alpha'_1, \ldots, \alpha'_n$ son los conjugados de α' y, como $E' = F'(\alpha')$ y F es irreducible sobre F', el Teorema 2.1.2 asegura la existencia de un único $\sigma'_i \in G' = Gal(E'|F')$ tal que $\sigma'_i(\alpha') = \alpha'_i$.
Del paso 1. de esta prueba (la definición de u), los valores de $\alpha_1, \ldots, \alpha_n$ son distintos. Consecuentemente, los automorfismos $\sigma_1, \ldots, \sigma_n$ son diferentes elementos de G. Además, por la proposición 2.1.3 $deg(f) = [E : F] = n = |G|$. De este modo, $G = \{\sigma_1, \ldots, \sigma_n\}$. Similarmente, como f' es irreducible, G' tiene cardinalidad n y $G' = \{\sigma'_1, \ldots, \sigma'_n\}$.
Ahora definimos el mapeo Φ de G a G' como $\Phi(\sigma_i) = \sigma'_i$. Probaremos que este mapeo es un isomorfismo. Primero, probaremos que

$$\forall s \in \tilde{R}[A],\ \forall \sigma_i \in G,\ \tilde{\omega}(\sigma_i(s)) = \sigma'_i(\tilde{\omega}(s)). \tag{2.1}$$

Como $\tilde{R}[A] = \tilde{R}[\alpha]$, es suficiente probar la identidad para α y para los elementos de R. Para α tenemos

$$\tilde{\omega}(\sigma_i(\alpha)) = \tilde{\omega}(\alpha_i) = \alpha'_i = \sigma'_i(\alpha') = \sigma'_i(\tilde{\omega}(\alpha)).$$

Si $t \in \tilde{R}$, entonces $t \in F$, por lo cual

$$\begin{aligned}\tilde{\omega}(\sigma_i(t)) = \tilde{\omega}(t) = \gamma \circ \tilde{\phi}^{-1}(t) = \gamma(t + \langle f \rangle) = \rho \circ \hat{\omega}_1(t) \\ = \hat{\omega}_1(t) + \langle g' \rangle = \hat{\omega}_1(t) + \langle f' \rangle,\end{aligned}$$

porque $g' = f'$. Sin embargo, $\hat{\omega}_1(t) \in F'$, por lo tanto,

$$\hat{\omega}_1(t) + \langle f' \rangle = \sigma'_i(\hat{\omega}_1(t) + \langle f' \rangle).$$

De este modo

$$\tilde{\omega}(\sigma_i(t)) = \sigma'_i(\tilde{\omega}(t)).$$

Se sigue que la identidad (2.1) se cumple. Usaremos esta identidad para probar que Φ es un homomorfismo. Desde $\sigma_i(\alpha) \in A$, para $i = 1, \ldots, n$, tenemos

$$\begin{aligned}\Phi(\sigma_i\sigma_j) &= (\sigma_i\sigma_j)'(\alpha') \\ &= (\sigma_i\sigma_j)'(\tilde{\omega}(\alpha)) \\ &= \tilde{\omega}((\sigma_i\sigma_j)(\alpha)) \\ &= \tilde{\omega}(\sigma_i(\sigma_j(\alpha))) \\ &= \sigma'_i(\tilde{\omega}(\sigma_j(\alpha))) \\ &= \sigma'_i\sigma'_j(\tilde{\omega}(\alpha)) \\ &= \sigma'_i\sigma'_j(\alpha') \\ &= \Phi(\sigma_i)\Phi(\sigma_j).\end{aligned}$$

Por lo tanto Φ es un homomorfismo. Claramente Φ es sobreyectiva. Como $|G| = |G'|$, Φ también es inyectiva, por tanto un isomorfismo. Esto finaliza la prueba. ■

Capítulo 3

Teorema de Irreducibilidad de Hilbert

Un campo F es Hilbertiano si para cada $f \in F[x,y]$ que sea irreducible, existen un número infinito de valores $b \in F$ tal que $f_b(y) = f(b,y) \in F[y]$ es irreducible. El propósito principal de este capítulo es probar que $\mathbb{Q}$ es Hilbertiano y presentar algunas consecuencias de este hecho.

3.1. Valores regulares y raíces de polinomios

Definición 3.1.1. Suponga que $f(x,y)$ es un polinomio con coeficientes en $\mathbb{C}$, de grado mayor que cero en y, escrito de la forma

$$f = a_0(x) + a_1(x)y + \cdots + a_n(x)y^n.$$

Dado $b \in \mathbb{C}$, si el polinomio $f_b \in \mathbb{C}[y]$, establecido como $f_b(y) = f(b,y)$ cumple que $a_n(b) \neq 0$, entonces f_b tiene n raíces contando su multiplicidad. Si estas raíces son distintas, entonces diremos que b es un valor regular de f.

Lema 3.1.1. *Si $b \in \mathbb{C}$ es un valor regular del polinomio $f(x,y)$ y $u_1(z), \ldots, u_n(z)$ funciones en $\mathbb{C}$, entonces existe una vecindad W de b en $\mathbb{C}$ tal que las funciones $u_1(z), \ldots, u_n(z)$ son analíticas en W.*

Demostración. Supondremos que las funciones u_i existen y encontraremos sus posibles formas, después mostraremos que las funciones obtenidas satisfacen las condiciones.
Sea $u(z)$ una de las funciones raíz de f, supongamos que $b = 0$ y $u(0) = 0$.
A continuación, buscaremos una serie de potencias $u(z) = \sum_{k=1}^{\infty} b_k z^k$, con $b_k \in \mathbb{C}$, que converja en algún conjunto $W = \{z \in \mathbb{C} \ : \ |z| < R\}$, con $R > 0$, dentro de los cuales $f(z, u(z)) = 0$.
Podemos escribir $f(z, u(z))$ de la forma

$$f(z,u) = a_{00} + a_{10}z + a_{01}u + \sum_{i+j \geq 2} a_{ij} z^i u^j \ .$$

Notemos que $f(0,0) = a_{00}$ y por otra parte $0 = f(0, u(0)) = f(0,0) = a_{00}$, por lo que el termino constante en la expresión es 0 y obtenemos

$$f(z,u) = a_{10}z + a_{01}u + \sum_{i+j\geq 2} a_{ij}z^i u^j \ .$$

La suma de la derecha es finita ya que, f es un polinomio.
Sea f_u la derivada de f con respecto a la variable u. Ahora, como los demás coeficientes de un polinomio en una variable con coeficiente principal 1, quedan dados en las funciones simétricas elementales σ_n evaluadas en las raíces (hasta un factor $\pm$). Sea $z = 0$ un valor regular. Consideremos así

$$\begin{aligned} f(0,u) &= (u-u_1)(u-u_2)\cdots(u-u_n) \\ &= u^n - \sigma_1(u_1,...,u_n)u^{n-1} + \sigma_2(u_1,...,u_n)u^{n-2} + \cdots + (-1)^{n-1}\sigma_{n-1}(u_1,...,u_n)u \\ &\quad + (-1)^n\sigma_n(u_1,...,u_n) \ . \end{aligned}$$

Entonces

$$f(0,0) = (-1)^n\sigma_n(u_1,...,u_n) = 0 = a_{00},$$

donde $\sigma_n(u_1,...,u_n) = u_1u_2\cdots u_n$, obtenemos que

$$f(0,0) = (-1)^n\sigma_n = u_1u_2\cdots u_n = 0 = a_{00}.$$

Por lo cual,

$$u_1u_2\cdots u_n = 0 \Rightarrow u_i(0) = 0 \text{ para algún } i.$$

Sin pérdida de generalidad supongamos $u_1(0) = 0$, entonces

$$\frac{\partial f}{\partial u}(0,0) = (-1)^{n-1}\sigma_{n-1}(u_1,...,u_n) = a_{01},$$

donde $\sigma_{n-1}(u_1,...,u_n) = \sum_{i_1<i_2<\cdots<i_{n-1}} u_{i_1}u_{i_2}\cdots u_{i_{n-1}}$ y $u_1(0) = 0 \Rightarrow \sigma_{n-1}(u_1,...,u_n) = \prod_{j=2}^{n} u_j$

$$\Rightarrow \frac{\partial f}{\partial z}(0,0) = (-1)^{n-1}\prod_{j=2}^{n} u_j(0) = a_{01} \ .$$

Ahora supongamos que $a_{01} = 0 = (-1)^{n-1}\prod_{j=2}^{n} u_j$, entonces $\prod_{j=2}^{n} u_j = 0$ y en consecuencia, $u_j(0) = 0$ para algún $j \neq 1$. Así tenemos que $u_1(0) = u_j(0) = 0$ con $j \neq 1$, por lo que $z = 0$ no es un valor regular!!.
De lo anterior concluimos que $f_u(0,0) = a_{01} \neq 0$. Así podemos escribir

$$f(z,u) = -a_{01}\left(-\frac{a_{10}}{a_{01}}z - u + \sum_{i+j\geq 2} -\frac{a_{ij}}{a_{01}}z^i u^j\right) = -a_{01}\left(a'_{10}z - u + \sum_{i+j\geq 2} a'_{ij}z^i u^j\right). \quad (3.1)$$

Y podemos deducir

$$f_u(z,u) = -a_{01}(-1 + g(z,u)) \ ,$$

donde cada monomio de g tiene grado al menos 1.

Ahora sustituimos $u(z) = \sum_{k=1}^{\infty} b_k z^k$ en la ecuación anterior $f(z,u(z)) = 0$:

$$f(z,u(z)) = -a_{01}\left(a'_{10}z - \sum_{k\geq 1} b_k z^k + \sum_{i+j\geq 2}\left[a'_{ij}z^i\left(\sum_{k\geq 1} b_k z^k\right)^j\right]\right) = 0 \ . \tag{3.2}$$

Como $u(z)$ es una serie de potencias en z, que si suponemos converge a una vecindad de 0, entonces los coeficientes de z, específicamente $a'_{10} - b_1$ toma el valor de 0, lo que implica que $b_1 = a'_{10}$.

Nuestro siguiente paso, es tomar una expansión de Taylor del polinomio $f(z,u)$ en u, alrededor de un punto $u_0 = \sum_{i=1}^{k-1} b_i z^i$. Para $u(z) = \sum_{k\geq 1} b_k z^k$, obtenemos

$$\begin{aligned} f(z,u_0) &= f\left(z, \sum_{i=1}^{k-1} b_i z^i\right) = f\left(z, \sum_{i=1}^{k-1} b_i z^i\right) + f_u(z,u_0)(u-u_0) + \frac{f'_u(z-u_0)}{2}(u-u_0)^2 + \cdots \\ &= f\left(z, \sum_{i=1}^{k-1} b_i z^i\right) + \left(-a_{01}\left(1 + g\left(z, \sum_{i=1}^{k-1} b_i z^i\right)\right)\right)\left(\sum_{k\geq 1} b_k z^k - \sum_{i=1}^{k-1} b_i z^i\right) + \cdots \\ &= f\left(z, \sum_{k=1}^{-1} b_k z^k\right) + \left(-a_{01}\left(-1 + g\left(z, \sum_{i=1}^{k-1} b_i z^i\right)\right)\right)\left(\sum_{i=k}^{\infty} b_i z^i\right) + R, \end{aligned}$$

donde R involucra términos de grado al menos $2k$. Al igualar la expresión anterior a 0, los coeficientes de cada potencia de z deben ser 0. En particular, el coeficiente de z^k es $a_{01}b_k$ más el coeficiente c_k de z^k en la expresión del polinomio $f\left(z, \sum_{i=1}^{k-1} b_i z^i\right)$. Por lo anterior, $a_{01}b_k + c_k = 0 \Rightarrow b_k = -\frac{c_k}{a_{01}}$ y así $b_1 = \dfrac{a_{10}}{a_{01}} = a'_{10}$. Ahora bien, consideremos la expresión multinomial de u_0^j,

$$u_0^j = \left(\sum_{i=1}^{k-1} b_i z^i\right)^j = \sum_{s_1+\cdots s_{k-1}=j} \binom{j}{s_1, \cdots, s_{k-1}} \prod_{t=1}^{k-1} (b_t z^t)^{s_t}$$

donde $\binom{j}{s_1, ..., s_{k-1}} = \dfrac{j!}{s_1! \cdots s_{k-1}!}$, así

$$u_0^j = \sum_{s_1+\cdots s_{k-1}=j} \binom{j}{s_1, \cdots, s_{k-1}} \prod_{t=1}^{k-1} b_t^{s_t} z^{ts_t}.$$

De este modo,

$$a_{ij}z^i\left(\sum_{i=1}^{k-1}b_iz^i\right)^j=a_{ij}z^i\sum_{s_1+\cdots s_{k-1}=j}\binom{j}{s_1,\cdots,s_{k-1}}\prod_{t=1}^{k-1}b_t^{s_t}z^{ts_t}.$$

Notar que

$$\begin{aligned}\prod_{t=1}^{k-1}b_t^{st}z^{tst}&=\left(\prod_{t=1}^{k-1}b_t^{s_t}\right)\left(\prod_{t=1}^{k-1}z^{ts_t}\right)=\left(\prod_{t=1}^{k-1}b_t^{s_t}\right)z^{s_1}z^{2s_2}\cdots z^{(k-1)s_{k-1}}\\&=\left(\prod_{t=1}^{k-1}b_t^{s_t}\right)z^{s_1+2s_2+\cdots+(k-1)s_{k-1}},\end{aligned}$$

por consiguiente,

$$a_{ij}z^i\left(\sum_{i=1}^{k-1}b_iz^i\right)^j=a_{ij}z^i\sum_{s_1+\cdots s_{k-1}=j}\binom{j}{s_1,\cdots,s_{k-1}}\left(\prod_{t=1}^{k-1}b_t^{s_t}\right)z^{i+\sum_{t=1}^{k-1}ts_t}.$$

Se concluye que,

$$f(z,u_0)=\sum_{i,j}\left[a_{ij}z^i\left(\sum_{r=1}^{k-1}b_rz^r\right)^j\right]=\sum_{i+j\geq 2}\left[a_{ij}\sum_{s_1+\cdots s_{k-1}=j}\binom{j}{s_1,\cdots,s_{k-1}}\left(\prod_{t=1}^{k-1}b_t^{s_t}\right)z^{i+\sum_{t=1}^{k-1}ts_t}\right].$$

Donde en $z^{i+\sum_{t=1}^{k-1}ts_t}$ hay que seleccionar los sumandos para los cuales $i+\sum_{t=1}^{k-1}ts_t=k$.

Con la expresión anterior queda expuesto que los coeficientes de z^k están definidos en términos de a_{ij} dados y algunos b_i's con $i<k$ obtenidos de manera recursiva (recordar $b_1=a_{10}'$), de modo que toda la sucesión de los b_i's queda determinada.
Tenemos así, un candidato para la serie, $u(z)=\sum_{k\geq 1}b_kz^k$, para probar su convergencia debemos mostrar que la serie tiene un radio positivo de convergencia, para ello construiremos una serie de potencias $\sum_{k=1}^{\infty}A_kz^k$ con radio positivo de convergencia R tal que $\forall k,\ A_k\geq|b_k|$.

Consideremos

$$f(z,u)=\sum_{i+j\geq 2}\left[a_{ij}\sum_{s_1+\cdots+s_N=j}\binom{j}{s_1,\cdots,s_N}\left(\prod_{t=1}^{N}b_t^{s_t}\right)z^{i+\sum_{t=1}^{N}ts_t}\right].\tag{3.3}$$

Nos fijaremos en los coeficientes de los términos z^k, para ello debemos considerar los coeficientes que acompañan a z cuando $i+\sum_{t=1}^{N}ts_t=i+s_1+2s_2+\cdots+Ns_N=k$ y $j=s_1+\cdots s_N$, con N entero positivo e $i,s_1,s_2,...,s_N\in\mathbb{N}\cup\{0\}$, por lo que $0\leq i\leq k$ y obtenemos los siguientes casos:

Si $i = k \Rightarrow s_1 + \cdots + Ns_N = 0 \Leftrightarrow s_1 = s_2 = \cdots = s_N = 0 \Rightarrow s_1 + \cdots + s_N = 0 = j$, con esto obtenemos el coeficiente

$$a_{ij}\binom{j}{s_1, ..., s_N}\left(\prod_{t=1}^{N} b_t^{s_t}\right) = a_{k0}\binom{0}{0, \ldots, 0}\left(\prod_{t=1}^{N} b_t^0\right),$$

donde $\binom{j}{s_1, ..., s_N} = \dfrac{j!}{s_1! \cdots s_N!} \Rightarrow \binom{0}{0, \ldots, 0} = 1.$
Entonces,

$$a_{k0}\binom{0}{0, \ldots, 0}\left(\prod_{t=1}^{N} b_t^0\right) = a_{k0}\ .$$

Así en la expresión $f(u, z)$ encontramos el término $a_{k0}z^k$.

Continuando de manera recursiva, para $0 < m \leq k - 1$, sea $i = k - m \Rightarrow s_1 + \cdots Ns_N = m < k - 1 \Rightarrow N < k - 1$, luego $\sum_{t=1}^{N} s_t = j$ y los coeficientes obtenidos se expresan como

$$a_{k-m\ j}\binom{j}{s_1, s_2, ..., s_N}\left(\prod_{t=1}^{N} b_t^{s_t}\right)$$

con $N < k - 1$ por lo que los $b'is$ involucrados son conocidos al ser obtenidos de manera recursiva a partir de b_1.

Por último, si $i = 0 \Rightarrow s_1 + \cdots + Ns_N = k$ y para $t > k$ es claro que $s_t = 0 \ \Rightarrow s_1 + 2s_2 + \cdots + ks_k = k$ y $\sum_{t=1}^{k} s_t = j$. Aquí, podemos encontrar distintas combinaciones que cumplan la igualdad, dentro de las cuales tenemos que si $s_k \neq 0 \Rightarrow s_k = 1$ y $s_t = 0\ \forall t < k \Rightarrow N = k$ y $s_1 + \cdots + s_k = 0 + \cdots + 0 + 1 = 1 = j$, obteniendo el coeficiente

$$a_{01}\binom{1}{0, \ldots, 0, 1}\left(\prod_{t=1}^{k} b_t^{s_t}\right) = a_{01}(1)\left(b_k^{s_k}\right) = a_{01}b_k\ .$$

En la expresión (3.3) encontramos el término $a_{01}b_kz^k$.

De este modo si sumamos todos los términos de z^k e igualamos a cero obtenemos

$$\begin{aligned}
&a_{k0}z^k + \sum_{m=1}^{k-1}\left[a_{k-m\ j}\binom{j}{s_1, s_2, \ldots, s_N}\left(\prod_{t=1}^{N} b_t^{s_t}\right)\right] z^k + a_{01}b_k z^k = 0 \\
\Rightarrow &\left(a_{k0} + \sum_{m=1}^{k-1}\left[a_{k-m\ j}\binom{j}{s_1, s_2, \ldots, s_N}\left(\prod_{t=1}^{N} b_t^{s_t}\right)\right] + a_{01}b_k\right) z^k = 0 \\
\Rightarrow &a_{k0} + \sum_{m=1}^{k-1}\left[a_{k-m\ j}\binom{j}{s_1, s_2, \ldots, s_N}\left(\prod_{t=1}^{N} b_t^{s_t}\right)\right] + a_{01}b_k = 0 \\
\Rightarrow &b_k = \frac{-a_{k0} - \sum_{m=1}^{k-1}\left[a_{k-m\ j}\binom{j}{s_1, s_2, \ldots, s_N}\left(\prod_{t=1}^{N} b_t^{s_t}\right)\right]}{a_{01}} \\
\Rightarrow &b_k = a'_{k0} + \sum_{m=1}^{k-1}\left[a'_{k-m\ j}\binom{j}{s_1, s_2, \ldots, s_N}\left(\prod_{t=1}^{N} b_t^{s_t}\right)\right],
\end{aligned}$$

con j y N descritas como antes, $\binom{j}{s_1, s_2, \ldots, s_N}$ un número entero positivo y los b_t's expresados en algunos a'_{ij}'s, encontramos así, para cada k, un polinomio en varias variables con coeficientes enteros positivos, el cual denotamos p_k, tal que b_k es el valor de p_k evaluado en el conjunto de coeficientes a'_{ij}. Escribiremos $b_k = p_k(a'_{ij})$, $i + j \geq 2$.
Sea $A \in \mathbb{Z}$ tal que $A \geq |a'_{ij}|\ \forall a'_{ij}$. Si remplazamos a'_{ij} por A en (3.1) e igualamos a 0, podemos conseguir una nueva ecuación

$$h(z, v) = Az - v + A\sum_{i+j\geq 2} z^i v^j = 0\ .$$

Ahora rehaciendo los cálculos que hicimos para la ecuación (3.1) obtenemos una solución con la forma $\sum_{k=1}^{\infty} A_k z^k$, donde A_k es la la expresión polinomial obtenida de $p_k(a'_{ij})$ reemplazando el a'_{ij} por A, *i.e.*, $p_k(A) = A_k$.
Claramente $A_k \geq |b_k|\ \forall k$, ya que los coeficientes de p_k son positivos.

Para $|z| < 1$ y $|u| < 1$, tenemos que $h(z, v)$ es

$$0 = Az - v + Az^0\sum_{j=2}^{\infty} v^j + Az^1\sum_{j=1}^{\infty} v^j + A\sum_{i=2}^{\infty} z^i\left(\sum_{j=0}^{\infty} v_j\right).$$

Donde las series geométricas anteriores para $|z| < 1$ convergen

$$0 = Az - v + A\frac{v^2}{1-v} + A\frac{zv}{1-v} + A\left(\frac{z^2}{1-z}\right)\left(\frac{1}{1-v}\right).$$

Multiplicando por $1-v$ obtenemos

$$\begin{aligned} 0 &= Az(1-v) - v(1-v) + Av2 + Azv + A\frac{z^2}{1-z} \\ &= Az - Azv - v + v^2 + Av^2 + Azv + \frac{Az^2}{1-z} \\ &= (A+1)v^2 - v + \left(Az + \frac{Az^2}{1-z}\right) \end{aligned}$$

Así

$$h(z,v) = (A+1)v^2 - v + \frac{Az}{1-z} \tag{3.4}$$

es una ecuación cuadrática en v.
Si tomamos un z suficientemente pequeño

$$v(z) = \frac{1 - \left(1 - 4(A+1)\frac{Az}{1-z}\right)^{1/2}}{2(A+1)} \ ,$$

entonces $v(z)$ es la solución de la ecuación (3.4) con $v(0) = 0$. Para ver dónde $v(z)$ es analítica, escogemos la rama principal, es decir donde la raíz cuadrada en la expresión es analítica, esto es $z \in \mathbb{C}$ tal que $|z| < 1$ *i.e.*, el disco unitario. Sean $w_1(z) = (1-z)^{1/2}$ y $w_2(z) = \frac{z}{1-z}$, notar que para

$$\begin{aligned} |z| &< \frac{1}{2} \\ \Rightarrow -|z| &> -\frac{1}{2} \quad \Rightarrow 1 - |z| > \frac{1}{2} \\ \Rightarrow |z| &< \frac{1}{2} < 1 - |z| \leq |1-z| \\ \Rightarrow |z| &< |1-z| \\ \Rightarrow \left|\frac{z}{1-z}\right| &< 1 \ . \end{aligned}$$

Así la imagen de w_2 cae en el dominio de analiticidad de w_1. Por lo que, tomando la composición de funciones analíticas $w_1 \circ w_2$, se concluye que $v(z) = \frac{1}{2(A+1)}(w_1 \circ w_2)$ es analítica en una vecindad de 0.

Recordar $b_k \leq A_k \ \forall k$; sea $p_k : \mathbb{Z}[X] \to \mathbb{R}$ como antes, tenemos que $|p_k(a'_{ij})| = |b_k| \leq A_k \ \forall k$ para todo $a'_{ij} \Rightarrow |p_k(a'_{ij})z^k| = |b_k z^k| \leq A_k z^k$, con $\sum_{k=1}^{\infty} A_k z^k < \infty$ (ya que es la expresión en serie de potencias de $v(z)$ convergente). Entonces por la prueba de M-Weierstrass $\sum_{k=1}^{\infty} b_k z^k$ converge. Por lo que $u(z) = \sum_{k=1}^{\infty} b_k z^k$ es analítica en una vecindad de cero.

Supondremos que $u(0) = 0$ como al comienzo.

Si $u(0) = a$, donde a no es necesariamente 0, entonces escribimos $y(z) = u(z) - a$, entonces tenemos $y(0) = u(0) - a = a - a = 0$, así que obtenemos un nuevo polinomio $g(z, y(z)) = f(z, y + a)$ para el cual y es raíz de g, así que $y(z)$ es analítica para z en una vecindad de 0, por lo cual $u(z)$ es analítica para z suficientemente pequeños.
Finalmente, si suponemos $u(b) = a$, entonces escribimos $y(z) = u(b - z)$, entonces $y(0) = u(b - 0) = u(b) = a$, así tenemos un nuevo polinomio $h(z, y(z)) = f(z, a - y)$, para el cual y es raíz de h, así $y(z)$ es analítica para z suficientemente cercanas a 0, lo que implica que $u(z)$ es analítica para z suficientemente cercanas a b.

De este modo para cada raíz a_i de f_b podemos encontrar una función raíz $a_i(z)$ con $u_i(b) = a_i$ definida en vecindades W_i de b tal que $u_i(b) = a_i \neq a_j = u_j(b)$, $i \neq j$ $\forall i, j = 1, ..., n$, entonces existe una vecindad de $b, W = \cap_{i,j} W_{ij}$, tal que $u_i(z) = a_i \neq u_j(z)$ $\forall z \in W$.

Esto finaliza la prueba. ■

Observación. Para $z \in W$ es posible escribir

$$f(z, Y) = a_n(z) \prod_{i=1}^{n} (-u_i(z) + Y) \ ,$$

donde $a_n(z)$ es un polinomio en z y las u_i's son funciones analíticas definidas en W.

Adicionalmente, consideramos el siguiente resultado.

Tomamos $m+1$ valores crecientes de la variable real t: $t_0 < t_1 < t_2 < \cdots < t_m$ y denotaremos por V_m el determinante de Vandermonde de los t_i's, *i.e.*,

$$V_m = \begin{vmatrix} 1 & t_0 & t_0^2 & \cdots & t_0^{m-1} & t_0^m \\ 1 & t_1 & t_1^2 & \cdots & t_1^{m-1} & t_1^m \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 1 & t_m & t_m^2 & \cdots & t_m^{m-1} & t_m^m \end{vmatrix} .$$

Ahora, sea $f : [t_0, t_m] \to \mathbb{R}$ una función diferenciable m veces y defina

$$W_m = \begin{vmatrix} 1 & t_0 & t_0^2 & \cdots & t_0^{m-1} & f(t_0) \\ 1 & t_1 & t_1^2 & \cdots & t_1^{m-1} & f(t_1) \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 1 & t_m & t_m^2 & \cdots & t_m^{m-1} & f(t_m) \end{vmatrix} .$$

Lema 3.1.2. *Existe $u \in (t_0, t_m)$ tal que*

$$\frac{W_m}{V_m} = \frac{f^{(m)}(u)}{m!} \ .$$

Demostración. Supongamos que $g : [t_0, t_m] \to \mathbb{R}$ es una función m veces diferenciable y que $g(t_i) = f(t_i)\ \forall i$ y f como antes. Así $f - g$ es diferenciable en $[t_0, t_m]$, en particular lo es en $(t_i, t_{i+1})\ \forall i$, a su vez esto implica que $f-g$ es continua en $[t_0, t_m]$, en particular en $[t_i, t_{i+1}]\ \forall i$. Además $f(t_0) = g(t_0) \Rightarrow f(t_0) - g(t_0) = 0 \Rightarrow (f-g)(t_0) = 0$ y $f(t_m) = g(t_m)$ en consecuencia $f(t_m) - g(t_m) = 0$ y $(f-g)(t_m) = 0$, es decir $(f-g)(t_0) = 0 = (f-g)(t_m)$. Por lo que aplicando el Teorema de Rolle en cada intervalo (t_i, t_{i+1}) existe a_i tal que

$$(f-g)'(a_i) = f'(a_i) - g'(a_i) = 0,$$

así

$$f'(a_i) = g'(a_i) \qquad \forall i\ .$$

Así tenemos m puntos $a_0 < a_1 < \cdots < a_{m-1}$ tal que $f'(a_i) = g'(a_i)\ \ \forall i$.

Ahora, aplicando nuevamente el Teorema de Rolle a la función $(f-g)'$, obtenemos $m-1$ puntos $b_0 < b_1 < \cdots < b_{m-2}$ tal que $f^{(2)}(b_i) = g^{(2)}(b_i)\ \ \forall i$.

Continuando de la misma manera, finalmente obtenemos un punto u tal que $f^{(m)}(u) = g^{(m)}(u)$.

Consideremos el sistema

$$\begin{pmatrix} 1 & t_0 & \cdots & t_0^m \\ \vdots & \vdots & \ddots & \vdots \\ 1 & t_m & \cdots & t_m^m \end{pmatrix} \begin{pmatrix} c_0 \\ \vdots \\ c_m \end{pmatrix} = \begin{pmatrix} f(t_0) \\ \vdots \\ f(t_m) \end{pmatrix}\ .$$

En el sistema anterior, la matriz de Vandermonde tiene determinante $V_m = \prod_{0 \le i < j < m} (t_j - t_i)$ con $t_0 < t_1 < \cdots < t_m$, por lo que $V_m \neq 0$ y el sistema tiene solución única, con la cual podemos construir un único polinomio $g(x) = c_0 + c_1 x + c_2 x^2 + \cdots + c_n x^n$ de grado menor o igual que m en $\mathbb{R}[x]$ tal que $g(t_i) = f(t_i)\ \forall i$.

Por el análisis previo, existe un elemento $u \in (t_0, t_m)$ tal que

$$f^{(m)}(u) = g^{(m)}(u) = m! c_m \quad \Rightarrow c_m = \frac{f^{(m)}(u)}{m!}.$$

Aplicando la regla de Cramer al sistema dado, obtenemos

$$c_m = \frac{f^{(m)}(u)}{m!} = \frac{W_m}{V_m} \quad \Rightarrow \quad \frac{W_m}{V_m} = \frac{f^{(m)}(u)}{m!}\ .$$

Esto termina la prueba. ■

Lema 3.1.3. *Sean G un subconjunto abierto conexo de $\mathbb{C}$, f y g funciones analíticas de G en $\mathbb{C}$. Si existe una sucesión $\{z_n\}_{n=1}^{\infty}$ en G y $z_0 \in G$ tal que*

- *Para toda* $n \geq 1$, $z_n \neq z_0$.
- $\lim_{n\to\infty} z_n = z_0$.
- *Para toda* $n \geq 1$, $f(z_n) = g(z_n)$.

Entonces, para toda $z \in G$, $f(z) = g(z)$.

Demostración. Como f y g son analíticas, entonces $f - g$ también lo es, de modo que $(f-g)(z_n) = 0\ \forall n \geq 1$. De manera que el conjunto $Z = \{z \in G : (f-g)(z) = 0\}$ tiene un punto de acumulación (punto límite).
Sea a un punto límite de Z, sea $R > 0$ de modo que $D(a,r) \subseteq G$. Como a es punto límite de Z y $f - g$ es continua, se sigue que $(f-g)(z) = 0 = (f-g)^{(0)}(a)$.
Por contradicción: supongamos que existe i tal que $(f-g)^{(i)}(a) \neq 0$. Elegimos n de modo que

$$(f-g)^{(1)}(a) = (f-g)^{(2)}(a) = \cdots = (f-g)^{(n-1)}(a) = 0 \quad \text{pero } (f-g)^{(n)}(a) \neq 0\ .$$

Como $f - g$ es analítica en G tiene un desarrollo en serie de potencias

$$(f-g)(z) = \sum_{k=n}^{\infty} (z-a)^k$$

para $z \in D(a,R)$.
Sea $h(z) = \sum_{k=n}^{\infty} a_k (z-a)^{k-n} = \sum_{s=0}^{\infty} a_{s+n}(z-a)^s$.
Sea $R = \lim \left|\frac{a_k}{a_{k+1}}\right|$. $R_0 = \lim \left|\frac{b_s}{b_{s+1}}\right| = \lim \left|\frac{a_{s+n}}{b_{s+n+1}}\right| = \lim \left|\frac{a_k}{a_{k+1}}\right| = R$, es decir h es analítica con radio de convergencia R. Además $(z-a)^n h(z) = (f-g)(z)$. Entonces $h(a) = a_n \neq 0$, ya que $a_n = \frac{(f-g)^{(n)}(a)}{n!} \neq 0$. Luego, como h es analítica podemos encontrar r tal que $0 < r < R$ y $h(z) \neq 0\ \forall z \in D(a,r)$. Como a es punto de acumulación de Z, entonces existe $b \in (Z - \{a\}) \cap D(a,r)$, *i.e.*, $(f-g)(b) = 0$, por lo cual $0 = (f-g)(b) = (b-a)^n h(b)$, lo que implica que $h(b) = 0$!! ($h(z) \neq 0\ \forall a \in D(a,r)$).
Por lo tanto, $(f-g)^{(n)}(a) = 0\ \forall n \geq 0$.

Sea $A = \{z \in G : (f-g)^{(n)}(z) = 0\ \forall n \geq 0\}$, por lo visto anteriormente $A \neq \emptyset$. Mostraremos que A es abierto y cerrado. Sea $a \in \overline{A}$. Para $m \in \mathbb{N}$, existe $a_m \in A$ tal que $|a - a_m| < \frac{1}{m}$ tal que $\lim_{m\to\infty} a_m = a$ y como $(f-g)^{(n)}$ es continua, entonces

$$(f-g)^{(n)}(a) = (f-g)^{(n)}\left(\lim_{m\to\infty} a_m\right) = \lim_{m\to\infty} (f-g)^{(n)}(a_m) = 0\ \forall n \geq 0.$$

Se concluye que

$$\Rightarrow a \in A \Rightarrow \overline{A} \subset A$$

y como es un hecho que $A \subset \overline{A}$, se concluye que $A = \overline{A}$, es decir A es cerrado.
Ahora, sea $b \in A$ y sea $R > 0$ tal que $D(b,R) \subset G$, entonces $(f-g)(z) = \sum_{m=0}^{\infty} a_m (z-b)^n\ \forall z \in$

$D(b,R)$ y $a_n = \dfrac{(f-g)^{(n)}(a)}{n!} = 0\ \forall n \geq 0 \ \Rightarrow (f-g)(z) = 0\ \forall z \in D(b,R),\ \forall n \geq 0$, así $D(b,R) \subseteq A$, lo que nos dice que A es abierto.
Como G es conexo, $A \neq \emptyset$ y A es tanto abierto como cerrado, se sigue que $A = G$, en particular $(f-g)(z) = 0\ \forall z \in G$ y se concluye que $f(z) = g(z)\ \forall z \in G$. ■

Proposición 3.1.1. *Sea $g \in \mathbb{C}[x]$ con $deg(g) = m$ y $m+1$ enteros t_i tal que $g(t_i) \in \mathbb{Q}$. Entonces $g \in \mathbb{Q}[x]$.*

Demostración. Sea $g \in \mathbb{C}[x]$, procediendo por inducción sobre g, si $deg(g) = 1$, entonces $g(x) = ax + b$ y existen $t_1, t_2 \in \mathbb{Z}$ tal que $g(t_1), g(t_2) \in \mathbb{Q}$, así

$$g(t_1) = at_1 + b \in \mathbb{Q} \qquad g(t_2) = at_2 + b \in \mathbb{Q}$$

$$\Rightarrow g(t_1) - g(t_2) = a(t_1 - t_2) \quad \Rightarrow a = \frac{g(t_1) - g(t_2)}{t_1 - t_2} \in \mathbb{Q}$$

$$\Rightarrow b = g(t_1) - at_1 \in \mathbb{Q}\ .$$

Por lo tanto, para $deg(g) = 1$, $g \in \mathbb{Q}[x]$.

Supongamos que para $deg(g) = m$ se cumple.

Sea $deg(g) = m+1$ y $m+2$ enteros t_i tal que $g(t_i) \in \mathbb{Q}$; por el algoritmo de la división $g(x) = q(x)(x - t_i) + r$. Claramente $x - t_i \in \mathbb{Q}[x]\ \forall i = 1, ..., m+2$. Veamos que $r \in \mathbb{Q}[x]$,

$$r = q(t_i)(t_i - t_i) + r = g(t_i) \in \mathbb{Q}\ .$$

Consideremos $t_1 \in \mathbb{Z}$

$$\Rightarrow g(t_i) = q(t_i)(t_i - t_1) + r \in \mathbb{Q}$$

$$\Rightarrow q(t_i) = \frac{g(t_i) - r}{t_i - t_1} \in \mathbb{Q}, \quad \forall i \neq 1.$$

Por lo cual $deg(q) = m$ y existen $m+1$ enteros: $t_2, \ldots, t_{m+1}, t_{m+2}$, por la hipótesis de inducción concluimos que $q \in \mathbb{Q}[x]$, por lo que $g \in \mathbb{Q}[x]$. ■

Proposición 3.1.2. *Sea $m \geq 1$ y $f(x) = \sum_{i=0}^{m} a_i x^i \in \mathbb{Z}[x]$. Si $\alpha = \frac{p}{q}$, con $(p,q) = 1$, es una raíz de f, entonces $p|a_0$ y $q|a_m$. Además, si f es mónico, entonces toda raíz racional de f es un entero.*

Demostración. Para $f(x) \in \mathbb{Z}[x]$, consideremos la expresión

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots a_m x^m\ .$$

Sea $\alpha = \frac{p}{q}$ con $p, q \in \mathbb{Z}$ y $(p, q) = 1$ una raíz de f,

$$f\left(\frac{p}{q}\right) = a_0 + a_1\left(\frac{p}{q}\right) + a_2\left(\frac{p}{q}\right)^2 + \cdots a_m\left(\frac{p}{q}\right)^m = 0, \quad q \neq 0 \ .$$

Multiplicando por q^m obtenemos

$$a_0 q^m + a_1 p q^{m-1} + a_2 p^2 q^{m-2} + \cdots + a_m p^m = 0 \tag{3.5}$$

$$\Rightarrow p(a_1 q^{m-1} + a_2 p q^{m-2} + \cdots + a_m p^{m-1}) = -a_0 q^m$$

$$\Rightarrow p| - a_0 q^m \qquad \Rightarrow p|a_0 \quad \text{ó} \quad p| - q^m \ .$$

Si $p| - q^m \ \Rightarrow p|q$!! $((p, q) = 1) \Rightarrow p|a_0$.
Similarmente, de (3.5) obtenemos

$$\Rightarrow q(a_0 q^{m-1} + a_1 p q^{m-2} + \cdots + a_{m-1} p^{m-1} q) = -a_m p^m$$

$$\Rightarrow q| - a_m p^m \qquad \Rightarrow q|a_m \quad \text{ó} \quad q| - p^m \ .$$

Si $q| - p^m \Rightarrow q|p$!! $((p, q) = 1) \Rightarrow q|a_m$.
Ahora, consideremos que f es mónico, y $\alpha \in \mathbb{Q}$ una raíz de f, entonces α puede expresarse como $\frac{c}{d}$ con $c, d \in \mathbb{Z}$ y $(c, d) = 1$, así por lo mostrado previamente

$$d|1 \Rightarrow dk = 1 \text{ p. a. } k \in \mathbb{Z}^+$$

$$\Rightarrow c = cdk$$

$$\Rightarrow \alpha = \frac{c}{d} = ck \in \mathbb{Z} \ .$$

■

Proposición 3.1.3. *Sea $f(x, y)$ un polinomio de grado mayor que 0 en la variable y sobre un campo F de característica 0. Entonces todos excepto un número finito de valores $b \in F$ son regulares.*

Demostración. Podemos escribir a f como

$$f(x, y) = a_0(x) + a_1(x)y + a_2(x)y^2 + \cdots + a_n(x)y^n,$$

donde los $a_i(x)$ son polinomios en x y $a_n(x) \neq 0$.
Si eliminamos los valores de b, tales que $a_n(b) = 0$, entonces $deg(f) = n$. Consideremos $f, f' \in F[x][y]$ con grado total l y $l - 1$ respectivamente. Sea $\Delta(f)$ (respectivamente $\Delta(f_b)$) el discriminante de f (respectivamente f_b), de modo que

$$\Delta(f) = \frac{(-1)^{n(n-1)/2}}{a_n(x)} Res(f, f', y)(x) \ .$$

Sea $b \in F$ tal que

I) $f(b,y) \in F[y]$ tiene grado total $l = deg(a_n(x) + n)$.

II) $\frac{\partial f}{\partial y}(b,y) \in F[y]$ tiene grado total $l-1$.

Entonces, por la proposición 3 de (Cox y cols., 2018) (p. 164) $h = Res(f, \frac{\partial f}{\partial y}, y) \in F[x]$ satisface

$$h(b) = a_n(b)^{l-1-(l-1)} Res(f(b,y), f'(b,y), y) = Res(f_b(y), f_b'(y), y) \ .$$

Como consecuencia

$$Res\left(f, \frac{\partial f}{\partial y}, y\right)(b) = det \begin{pmatrix} a_l(b) & & & d_{l-1}(b) & & \\ \vdots & \ddots & & \vdots & \ddots & \\ \vdots & & a_l(b) & \vdots & & d_{l-1}(b) \\ a_0(b) & & \vdots & d_0(b) & & \vdots \\ & \ddots & \vdots & & \ddots & \vdots \\ & & a_0(b) & & & d_0(b) \end{pmatrix}$$
$$= Res(f_b(y), f_b'(y), y).$$

Así

$$\Delta(f)(b) = \frac{(-1)^{n(n-1)/2}}{a_n(b)} Res\left(f_b(y), f_b'(y), y\right) \ .$$

Por otra parte, $f_b, f_b' \in F[y]$, escribimos f_b como

$$f_b(y) = a_0(b) + a_1(b)y + a_2(b)y^2 + \cdots + a_n(b)y^n \ ,$$

con $deg(f_b) = n$ y $deg(f_b') = n-1$, entonces

$$\Delta(f_b) = \frac{(-1)^{n(n-1)/2}}{a_n(b)} Res\left(f_b, f_b', y\right) \ .$$

De lo anterior concluimos que

$$\Delta(f)(b) = \Delta(f_b) \ ,$$

Luego, como $\Delta(f)$ es un elemento en el campo de funciones racionales de F,

$$\Delta(f)(b) = \frac{a(b)}{d(b)} = \Delta(f_b) = 0 \Leftrightarrow a(b) = 0,$$

donde $a(b)$ y $d(b)$ son polinomios con coeficientes en F; entones existe un número de elementos $u \in F(x)$ para los cuales $\Delta(f)(u) = 0$; en particular, hay un número finito de valores $b \in F$ para los cuales $\Delta(f)(b) = 0$. Si excluimos estos valores, obtenemos que $\Delta(f_b) = \Delta(f)(b) \neq 0$ *i.e.*, b es regular. ■

3.2. $\mathbb{Q}$ es Hilbertiano

El principal objetivo de esta sección es demostrar que el campo de los números racionales $\mathbb{Q}$ es un campo Hilbertiano. Para ello, utilizaremos propiedades fundamentales de los polinomios y resultados relevantes de la teoría de campos.

Teorema 3.2.1 (Teorema de Irreducibilidad de Hilbert)**.** *Si $f(X,Y) \in \mathbb{Q}[X,Y]$ es irreducible, entonces existe un número infinito de números racionales b tal que $f_b(Y) = f(b,Y)$ es irreducible en $\mathbb{Q}[Y]$.*

Demostración. Procederemos a la demostración por pasos.

1. Las funciones coeficientes p_j: De la proposición 3.1.3 sabemos que todos excepto un número finito de valores $b \in \mathbb{Q}$ son valores regulares de f. En consecuencia, elegimos $s_0 \in \mathbb{Q}$ un valor regular de f.
El lema 3.1.1 nos garantiza la existencia de n raíces $u_1(s), \cdots, u_n(s)$ de $f(s,y)$, que son funciones analíticas en W una vecindad en $\mathbb{C}$ de s_0, que supondremos es conexa. Describimos

$$f(x,y) = a_0(x) + a_1(x)y + a_2(x)y^2 + \cdots + a_n(x)y^n$$

donde los $a_i \in \mathbb{Q}[x]$, para $i = 0, , 1, \cdots, n$ y $a_n(x) \neq 0$. Consideremos

$$f(y) = a_0 + a_1 y + a_2 y^2 + \cdots + a_n y^n \ ,$$

donde para $i = 0, 1, ..., n$, a_i es la función polinomial con coeficientes en $\mathbb{Q}$ asociada a cada polinomio $a_i(x)$; estas funciones están definidas en W. Claramente $f \in \mathscr{F}[y]$, donde $\mathscr{F}$ es el anillo de funciones polinomiales en W, con coeficientes en $\mathbb{Q}$. Además, es claro que las funciones $u_1, ..., u_n$ son raíces de f y pertenecen al anillo $\mathscr{A}$ de funciones analíticas definidas en W. Tenemos así

$$f(y) = a_n \prod_{i=1}^{n} (-u_i + y) \ .$$

Ahora sea S un subconjunto propio de $N_n = \{1, ..., n\}$ *i.e.*, $S \neq \emptyset, N_n$ y escribimos

$$\alpha(y) = \prod_{i=1}^{n} (-u_i + y), \qquad \beta(y) = \prod_{i \in S} (-u_i + y) \qquad \text{y} \qquad \gamma(y) = \prod_{i \notin S} (-u_i + y) \ .$$

Entonces, $\alpha, \beta, \gamma \in \mathscr{A}[y]$ y $\alpha = \beta\gamma$. Si los coeficientes tanto de β y γ están en $\mathscr{F}$, entonces el polinomio $f(x,y)$ puede escribirse como un producto de polinomio de grado al menos uno en $\mathbb{Q}[x][y]$. Para ver esto, es suficiente con escribir las igualdades satisfechas por los coeficientes $a_0, a_1, ..., a_n$ en la igualdad $f(y) = a_n\beta\gamma$, donde $a_n \neq 0$. En efecto,

$$\beta(y) = \sum_{i=0}^{k} b_i y^i \qquad \text{y} \quad \gamma(y) = \sum_{j=0}^{l} c_j y^j \ ,$$

donde $b_0, \ldots, b_k, c_0, \ldots, c_l \in \mathscr{F}$. Así,

$$a_0(s) = a_n(s) b_0(s) c_0(s),$$

para un número infinito de números racionales s, por consiguiente

$$a_0(x) = a_n(x)b_0(x)c_0(x).$$

También,

$$a_1(s) = a_n(s)\left(b_0(s)c_1(s) + b_1(s)c_0(s)\right),$$

para un número infinito de números racionales s, por consiguiente

$$a_1(x) = a_n(x)\left(b_0(x)c_1(x) + b_1(x)c_0(x)\right).$$

Continuando de la misma manera encontramos que

$$a_k(x) = a_n(x)\sum_{i+j=k} b_i(x)c_j(x),$$

para $k = 0, 1, \ldots, n$. Si establecemos

$$\beta(x,y) = \sum_{i=0}^{k} b_i(x)y^i \quad \text{y} \quad \gamma(x,y) = \sum_{j=0}^{l} c_j(x)y^j \ ,$$

entonces

$$f(x,y) = a_n(x)\beta(x,y)\gamma(x,y),$$

lo que implica que $f(x,y)$ no es irreducible, una contradicción (que proviene de suponer que tanto $\beta, \gamma \in \mathscr{F}[y]$, es decir β y γ tienen coeficientes en $\mathbb{Q}$). De ello, se deduce que para algún subconjunto propio S de N_n, ya sea β o γ tienen un coeficiente p que no es una función polinomial con coeficientes racionales.

Si reemplazamos los b_i y c_j con cociente de funciones polinomiales con coeficientes racionales, con cálculos análogos a los anteriores concluimos que $f(x,y)$ es reducible en $F(x)[y]$, lo cual no es posible ya que por hipótesis f es irreducible en $\mathbb{Q}[x,y]$ y también lo es en $\mathbb{Q}[x][y]$, se sigue así del Lema de Gauss que f es irreducible en $F[x][y]$. Por lo tanto, asumimos que p no es un cociente de funciones polinomiales con coeficientes racionales. Considerando que n es el grado de f, tenemos que la cardinalidad de conjunto de funciones p es 2^n, pero no consideraremos las posibilidades cuando $deg(p) = 0$ ó $deg(p) = n$, ya que en este caso no tendríamos la factorización de f, numeramos así las distintas funciones $p_1, \ldots, p_{2^n-2}$ (No estamos diciendo que estas funciones son distintas, ciertamente algunas de ellas pueden ser las mismas.)

2. Una condición para la irreducibilidad de $f(s,y)$: Supongamos que $s \in W \cap \mathbb{Q}$ y que todas las $p_1(s), \ldots, p_{2^n-2}(s)$ están en $\mathbb{C}\backslash\mathbb{Q}$. Afirmamos que $f(s,y)$ es irreducible en $\mathbb{Q}[y]$. En efecto, podemos escribir

$$f(s,y) = a_n(s)\prod_{i\in S}(-u_i(s)+y)\prod_{i\notin S}(-u_i(s)+y),$$

para algún subconjunto propio S de N_n. Como s es racional, $a_n(s)$ también lo es. Si evaluamos los coeficientes de β y γ en s, obtenemos los coeficientes de $\prod_{i\in S}(-u_i(s)+y)$ y $\prod_{i\notin S}(-u_i(s)+y)$.

Por la elección de s, al menos uno de estos coeficientes no es racional. De este modo, $f(s, y)$ es irreducible en $\mathbb{Q}[y]$. Para demostrar nuestro Teorema, es suficiente obtener un número infinito de elementos $s \in W \cap \mathbb{Q}$ tal que $p_1(s), \ldots, p_{2^n-2}(s)$ estén en $\mathbb{C}\backslash\mathbb{Q}$.

3. Estudiando las funciones p_j: Nuestro objetivo es mirar las funciones p_j con más detalle. Para simplificar la notación, escribiremos p por p_j. Notemos que existe $T' > 0$ tal que si $t > T'$, entonces $s_0 + \frac{1}{t} \in W$.
Definimos la función δ en (T', ∞) como

$$\delta(t) = p\left(s_0 + \frac{1}{t}\right).$$

Denotemos $\mathscr{G}$ como el conjunto de funciones definidas en (T', ∞) de la forma

$$\xi(t) = \frac{h(t)}{g(t)},$$

donde h y g son funciones polinomiales con coeficientes racionales y g no es la función cero. Claramente $\mathscr{G}$ es un campo. Afirmamos que δ es algebraico sobre $\mathscr{G}$. Para ver esto, primero definiremos la función v_i en (T', ∞) por

$$v_i(t) = u_i\left(s_0 + \frac{1}{t}\right).$$

Entonces, para toda $t > T'$, tenemos

$$a_0\left(s_0 + \frac{1}{t}\right) + a_1\left(s_0 + \frac{1}{t}\right) v_i(t) + a_2\left(s_0 + \frac{1}{t}\right) v_i(t)^2 + \cdots + a_n\left(s_0 + \frac{1}{t}\right) v_i(t)^n = 0.$$

Multiplicamos por una potencia apropiada de t, para obtener la expresión

$$h_0(t) + h_1(t)v_i(t) + h_2(t)v_i(t)^2 + \cdots + h_n(t)v_i(t)^n = 0,$$

donde $h_0, \ldots, h_n$ son funciones polinomiales definidas en (T', ∞), con coeficientes en $\mathbb{Q}$. Así,

$$h_0 + h_1 v_i + h_2 v_i^2 + \cdots + h_n v_i^n$$

es la función cero por lo que v_i es algebraico sobre $\mathscr{G}$. Como los elementos algebraicos de un campo forman un subcampo, $\delta \in \mathscr{G}$ y p es un polinomio simétrico elemental en algunas de las u_i's, entonces δ es polinomio simétrico elemental en algunas de las v_i's y como estas son algebraicas sobre $\mathscr{G}$, se sigue que δ es algebraico sobre $\mathscr{G}$ y en consecuencia es raíz de una ecuación

$$d_0 + d_1 H + \cdots + d_m H^m = 0,$$

donde $d_0, \cdots, d_m \in \mathscr{G}$ y 0 denota la función cero. Supondremos que los d_i son funciones polinomiales. (Es suficiente multiplicar por el producto de los denominadores de los d_i si es necesario.) Si hacemos esto, incluso podemos suponer que los coeficientes de las funciones

polinomiales d_i son enteros. Ahora multiplicando d_m^{m-1} por los coeficientes de las ecuaciones satisfechas por δ para obtener

$$\begin{aligned} d_0 d_m^{m-1} + d_1 d_m^{m-1}\delta + d_2 d_m^{m-1}\delta^2 + \cdots + d_{m-1} d_m^{m-1}\delta^{m-1} + d_m d_m^{m-1}\delta^m &= 0 \\ d_0 d_m^{m-1} + d_1 d_m^{m-2} d_m\delta + d_2 d_m^{m-3} d_m^2\delta^2 + \cdots + d_{m-1} d_m^{m-1}\delta^{m-1} + d_m^m\delta^m &= 0 \\ d_0 d_m^{m-1} + d_1 d_m^{m-2} d_m\delta + d_2 d_m^{m-3}(d_m\delta)^2 + \cdots + d_{m-1}(d_m\delta)^{m-1} + (d_m\delta)^m &= 0\ . \end{aligned}$$

De este modo $z = d_m\delta$ es una raíz del polinomio

$$g(Z) = b_0 + b_1 Z + \cdots b_{m-1} Z^{m-1} + Z^m,$$

donde $b_j = d_j d_m^{m-j-1}$, para $j = 0, 1, \cdots, m-1$. Claramente, los coeficientes de $g(Z)$ son polinomios con coeficientes enteros (por lo supuesto antes). Afirmamos que, si $t \in \mathbb{Z}$, con $t > T'$ y $\delta(t) \in \mathbb{Q}$ entonces $z(t) \in \mathbb{Z}$. En efecto $z(t) = d_m(t)\delta(t)$ implica que $z(t) \in \mathbb{Q}$. También, $z(t)$ es una raíz de la ecuación

$$b_0(t) + b_1(t)Z + \cdots + b_{m-1}(t)Z^{m-1} + Z^m,$$

que es un polinomio mónico con coeficientes en $\mathbb{Z}$. Por la proposición 3.1.2, $z(t)$ es un entero.

4. Estudiando las funciones z_j: Como z está en términos de δ y esta en términos de p_j, tenemos una función $z_j = d_m\delta$ para cada j, pero para simplificar la notación, escribiremos z por z_j; nuestro siguiente paso es mostrar que hay relativamente pocos enteros $t > T'$ tal que $z(t)$ es un entero. Si este es el caso, entonces encontraremos muchos enteros t tal que $z(t)$ no es un entero. Para tales t, $\delta(t)$ no puede ser racional, lo que implica que $p(s_0 + \frac{1}{t})$ no es racional.

El lema 3.1.1 nos asegura que, para $i = 1, \ldots, n$ la función u_i es analítica en la vecindad W de s_0. Como sumas y productos de funciones analíticas son analíticas, para $j = 1, ..., 2^{n-2}$, p_j es analítica en W. Reduciendo el tamaño de W a una vecindad W' de s_0 de ser necesario, para $s_0 + x \in W'$, escribimos

$$p(s_0 + x) = e_0 + e_1 x + e_2 x^2 + \cdots + e_k x^k + \cdots\ ,$$

donde los coeficientes $e_i \in \mathbb{C}$. Entonces existe $T'' \geq T'$ tal que, si $t > T''$, entonces $(s_0 + \frac{1}{t}) \in W'$ y así

$$p\left(s_0 + \frac{1}{t}\right) = e_0 + e_1\frac{1}{t} + e_2\left(\frac{1}{t}\right)^2 + \cdots + e_k\left(\frac{1}{t}\right)^k + \cdots.$$

Como d_m es un polinomio, podemos escribir

$$z(t) = d_m(t)\delta(t) = d_m(t)p\left(s_0 + \frac{1}{t}\right) = c_l t^l + \cdots + c_1 t + c_0 + c_{-1}t^{-1} + \cdots + c_{-k}t^{-k} + \cdots\ ,$$

con $c_i \in \mathbb{C}$.

Tenemos tres posibilidades:

a) z es una función polinomial;

b) z no es una función polinomial y tiene al menos un coeficiente $c_i \in \mathbb{C}\backslash\mathbb{R}$;

c) z no es una función polinomial y todos los coeficientes de z son reales.

Consideraremos el primer caso. Afirmamos que al menos uno de los coeficientes debe de estar en $\mathbb{C}\backslash\mathbb{Q}$. Si este no es el caso, entonces $\delta(t) = \frac{z(t)}{d_m(t)}$ para $t > T''$. Sea $\{t_n\}$ una sucesión de valores $t > T''$ convergente a ∞. Si establecemos $s_n = s_0 + \frac{1}{t_n}$, entonces los números s_n convergen a s_0 y

$$p(s_n) = p\left(s_0 + \frac{1}{t_n}\right) = \delta(t_n) = \frac{z(t_n)}{d_m(t_n)} = \frac{z\left((s_n - s_0)^{-1}\right)}{d_m\left((s_n - s_0)^{-1}\right)} \ .$$

Si multiplicamos ambos lados de la igualdad por una potencia apropiada de $s_n - s_0$, entonces podemos encontrar una función polinomial con coeficientes racionales $\hat{z}$ y $\hat{d}_m$ tal que

$$\frac{z\left((s_n - s_0)^{-1}\right)}{d_m\left((s_n - s_0)^{-1}\right)} = \frac{\hat{z}(s_n)}{\hat{d}_m(s_n)}.$$

Del lema 3.1.3, obtenemos que $p = \frac{\hat{z}}{\hat{d}_m}$, una contradicción, porque p no es un cociente de funciones polinomiales con coeficientes racionales. (Podemos aplicar el lema 3.1.3, porque p y $\frac{\hat{z}}{\hat{d}_m}$ están definidas en el conjunto conexo W.) Esto prueba nuestra afirmación.

Así al menos un coeficiente de z pertenece al conjunto $\mathbb{C}\backslash\mathbb{Q}$. Consecuentemente, de la proposición 3.1.1, solo puede haber un número finito de enteros t tal que $z(t)$ es un entero. En este caso podemos elegir $T''' > T''$ tal que $z(t)$ no es un entero, si $t > T'''$.

Ahora consideremos el segundo caso. Supongamos que i_0 es el subíndice i más grande para el cual $c_i \in \mathbb{C}\backslash\mathbb{R}$. Entonces

$$\begin{aligned}
z(t) &= c_{-k}t^{-k} + c_{-(k-1)}t^{-(k-1)} + \cdots + c_{-1}t^{-1} + c_0 + c_1 t + c_2 t^2 + \cdots + c_l t^l \\
&= \sum_{j=-k}^{l} c_j t^j \\
&= \sum_{j=-k}^{i_0-1} c_j t^j \ + c_{i_0} t^{i_0} \ + \sum_{j=i_0+1}^{l} c_j t^j \\
\Rightarrow Im(z(t)) &= Im\left(\sum_{j=-k}^{i_0-1} c_j t^j \ + c_{i_0} t^{i_0} \ + \sum_{j=i_0+1}^{l} c_j t^j\right) \\
\Rightarrow Im(z(t)) &= \sum_{j=-k}^{i_0-1} Im\left(c_j t^j\right) \ + Im\left(c_{i_0} t^{i_0}\right) = \sum_{j=-k}^{i_0-1} t^j Im\left(c_j\right) \ + t^{i_0} Im\left(c_{i_0}\right) \\
\Rightarrow \frac{Im(z(t))}{t^{i_0}} &= \frac{\sum_{j=-k}^{i_0-1} t^j Im\left(c_j\right) \ + t^{i_0} Im\left(c_{i_0}\right)}{t^{i_0}} = \frac{\sum_{j=-k}^{i_0-1} t^j Im\left(c_j\right)}{t^{i_0}} + Im\left(c_{i_0}\right) \\
\Rightarrow \lim_{t\to\infty} \frac{Im(z(t))}{t^{i_0}} &= \lim_{t\to\infty} \left(\frac{\sum_{j=-k}^{i_0-1} t^j Im\left(c_j\right)}{t^{i_0}} + Im(c_{i_0})\right) = \sum_{j=-k}^{i_0-1} Im\left(c_j\right) \lim_{t\to\infty} \frac{1}{t^{i_0-j}} + Im(c_{i_0}) = Im(c_{i_0}) \neq 0 \ .
\end{aligned}$$

De lo anterior se tiene que

$$\lim Im\left(\frac{z}{t^{i_0}}\right) = \lim \frac{Im(z)}{t^{i_0}} \neq 0 \;\Rightarrow\; \frac{z}{t^{i_0}} = w \notin \mathbb{R} \Rightarrow z = t^{i_0} w \notin \mathbb{R}\ .$$

Por eso, podemos encontrar $T''' \geq T''$ tal que $\frac{z(t)}{t^{i_0}} \notin \mathbb{R}$ para $t > T'''$. Esto implica que $z(t) \notin \mathbb{R}$ y entonces no es un entero, para $t > T'''$.

El tercer caso es más difícil de manejar. Aquí todos los coeficientes c_i, con i negativo, son distintos de cero. Diferenciando z un número suficiente de veces podemos eliminar todas las potencias no negativas de t obteniendo

$$z^{(m)}(t) = rt^{-q} + \cdots\ ,$$

donde r es un número real distinto de cero, q es un entero positivo mayor que m y los puntos suspensivos representan términos de potencias superiores de t^{-1}. Como

$$\begin{aligned}
\lim_{t\to\infty} t^q z^{(m)} &= t^q \left[\frac{r}{t^q} + \frac{r_{q+1}}{t^{q+1}} + \frac{r_{q+2}}{t^{q+2}} + \cdots\right] \\
&= \lim_{t\to\infty} t^q \left(\frac{r}{t^q}\right) + \lim_{t\to\infty} t^q \left[\frac{r_{q+1}}{t^{q+1}} + \frac{r_{q+2}}{t^{q+2}} + \cdots\right] \\
&= r \lim_{t\to\infty} \left(\frac{t^q}{t^q}\right) + \lim_{t\to\infty} t^q \left[\frac{r_{q+1}}{t^{q+1}} + \frac{r_{q+2}}{t^{q+2}} + \cdots\right] \\
&= r(1) + \left[\lim_{t\to\infty} t^q(0)\right] \\
&= r + 0 \\
&= r\ ,
\end{aligned}$$

así $\forall \epsilon > 0,\ T''' > 0$ tal que si $t > T''' \Rightarrow \left|t^q z^{(m)}(t) - r\right| < \epsilon$, luego

$$\begin{aligned}
\left||t^q z^{(m)}(t)| - |r|\right| &< |t^q z^{(m)}(t) - r| < \epsilon \\
\Rightarrow |t^q z^{(m)}(t)| - |r| &< \epsilon \\
\Rightarrow |t^q z^{(m)}(t)| &< \epsilon + |r| \\
\Rightarrow |z^{(m)}(t)| &< \frac{\epsilon + |r|}{t^q}, \quad t > 0.
\end{aligned}$$

Sea $\epsilon = |r|$, obtenemos que

$$|z^{(m)}(t)| \;<\; \frac{|r| + |r|}{t^q} = \frac{2|r|}{t^q}.$$

Entonces, existe $T''' > T''$ tal que

$$t > T''' \Rightarrow 0 < |z^{(m)}(t)| \leq 2|r|t^{-q}\ .$$

Ahora usando el Lema 3.1.2. Sean $t_0 < t_1 < \cdots < t_m$ enteros tal que $t_i \geq T'''$ y $z(t_i) \in \mathbb{Z}\ \forall i$. Para cierto número $u \in (t_0, t_m)$ tenemos

$$\frac{2|r|}{m! t_0^q} > \frac{2|r|}{m! u^q} \geq \frac{|z^{(m)}(u)|}{m!} = \frac{|W_m|}{|V_m|}\ .$$

Como $z^{(m)}(u) \neq 0$, $W_m \neq 0$, implica que W_m es un entero y entonces $|W_m| \geq 1$. De la desigualdad anterior tenemos que

$$\frac{2|r|}{m!t_0^q} > \frac{|W_m|}{|V_m|} \Rightarrow \frac{m!t_0^q}{2|r|} \leq \frac{m!t_0^q}{2|r|}|W_m| < |V_m| \ .$$

Notemos también que $(t_i - t_j) \leq (t_m - t_0)\ \forall i, j$, así

$$|V_m| = \prod_{i>j}(t_i - t_j) < (t_m - t_0)^{\frac{m(m-1)}{2}} \ .$$

Por lo tanto,

$$\frac{m!}{2|r|}t_0^q < |V_m| = \prod_{i>j}(t_i - t_j) < (t_m - t_0)^{\frac{m(m-1)}{2}} \ .$$

Esto implica que hay constantes positivas α y β tal que $\alpha t_0^\beta < t_m - t_0$.

Ahora sea $\tilde{r}$ el número de funciones distintas z_j en este tercer caso. Sin pérdida de generalidad, suponemos que estas son las funciones $z_1, \ldots, z_{\tilde{r}}$. Para cada j tenemos m_j, α_j y β_j, tal que, si tenemos enteros $t_0 < t_1 < \cdots < t_{m_j}$, con $z_j(t_i) \in \mathbb{Z}$, para $i = 0, 1, \ldots, m_j$, entonces $\alpha_j t_0^{\beta_j} < t_{m_j} - t_0$. Establezcamos $\overline{m} = max\ m_j$ y tomemos $U \in \mathbb{Z}$ tal que $\alpha_j U^{\beta_j} \geq \tilde{r}\overline{m}$. Ahora consideremos el intervalo $I = [U, U + \tilde{r}\overline{m}]$. Queremos establecer una cota de los t_is que contiene el intervalo. Por contradicción, supongamos que tenemos $m_j + 1$ enteros $t_{0_j}, t_{1_j}, \ldots, t_{m_j}$, donde cada t_i depende de j, por simplicidad escribiremos $t_0, t_1, \ldots, t_j$. Si $t_0 < t_1 < \cdots < t_{m_j}$ es una sucesión de $m_j + 1$ enteros en I, entonces

$$\alpha_j t_0^{\beta_j} \geq \alpha_j U^{\beta_j} \geq \tilde{r}\overline{m} = (t_0 + \tilde{r}\overline{m}) - t_0 \geq U + \tilde{r}\overline{m} - t_0 \geq t_{m_j} - t_0$$

$$\Rightarrow \alpha_j t_0^{\beta_j} \geq t_{m_j} - t_0\ !.$$

Esto implica que I contiene a lo más m_j enteros tal que $z_j(t) \in \mathbb{Z}$.

Si ahora consideramos todas las z_j en el tercer caso, vemos que el intervalo contiene a los más $m_1 + \cdots + m_{\tilde{r}}$ enteros t tal que $z_j(t) \in \mathbb{Z}$ para para $j = 1, \ldots, \tilde{r}$, *i.e.*, a lo más $\tilde{r}\overline{m}$ enteros t tal que $z_j(t) \in \mathbb{Z}$, para $j = 1, \ldots, \tilde{r}$. Sin embargo, I contiene $\tilde{r}\overline{m} + 1$ enteros, así que hay al menos un entero $t \in I$ tal que $z_j(t) \notin \mathbb{Z}$, para $j = 1, \ldots, \tilde{r}$. Podemos encontrar un número infinito de intervalos $I_k = [U_k, U_k + \tilde{r}\overline{m}]$, con $U_{k+1} > U_k + \tilde{r}\overline{m}$.

5. El paso final: Usando nuestro trabajo previo, mostramos que hay un infinito número de sucesiones de enteros t tal que $z_j(t)$ no es un entero, para toda z_j. Como hemos visto hay tres posibilidades para z_j. Para aquellas que caen en el caso a) o b), hay un número T''' tal que, si $t > T'''$, entonces $z_j(t) \notin \mathbb{Z}$. Si tomamos T''' igual a el máximo de todas estas T''', entonces $z_j(t) \notin \mathbb{Z}$, para esas $z_j(t)$, donde z_j está en el caso a) o b). Si el caso c) es vacío, entonces ya terminamos. Si este no es el caso y $z_1, \ldots, z_{\tilde{r}}$ pertenecen al tercer caso, entonces podemos encontrar una sucesión de enteros t tal que $z_j(t) \notin \mathbb{Z}$ para $j = 1, \ldots, \tilde{r}$. Podemos tomar estos enteros mayores que T''' y así tenemos una sucesión infinita de enteros t tal que $z_j(t) \notin \mathbb{Z}$ para toda j. Esto finaliza la prueba. ■

Proposición 3.2.1. *Las siguientes proposiciones son equivalentes:*

a) Si $f \in \mathbb{Q}[x,y]$ es irreducible, entonces $\exists$ infinitos $b \in \mathbb{Q}$ tal que $f(b,y)$ es irreducible en $\mathbb{Q}[y]$.

b) Si $f \in \mathbb{Q}(x)[y]$ es irreducible, entonces $\exists$ infinitos $b \in \mathbb{Q}$ tal que $f(b,y)$ es irreducible en $\mathbb{Q}[y]$.

Demostración. b) $\Rightarrow$ a). Sea $f \in \mathbb{Q}[x][y] \subset \mathbb{Q}(x)[y]$ irreducible, existen infinitos $b \in \mathbb{Q}$ tal que $f(b,y)$ es irreducible en $\mathbb{Q}[y]$.

a) $\Rightarrow$ b). Sea $f \in \mathbb{Q}(x)[y]$ irreducible, así $f = \dfrac{a_0(x)}{b_0(x)} + \dfrac{a_1(x)}{b_1(x)}y + \cdots + \dfrac{a_n(x)}{b_n(x)}y^n, \quad a_i, b_i \in \mathbb{Q}[x]$ puede escribirse como

$$uf = a_0 \prod_{i\neq 0} b_i + a_1 \prod_{i\neq 1} b_i y + \cdots + a_n \prod_{i\neq n} b_i y^n, \quad a_i \prod_{i\neq j} b_j \in \mathbb{Q}[x];$$

donde $u = \prod_{i=0}^{n} b_i \in \mathbb{Q}[x] \subseteq Q(x)[y]^*$ es una unidad producto de los denominadores de f, lo que implica que $uf \in \mathbb{Q}(x)[y]$ sigue siendo irreducible.
Denotemos $c(f)$, el contenido de f, *i.e.*, el máximo común divisor de sus coeficientes. Escriba en $\mathbb{Q}[x][y]$, $uf = c(uf)h$ donde $c(h) = 1$ ($h \in \mathbb{Q}[x][y] \subseteq \mathbb{Q}(x)[y]$). Entonces

$$h = \frac{u}{c(uf)}f \quad \text{y} \quad \frac{u}{c(uf)} \in \mathbb{Q}(x,y)^* \ ,$$

y como f es irreducible en $\mathbb{Q}(x)[y] \Rightarrow uf = c(uf)\ h$ es irreducible en $\mathbb{Q}(x)[y] \Rightarrow h = \dfrac{u}{c(uf)}f$ es irreducible en $\mathbb{Q}(x)[y]$ (y es primitivo en $\mathbb{Q}[x][y]$), así por el lema de Gauss h es irreducible en $\mathbb{Q}[x][y]$.
Como a) es cierto, existen infinitos $b \in \mathbb{Q}$ tales que $h_b(y)$ es irreducible en $\mathbb{Q}[y]$.
En $\mathbb{Q}(x)[y]$: $f = \dfrac{c(uf)}{u}h$ donde $c(uf), u \in \mathbb{Q}[x] \Rightarrow \dfrac{c(uf)}{u} \in \mathbb{Q}[x]$

$$\Rightarrow f_b(y) = \left.\frac{c(uf)}{u}\right|_{x=b} h_b(y) \ ,$$

con $\left.\dfrac{c(uf)}{u}\right|_{x=b} \in \mathbb{Q}$ si $u(b) \neq 0$, pero $u(x)$ un número finito de ceros y $c(uf)$ también tiene un número finito de ceros, además $h_b(y)$ irreducible. Entonces existe una infinidad de $b \in \mathbb{Q}$ tales que $\dfrac{c(uf)}{u} \in \mathbb{Q} - \{0\}$ y para los cuales $h_b(y)$ es irreducible, para dichos valores b, por lo cual $f_b(y)$ es irreducible en $\mathbb{Q}[y]$. ■

3.3. Consecuencias de que $\mathbb{Q}$ sea Hilbertiano

Observación. Sea E una extensión de Galois de grado n de $\mathbb{Q}(x)$, el campo de fracciones del anillo de polinomios $\mathbb{Q}[x]$. Por el Teorema del Elemento Primitivo 2.1.4, sabemos existe un elemento $\alpha \in E$, tal que $E = \mathbb{Q}(x)(\alpha)$ y $f(y) = min(\alpha, \mathbb{Q}(x)) \in \mathbb{Q}[x][y]$. Entonces f es irreducible en $\mathbb{Q}[x][y]$.

Con un razonamiento similar a la demostración anterior, se pueden probar los siguientes resultados.

Corolario 3.3.1. *Si $f \in \mathbb{Q}(x)[x_1, \ldots, x_n][y]$ con $n \geq 2$ irreducible, entonces existen infinitos $(b_1, \ldots, b_n) \in \mathbb{Q}^n$ tal que $f_b(y) = f(b_1, \ldots, b_n, y)$ es irreducible.*

Demostración. Procedimiento de inducción. ■

Observación. La propiedad Hilbertiana de $\mathbb{Q}$ garantiza que para cualquier polinomio irreducible en $\mathbb{Q}[x, y]$, podemos encontrar infinitos valores de x que produzcan un polinomio irreducible en $\mathbb{Q}[y]$.

Teorema 3.3.1. *$\mathbb{Q}(x_1, \ldots, x_k)$ es un campo Hilbertiano para $k \in \mathbb{N}^+$.*

Demostración. Similar a proposición 3.2.1 ■

Teorema 3.3.2. *Si $\mathbb{Q}(x_1, \ldots, x_k)$ es una extensión de Galois de $\mathbb{Q}(x_1, \ldots, x_k)^G$ con grupo de Galois G y G actuando en $\mathbb{Q}(X)$ con $X = \{x_1, \ldots, x_k\}$, entonces existe una extensión de Galois E' de $\mathbb{Q}$ tal que $Gal(\mathbb{Q}(X)|\mathbb{Q}(X)^G)$ es isomorfo a $Gal(E'|\mathbb{Q})$.*

Demostración. Procederemos por inducción sobre k. Para $k = 1$, es suficiente aplicar la proposición **??**. Supongamos ahora que el resultado es cierto para k y consideremos el caso $k+1$. Por el Teorema 3.3.1, $\mathbb{Q}(x_1, \ldots, x_k)^G$ es un campo Hilbertiano, como el caso $k = 1$ se cumple, si $\mathbb{Q}(X)$ es una extensión de Galois de $\mathbb{Q}(x_1, \ldots, x_k)(x_{k+1}) = \mathbb{Q}(x_1, \ldots, x_k)$, entonces existe una extensión de Galois E' de $\mathbb{Q}(x_1, \ldots, x_k)$ tal que

$$Gal(\mathbb{Q}(X)|\mathbb{Q}(x_1, \ldots, x_k, x_{k+1})) \cong Gal(E'|\mathbb{Q}(x_1, \ldots, x_k)).$$

Por la hipótesis de inducción existe una extensión E'' tal que

$$Gal(E'|\mathbb{Q}(x_1, \ldots, x_k)) \cong Gal(E''|\mathbb{Q}),$$

por lo que

$$Gal(\mathbb{Q}(X)|\mathbb{Q}(x_1, \ldots, x_k, x_{k+1})) \cong Gal(E''|\mathbb{Q}).$$

Esto finaliza el paso de inducción y la prueba. ■

Observación. De los teoremas 3.3.2 y 3.3.1, concluimos que existe una construcción sistemática de extensiones de Galois sobre $\mathbb{Q}$ con grupos de Galois finitos específicos.

Veremos más adelante, que los campos Hilbertianos son herramientas fundamentales en la resolución de contextos relacionados con el problema inverso de Galois.

Capítulo 4

Problema de Noether

En 1918, Emmy Noether tuvo un enfoque para resolver el problema inverso de Galois. La encomienda de este capítulo es detallar dicho enfoque y también presentar ejemplos concretos donde permite dar una respuesta positiva al problema inverso de Galois. Así mismo, para casos donde no es posible emplear el enfoque de Noether, surge una alternativa incluida también en este capítulo.

4.1. Enfoque de Noether al problema inverso de Galois

Sea $G = \{g_1, g_2, \ldots, g_n\}$ un grupo finito. Consideremos el conjunto de $|G|$ variables indexadas por los elementos de G:

$$X = \{x_g \mid g \in G\} .$$

En particular $|X| = |G|$. Queremos incorporar al conjunto X la operación binaria de G; para esto consideramos una acción de grupos en X.

Siguiendo el enfoque de Noether, para $g \in G$ definimos

$$\begin{array}{rccc} \varphi_g : & \mathbb{Q}(X) & \longrightarrow & \mathbb{Q}(X) \\ & \dfrac{A(x_{g_1}, x_{g_2}, \ldots, x_{g_n})}{B(x_{g_1}, x_{g_2}, \ldots, x_{g_n})} & \longmapsto & \dfrac{A(x_{gg_1}, x_{gg_2}, \ldots, x_{gg_n})}{B(x_{gg_1}, x_{gg_2}, \ldots, x_{gg_n})} \end{array} .$$

el cual es un automorfismo de $\mathbb{Q}(X)$ y $\varphi_g|_{\mathbb{Q}} = id_{\mathbb{Q}}$.
Notar que la función

$$\begin{array}{rccc} * : & G \times \mathbb{Q}(X) & \longrightarrow & \mathbb{Q}(X) \\ & \left(g, \dfrac{A}{B}\right) & \longmapsto & \varphi_g \left(\dfrac{A}{B}\right) \end{array}$$

nos define $*$ una acción de G en $\mathbb{Q}(X)$, en efecto

- $e * x_{g_i} = x_{eg_i} = x_{g_i} \ \forall i = 1, \ldots, n.$
- $g_j * (g_k * x_{g_i}) = g_j * (x_{g_k g_i}) = x_{g_j(g_k g_i)} = x_{(g_j g_k) g_i} = (g_j g_k) * x g_i \quad \forall i.$

En efecto G es un acción y actúa sobre $\mathbb{Q}(X)$.

Definimos la función

$$\begin{aligned} \Phi : G &\longrightarrow Aut\left(\mathbb{Q}(X)\right) \\ g &\longmapsto \varphi_g \quad . \end{aligned}$$

Veamos que Φ es un homomorfismo. Sean $g, h \in G$,

$$\begin{aligned} \Phi(gh)\left(\frac{A}{B}\right) &= \varphi_{gh}\left(\frac{A(x_{g_1}, x_{g_2}, \ldots, x_{g_n})}{B(x_{g_1}, x_{g_2}, \ldots, x_{g_n})}\right) \\ &= \frac{A(x_{ghg_1}, x_{ghg_2}, \ldots, x_{ghg_n})}{B(x_{ghg_1}, x_{ghg_2}, \ldots, x_{ghg_n})} \\ &= \varphi_g\left(\frac{A(x_{hg_1}, x_{hg_2}, \ldots, x_{hg_n})}{B(x_{hg_1}, x_{hg_2}, \ldots, x_{hg_n})}\right) \\ &= \varphi_g\left(\varphi_h\left(\frac{A}{B}\right)\right) = \left(\varphi_g \circ \varphi_h\right)\left(\frac{A}{B}\right) \\ &= \left(\Phi(g) \circ \Phi(h)\right)\left(\frac{A}{B}\right) \quad . \end{aligned}$$

Por lo tanto, Φ es un homomorfismo y además,

$$\begin{aligned} \text{Si } \Phi(g) = Id_\Phi \quad &\Rightarrow \varphi_g = Id_\varphi \\ \Rightarrow \frac{A(x_{gg_1}, x_{gg_2}, \ldots, x_{gg_n})}{B(x_{gg_1}, x_{gg_2}, \ldots, x_{gg_n})} &= \frac{A(x_{g_1}, x_{g_2}, \ldots, x_{g_n})}{B(x_{g_1}, x_{g_2}, \ldots, x_{g_n})} \quad \forall \frac{A}{B} \\ &\Rightarrow x_{gg_i} = x_{g_i} \ \forall i \\ &\Rightarrow gg_i = g_i \ \forall i \\ &\Rightarrow g = e_G \ , \end{aligned}$$

es decir, Φ es inyectivo *i.e.*, monomorfismo. Esto nos dice que podemos ver a G como un subgrupo del grupo de automorfismos de $\mathbb{Q}(X)$ que dejan fijo a $\mathbb{Q}$, identificando cada $g \in G$ con su imagen $\Phi(g)$, obteniendo así $|G| = m$ automorfismos de $\mathbb{Q}(X)$, donde $\mathbb{Q}(X) = \mathbb{Q}(x_1, \ldots, x_n)$ es el campo de funciones racionales sobre $\mathbb{Q}$.

Supongamos que $\mathbb{Q}(X)^G|\mathbb{Q}$ es puramente trascendente con $\mathbb{Q} \subseteq \mathbb{Q}(X)^G \subseteq \mathbb{Q}(X)$, entonces por la proposición 2.2.1 $[\mathbb{Q}(X) : \mathbb{Q}(X)^G] = |Gal(\mathbb{Q}(X)|\mathbb{Q}(X)^G)| = |G| < \infty$ y entonces $\mathbb{Q}(X)|\mathbb{Q}(X)^G$ es algebraica. Consideremos la extensión $\mathbb{Q}(X)|\mathbb{Q}(X)^G$, por construcción $\mathbb{Q}(X)^G$ es el campo fijo de G, denotado como $\mathscr{F}(G)$, entonces por el apartado 4 del lema 2.2.1

$$\mathbb{Q}(X)^G = \mathscr{F}\left(Gal(\mathbb{Q}(X)|\mathbb{Q}(X)^G\right) \ .$$

Por lo tanto, $\mathbb{Q}(X)|\mathbb{Q}(X)^G$ es de Galois con grupo de Galois G.

Teorema 4.1.1 (Emmy Noether)**.** *Si G es finito y $\mathbb{Q}(X)^G|\mathbb{Q}$ es racional (puramente trascendente), entonces hay una extensión de Galois $K|\mathbb{Q}$ con grupo de Galois G.*

Demostración. Si $\mathbb{Q}(X)^G|\mathbb{Q}$ es racional, entonces $\mathbb{Q}(X)^G \cong \mathbb{Q}(w_1, w_2, \ldots, w_n)$, donde los w_i's son variables y están en $\mathbb{Q}(X)^G$. Luego, como $\mathbb{Q}(X)|\mathbb{Q}(X)^G$ es finita y separable (en característica cero).

Por la proposición 2.2.2, existe $\alpha \in \mathbb{Q}(X)$ tal que $\mathbb{Q}(X) = \mathbb{Q}(X)^G(\alpha)$ y $min(\alpha, \mathbb{Q}(X)^G) \in \mathbb{Q}[w_1, \ldots, w_n][y] \subset \mathbb{Q}(w_1, \ldots, w_n)[y]$. Consideremos A el conjunto de raíces de f en $\mathbb{Q}(X)$ con $\alpha \in A$, entonces

$$\forall a \in A \ \forall \sigma \in G = Gal(\mathbb{Q}(X)|\mathbb{Q}(X)^G), \quad \sigma(a) \in A.$$

Se sigue del lema 2.2.2 que existe $u \in \mathbb{Q}[w_1, \ldots, w_n]$ tal que para $\mathbb{Q}$, el campo de los números racionales y el homomorfismo de anillos

$$\begin{aligned} \omega_b : \mathbb{Q}[w_1, \ldots, w_n] &\to \mathbb{Q} \\ g &\mapsto g(b) = g_b \quad b \in \mathbb{Q}^n, \end{aligned}$$

con $\omega(u) = u_b \neq 0$, podemos encontrar una extensión de Galois E' de $\mathbb{Q}$ y una extensión de homomorfismo de anillos $\tilde{\omega}_b : \mathbb{Q}[y][A] \to E'$ de ω_b con la propiedad $E' = \mathbb{Q}(\alpha')$, donde $\alpha' = \tilde{\omega}_b(\alpha)$. Ahora, escribamos $f = f(w_1, \ldots, w_n, y) = \sum_{i=0}^{n} a_i(w_1, \ldots, w_n)y^i$, $a_i \in \mathbb{Q}[w_1, \ldots, w_n][y]$, entonces si definimos f' como en el lema 2.2.2

$$f'(y) = \sum_{i=0}^{n} \omega_b(a_i)y^i = \sum_{i=0}^{n} a_i(b)y^i = f_b(y),$$

por el corolario 3.3.1 $f' = f_b$ es irreducible para una infinidad de elementos $b \in \mathbb{Q}^n$ en $\mathbb{Q}[w_1, \ldots, w_n][y]$. Además, del paso 4. y 5. del lema 2.2.2 $E' = \dfrac{\mathbb{Q}[y]}{\langle f' \rangle} = \dfrac{\mathbb{Q}[y]}{\langle f_b \rangle}$ es una extensión de $\mathbb{Q}$ y es campo de descomposición de f_b. Y en consecuencia

$$G = Gal(\mathbb{Q}(X)|\mathbb{Q}(X)^G) \cong Gal(E'|\mathbb{Q})$$

para un infinito número de valores $b \in \mathbb{Q}^n$. ■

A continuación damos como primer ejemplo, un caso sencillo de solución del problema inverso de Galois usando el enfoque de Noether.

Ejemplo 1. Sea G el grupo finito de 2 elementos, $G = \{0, 1\}$, con la operación binaria adición mod 2. Siguiendo el enfoque de Noether, tenemos $X = \{x_0, x_1\}$. G contiene dos elementos, el automorfismo identidad i y el automorfismo σ. Definidos como:

$$\begin{aligned} i(x_0) = x_0, \quad i(x_1) = x_1 \ \text{ y} \\ \sigma(x_0) = x_1, \quad \sigma(x_1) = x_0. \end{aligned}$$

Para encontrar $\mathbb{Q}(X)^G$, debemos encontrar combinaciones que involucren sumas y productos de x_0 y x_1:

$$\sigma(x_0+x_1)=\sigma(x_0)+\sigma(x_1)=x_1+x_0=x_0+x_1=\sigma_1(x_0,x_1)$$
$$\sigma(x_0x_1)=\sigma(x_0)\sigma(x_1)=x_1x_0=x_0x_1=\sigma_2(x_0,x_1),$$

donde σ_1 y σ_2 son las funciones simétricas elementales Por lo anterior, $\mathbb{Q}(X)^G$ invariante puede ser escrito con polinomios en las funciones simétricas elementales, $\mathbb{Q}(X)^G=\mathbb{Q}(x_0,x_1)^{\mathbb{Z}_2}=\mathbb{Q}(\sigma_1,\sigma_2)=\mathbb{Q}(x_0+x_1,x_0x_1)$.

Para $f_1=x_0x_1$ y $f_2=x_0+x_1$, calculamos su matriz Jacobiana:

$$J=Jac_{x_0,x_1}(f_1,f_2)=\begin{bmatrix}\frac{\partial f_1}{\partial x_0} & \frac{\partial f_2}{\partial x_0}\\ \frac{\partial f_1}{\partial x_1} & \frac{\partial f_2}{\partial x_1}\end{bmatrix}=\begin{bmatrix}x_1 & 1\\ x_0 & 1\end{bmatrix},$$

mediante el método Gauss Jordan obtenemos

$$\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}\Rightarrow rango(J)=2.$$

Como estamos en característica 0, se sigue del criterio Jacobiano que el grado de trascendencia de f_1,f_2 en $\mathbb{Q}[x_0,x_1]$ es 2, entonces $\{x_0+x_1,x_0x_1\}$ son algebraicamente independientes sobre $\mathbb{Q}[w_1,w_2]$, por lo que $\mathbb{Q}(X)^G|\mathbb{Q}$ es trascendente y aplicando el Teorema 4.1.1, existe una extensión de Galois sobre $\mathbb{Q}$ con grupo G. Procederemos a encontrar una extensión que cumpla lo anterior.

Notar que por las consideraciones en el enfoque de Noether $\mathbb{Q}(x_0,x_1)|\mathbb{Q}(x_0,x_1)^G$ es de Galois con grupo G y por el análisis anterior, dicha extensión es: $\mathbb{Q}(x_0,x_1)|\mathbb{Q}(x_0+x_1,x_0x_1)$. Por la proposición 2.2.2 $\mathbb{Q}(x_0,x_1)=\mathbb{Q}(x_0+x_1,x_0x_1)(\alpha)$ para algún $\alpha\in\mathbb{Q}(x_0,x_1)$ y $f(y)=min(\alpha,\mathbb{Q}(x_0,x_1)^G)\in\mathbb{Q}[x_0+x_1,x_0x_1][y]$ irreducible. En este caso, notar que podemos tomar $\alpha=x_0$, ya que $\mathbb{Q}(x_0,x_1)=\mathbb{Q}(x_0+x_1,x_0x_1)(x_0)$ y entonces siendo así, si $f(y)=y^2-(x_0+x_1)y+x_0x_1$ y $x_0\in\mathbb{Q}(x_0,x_1)$,

$$\begin{aligned}f(x_0)&=x_0^2-(x_0+x_1)x_0+x_0x_1\\&=x_0^2-x_0^2-x_0x_1+x_0x_1\\&=0\ .\end{aligned}$$

Por tanto, x_0 es algebraico sobre $\mathbb{Q}(x_0,x_1)^G$.

Además, como $\mathbb{Q}(x_0,x_1)^G=\mathbb{Q}(w_1,w_2)$ con $w_1=x_0+x_1$ y $\omega_2=x_0x_1$, $f=f(w_1,w_2,y)=y^2-w_1y+w_2$. Por la proposición **??** para un infinito número de valores $b=(b_1,b_2)\in\mathbb{Q}^2$, $f_b(y)=f(b_1,b_2,y)=y^2-b_1y+b_2$ es irreducible en $\mathbb{Q}[y]$ y encontraremos E' con $Gal(E'|\mathbb{Q})\cong G$, tomando un campo de descomposición de f_b para un valor de b adecuado.

Tomemos $b_1=0$ y $b_2=-2\Rightarrow f_b(y)=y^2-2$ es irreducible en $\mathbb{Q}[y]$ con $\alpha=\sqrt{2}$ raíz de f_b, entonces $E'=\dfrac{\mathbb{Q}[y]}{\langle f_b\rangle}\cong\mathbb{Q}(\sqrt{2})$ es una extensión de $\mathbb{Q}$ con grupo de Galois G.

Corroborando lo anterior, $\mathbb{Q}(\sqrt{2})$ es una extensión algebraica sobre $\mathbb{Q}$. Veamos que es de Galois: $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = deg\ min(\sqrt{2}, \mathbb{Q}) = 2$. Ahora bien, determinamos el grupo de Galois de $\mathbb{Q}(\sqrt{2})|\mathbb{Q}$:

Si $\sigma \in Gal(Q(\sqrt{2})|\mathbb{Q})$ y $u \in \mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : \ a, b \in \mathbb{Q}\}$, esto es $u = a + b\sqrt{2}\ q, b \in \mathbb{Q}$

$$\Rightarrow \sigma(u) = \sigma(a + b\sqrt{2}) = \sigma(a) + \sigma(b)\sigma(\sqrt{2}) = a + b\sigma(\sqrt{2})\ .$$

Por lo que σ queda determinada si decimos el valor de $\sigma(\sqrt{2})$. Además

$$\begin{aligned}(\sqrt{2})^2 - 2 = 0 = \sigma(\sqrt{2})^2 - 2 = 0 \\ \Rightarrow\ \sigma(\sqrt{2})\ \text{ es raíz de } f \\ \Rightarrow \sigma(\sqrt{2}) = \sqrt{2}\ \text{ o }\ \sigma(\sqrt{2}) = -\sqrt{2} \Rightarrow \sigma(-\sqrt{2}) = \sqrt{2}. \\ \Rightarrow \sigma_1 = i \qquad \sigma_2(a + b\sqrt{2}) = a - b\sqrt{2}.\end{aligned}$$

$\therefore |Gal(\mathbb{Q}(\sqrt{2})|\mathbb{Q})| = 2 = [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}]$, $\mathbb{Q}(\sqrt{2})|\mathbb{Q}$ es de Galois con grupo G.

También podemos considerar otras extensiones de $\mathbb{Q}$ con grupo de Galois G, al tomar $b_1 = 0$ y $b_2 = -a$ tal que $\sqrt{a} \notin \mathbb{Q}$.

4.2. Casos desfavorables bajo el enfoque de Noether

Se puede asegurar que G es favorable para el problema inverso de Galois si el problema inverso de Galois tiene solución. Como se vio previamente uno de los casos en lo que esto ocurre es cuando se cumplen las hipótesis del Teorema de Noether. Pero si el anillo de invariantes $\mathbb{Q}(X)^G$ no es puramente trascendente no podemos aplicar el enfoque de Noether para resolver el problema. Sin embargo, esto no significa que G no pueda surgir como grupo de Galois de una extensión de $\mathbb{Q}$, por ejemplo si G es abeliano tenemos el siguiente teorema.

Teorema 4.2.1 (Kronecker-Weber)**.** *Todo grupo abeliano finito G ocurre como un grupo de Galois sobre $\mathbb{Q}$. En efecto G es realizable como el grupo de Galois de un un subcampo del campo ciclotómico $\mathbb{Q}(\xi)$, donde ξ es una raíz n-ésima de la unidad para algún número natural n.*

Por ejemplo, en el corolario 7.2 de (Lenstra, 1972) (p.321) se prueba que $\mathbb{Q}(x_1, \ldots, x_8)^{\mathbb{Z}_8}|\mathbb{Q}$ no es racional. A pesar de eso, $\mathbb{Z}_8$ es abeliano y por el Teorema de Kronecker-Weber 4.2.1, $\mathbb{Z}_8$ ocurre como grupo de Galois sobre $\mathbb{Q}$.

En efecto, sea $G = \mathbb{Z}_8$, el grupo cíclico de orden 8. Por lo dicho anteriormente, $\mathbb{Z}_8$ es respuesta afirmativa al problema inverso de Galois, más aún dicha extensión es un subcampo de un campo cilotómico de $\mathbb{Q}(\xi)$, donde ξ es una raíz n-ésima de la unidad.

Por el corolario 1.20 de (Fulton Arrufat, 2018) en (p. 11), $Gal(\mathbb{Q}(\xi)|\mathbb{Q}) \cong (\mathbb{Z}_{17}/\mathbb{Z})^* = (\mathbb{Z}_{17})^* = J$, donde ξ es una raíz décimo séptima de la unidad, así $\mathbb{Q}(\xi)|\mathbb{Q}$ es finita, por el Teorema Fundamental de la Teoría de Galois 2.1.3, existe la siguiente biyección

$$L \longrightarrow Gal(\mathbb{Q}(\xi)|L) \leq J \quad \text{para } \mathbb{Q} \subset L \subset \mathbb{Q}(\xi)$$

con inversa

$$H \longrightarrow \mathscr{F}(H) \quad \text{para } H \leq J\ .$$

Notar que $(\mathbb{Z}_{17}^*)$ es un grupo cíclico de orden 16, generado por la clase del número 10, por lo que podemos tomar $H \leq J$ con $|H| = 2$, así H es cíclico y es el único subgrupo de orden 2, esto es $H = \{id, \sigma_{16}\}$, donde σ_{16} está definido como $\sigma_{16}\left(\sum_i q_i\xi^i\right) = \sum_i q_i\xi^{16i}$, además H es generado por un elemento de orden 2, $H = \langle\sigma_{16}\rangle$, tal que $id = \sigma_{16}^2$.

Considerando $L = \mathscr{F}(H)$, tenemos que $L = \left\{\sum_{i=0}^{8}\left(q_i\xi^i + q_{17-i}\xi^{17-i}\right) : q_j \in \mathbb{Q}\right\}$ y además L y H se corresponden, se sigue del Teorema Fundamental de la Teoría de Galois que $[\mathbb{Q}(\xi) : L] = 2 = |H|$; además como H es normal, $L|\mathbb{Q}$ es de Galois y

$$Gal(L|\mathbb{Q}) \cong \frac{J}{H} \Rightarrow |Gal(L|\mathbb{Q})| = \frac{|J|}{|H|} = \frac{16}{2} = 8.$$

Más aún, J y H son cíclicos, por lo que

$$Gal(L|\mathbb{Q}) \cong \mathbb{Z}_8.$$

4.3. Casos para aplicar el Teorema de Noether.

En contraste, el Teorema de Kronecker-Weber no se puede aplicar cuando tratamos grupos no abelianos, por lo que el enfoque de Noether toma relevancia en estos casos.

Consideremos ahora $G = Q_8$, el grupo de cuaterniones de orden 8, el cual es isomorfo al subgrupo de 8 elementos $\{e, i, j, k, \overline{e}, -i, -j, -k\}$ cuya presentación en términos de generadores y relaciones es

$$Q_8 = \langle \overline{e}, i, j, k \ :\ i^2 = j^2 = k^2 = ijk = \overline{e}, (\overline{e})^2 = e\rangle$$

Nótese que $i^4 = e$ y además $ij = k$, entonces

$$Q_8 = \langle j, k\rangle.$$

Por el Teorema de Cayley, Q_8 es isomorfo a un grupo de permutaciones, si establecemos

$$\sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 4 & 5 & 6 & 7 & 8 & 1 & 2 \end{pmatrix} \quad \text{y} \quad \sigma_3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 5 & 8 & 3 & 6 & 1 & 4 & 7 \end{pmatrix},$$

todo elemento de Q_8 se puede representar como un producto finito de σ_2 y σ_3. Usaremos la siguiente nomenclatura para sus elementos:

$$\begin{array}{cccccccc} e & i & j & k & \overline{e} & -i & -j & -k \\ \sigma_8 & \sigma_1 & \sigma_2 & \sigma_3 & \sigma_7 & \sigma_4 & \sigma_5 & \sigma_6 \end{array},$$

entonces

$$Q_8 = \langle \sigma_2, \sigma_3 \rangle \subset S_8.$$

En esta presentación del grupo

$$\sigma_7 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 6 & 7 & 8 & 1 & 2 & 3 & 4 \end{pmatrix},$$

y se puede comprobar que se cumple $\sigma_i^2 = \sigma_1\sigma_2\sigma_3$ para $i = 1, 2, 3$, $\sigma_7^2 = \sigma_8$ (la identidad en S_8) y $\sigma_1 = \sigma_2\sigma_3$.

Al buscar una respuesta afirmativa al problema inverso de Galois, conseguir la primera hipótesis del problema de Noether requiere que $\mathbb{Q}(x_1, \ldots, x_8)^{Q_8}|\mathbb{Q}$ sea puramente trascendente, es decir, $\mathbb{Q}(x_1, \ldots, x_8)^{Q_8} \cong \mathbb{Q}(w_1, \ldots, w_8)$ con $w_1, \ldots, w_8$ algebraicamente independientes sobre $\mathbb{Q}$, este hecho es cierto y fue probado en (Gröbner, 1934), de modo que

$$\mathbb{Q}(x_1, \ldots, x_8)^{Q_8} = \mathbb{Q}(t_1, \ldots, t_4, a_0, \ldots, a_3),$$

donde

$$t_1 = \frac{z_4 - \sigma_2(z_4)}{z_3}, \qquad t_2 = z_4 + \sigma(z_4), \qquad t_3 = \frac{z_2}{z_3}, \qquad t_4 = \frac{z_3(2z_3z_1 - z_2)}{2z_1z_2 + z_3}$$

con $z_i \in \mathbb{Q}(y_1, \ldots, y_4)$ definidas como

$$\begin{aligned} z_1 &= \frac{y_1y_2}{y_1^2 - y_2^2} \\ z_2 &= y_1y_4 + y_2y_3 \\ z_3 &= y_1y_3 - y_2y_4 \\ z_4 &= y_1^2 + y_2^2 \end{aligned},$$

tal que $\mathbb{Q}(z_1, \ldots, z_4) = \mathbb{Q}(y_1, \ldots, y_4)^{\langle \sigma_3 \rangle}$, donde las y_i's son definidas en las variables $x_1, \ldots, x_6$ como se describe en (Gröbner, 1934). Mientras que, $a_0, \cdots, a_3 \in \mathbb{Q}(y_1, \ldots, y_8)^{\mathbb{Q}_8}$ con $\mathbb{Q}(y_1, \ldots, y_8) = \mathbb{Q}(a_0, \ldots, a_3, y_1, \ldots, y_4)$.
Por la proposición 2.2.2 $\mathbb{Q}(x_1, \ldots, x_8) = \mathbb{Q}(a_0, \ldots, a_3, t_1, \ldots, t_4)(\alpha)$ para $\alpha \in \mathbb{Q}(x_1, \ldots, x_8)$ y $f = min(\alpha, \mathbb{Q}(x_0, \ldots, x_8)^{Q_8}) \in \mathbb{Q}[a_0, \ldots, a_3, t_1, \ldots, t_4][y]$ es irreducible. Más aún, en (Gröbner, 1934) se construye un método para obtener un polinomio genérico con coeficientes en $\mathbb{Q}(a_0, \ldots, a_3, t_1, \ldots, t_4)$ cuyo campo de descomposición L cumple que $Gal(L|\mathbb{Q}) = Q_8$. Dicho polinomio es

$$f(x) = x^8 + b_1x^7 + \cdots + b_8,$$

logrado de una transformación Tschirnhaus con

$$x = a_0 + y + a_1y^2 + a_4y^4 + a_3y^6 \quad a_i \in \mathbb{Q}[a_0, \ldots, a_3, t_1, \ldots, t_4]$$

en $g(y) = 0$, donde g es de la forma

$$g(y) = y^8 - p_1y^6 + p_2y^4 - p_3y^2 + p_4,$$

donde cada p_i tiene sus coeficientes expresados en términos de $t_1, \ldots, t_4$, esto es $p_i \in \mathbb{Q}[a_0, \ldots, a_3, t_1, \ldots, t_4]$; además x_i es raíz de f. En efecto $f \in \mathbb{Q}[a_0, \ldots, a_3, t_1, \ldots, t_4][y]$, además f y g comparten el mismo campo de descomposición, por lo que al momento de calcularlo, se vuelve más fácil usar el polinomio simplificado g. El ejemplo obtenido en (Gröbner, 1934), considera los valores

$$\begin{aligned} t_1 &= -12, & a_0 &= 15 \\ t_2 &= 8, & a_1 &= -\frac{175}{4} \\ t_3 &= 1, & a_2 &= \frac{80}{3} \\ t_4 &= 144, & a_3 &= -\frac{3}{8}, \end{aligned}$$

calculando de acuerdo a lo establecido, obtuvieron

$$g(y) = y^8 - 72y^6 + 180y^4 - 144y^2 + 36, \qquad x = 15 + y - \frac{175}{4}y^2 + 36$$

y finalmente

$$f(x) = x^8 - 92x^6 - 432x^5 - 366x^4 + 864x^3 + 1180x^2 + 48x - 239.$$

Teniendo en cuenta que f y g comparten campo de descomposición, se puede comprobar que las raíces de g son $\{\pm\sqrt{v_1}, \pm\sqrt{v_2}, \pm\sqrt{v_3}, \pm\sqrt{v_4}\}$, donde

$$\begin{aligned} v_1 &= 18 + 12\sqrt{2} + 10\sqrt{3} + 7\sqrt{6}, \\ v_2 &= 18 - 12\sqrt{2} + 10\sqrt{3} - 7\sqrt{6}, \\ v_3 &= 18 + 12\sqrt{2} - 10\sqrt{3} - 7\sqrt{6}, \\ v_4 &= 18 - 12\sqrt{2} - 10\sqrt{3} + 7\sqrt{6}\ . \end{aligned}$$

Más aún, L es campo de descomposición de f, *i.e.*, $L = \mathbb{Q}\left(\pm\sqrt{v_1}, \pm\sqrt{v_2}, \pm\sqrt{v_3}, \pm\sqrt{v_4}\right)$ y al mismo tiempo $L = \mathbb{Q}\left(\pm\sqrt{v_1}\right)$, con $Gal(L|\mathbb{Q}) \cong Q_8$.

4.4. S_3

Continuando con el estudio de grupos no abelianos, es una opción ser tratados con el enfoque de Noether, sin embargo el cumplir que $\mathbb{Q}(X)|\mathbb{Q}(X)^G$ sea racional se torna difícil de probar y claro, en ocasiones no se cumple, como es el caso para $G = S_3$, el grupo de todas las permutaciones de 3 elementos, las cuales son

$$S_3 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \right\},$$

así G es finito, con orden 6, además es no abeliano. En efecto usando el Teorema de Molien (en el algoritmo 2.2.5 descrito en (Sturmfels, 2008) p. 32) se puede justificar que $\mathbb{Q}(X)|\mathbb{Q}(X)^G$ no es puramente trascendente, cuestión que impide aplicar el Teorema de Noether.

No obstante, esto no nos da respuesta a la pregunta, ¿S_3 puede ocurrir como grupo de Galois de una extensión de $\mathbb{Q}$?, no podemos asegurar que no ocurre, solo nos dice que no encontraremos respuesta afirmativa mediante el enfoque de Noether o el Teorema de Kronecker-Weber.

A pesar de esto, el corolario 4.7 de (Hungerford, 2012) p. 271 asegura que, si el discriminante de $f \in \mathbb{Q}[y]$ irreducible no es el cuadrado de un número racional, S_3 es grupo de Galois de f, esto es, si E es el campo de descomposición de f sobre $\mathbb{Q}$, $Gal(E|\mathbb{Q}) \cong S_3$.

En efecto, sean $G = S_3$ y $f(y) = y^3 + y + 1$. Por la proposición 4.8 de (Hungerford, 2012) p. 271, como $f \in \mathbb{Q}[x]$ es irreducible, es decir f es separable ($Char(\mathbb{Q}) = 0$), *i.e.*, no tiene raíces repetidas en ningún campo de descomposición, entonces

$$\Delta(f) = -4(1)^3 - 27(-1)^2 = -4 - 27 = -31 \ \Rightarrow \sqrt{-31} \notin \mathbb{Q}$$

Se sigue que que $Gal(E|\mathbb{Q}) \cong S_3$.

4.5. Grupos no finitos

Hasta ahora, este trabajo se ha inclinado en el estudio del problema inverso de Galois para grupos finitos, aunque el problema general no excluye el caso cuando no lo es.

Considerando G no finito. ¿Se podrá aplicar el Teorema de Noether? Contemplando el análisis detallado de los Teoremas de Hilbert y Noether respectivamente, se puede determinar que, mientras G actué como acción de grupo en la forma en que describe el enfoque de Noether, será posible aplicar el Teorema de Noether y esperar una respuesta afirmativa si se cumple la hipótesis de dicho teorema. Una opción, para probar la racionalidad de extensiones del tipo $\mathbb{Q}(X)|\mathbb{Q}(X)^G$ con G no finito, es el siguiente teorema

Teorema 4.5.1 (Teorema de Miyata)**.** *Sea G un subgrupo del grupo de matrices triangulares superiores invertibles de $n \times n$ y $V = K^n$ (el campo de fracciones de K en n variables). Entonces $K(x_1, \ldots, x_n)^G$ es una extensión puramente trascendente de K.*

Demostración. Una prueba de este resultado se encuentra en (Böhning, 2009). ■

Como consecuencia del Teorema de Miyata, encontramos una solución afirmativa para algunos grupos no finitos: Si K es algebraicamente cerrado y G un grupo abeliano cuyos elementos son (o pueden verse como) matrices diagonalizables, podemos aplicar el Teorema de Noether y encontrar una respuesta afirmativa al problema inverso de Galois. Un ejemplo de estos grupos a los que se encontraría solución es el conjunto de números enteros bajo la adición $(\mathbb{Z}, +)$.

Capítulo 5

Resultados

El presente capítulo expone los resultados obtenidos a partir del tratamiento elemental del problema inverso de Galois mediante el enfoque de Noether y el Teorema de Irreducibilidad de Hilbert.

5.1. Extensiones de Galois y grupos finitos

1. **Extensiones con respuesta afirmativa:**

   Se mostró que si G es un grupo actuando en el campo de funciones racionales $\mathbb{Q}(X)$ entonces el grupo de Galois de la extensión $\mathbb{Q}(X)/\mathbb{Q}(X)^G$ siempre se puede realizar como grupo de Galois de un campo numérico.

2. **Ejemplos concretos:**

   - Si $G \cong \mathbb{Z}_2$, entonces G puede ser visto como grupo de Galois de alguna extensión de $\mathbb{Q}$, la cual es de la forma $\mathbb{Q}(\sqrt{a})$, con a raíz de $f_b \in \mathbb{Q}[y]$ irreducible.
   - $\mathbb{Z}_8$ ocurre como grupo de Galois de una extensión de $\mathbb{Q}$ y no se cumplió que $\mathbb{Q}(x)^{Z_8}|\mathbb{Q}$ sea puramente trascendente.
   - Q_8 tiene respuesta afirmativa al problema inverso de Galois, como Q_8 no es abeliano no es posible aplicar el teorema de Kronecker-Weber, pero cumple las hipótesis del Teorema de Noether.

5.2. Aplicaciones del Teorema de Irreducibilidad de Hilbert

1. **Construcción de polinomios irreducibles:**

   Utilizando el Teorema de Irreducibilidad de Hilbert, se probaron propiedades de irreducibilidad para polinomios definidos sobre $\mathbb{Q}$, asegurando que estos generan extensiones de Galois con grupo de Galois predeterminados.

2. **Campos Hilbertianos:**

- Se mostró una prueba detallada de que $\mathbb{Q}$ es Hilbertiano y en consecuencia $\mathbb{Q}(x_1, \ldots, x_k)$ es Hilbertiano para todo k entero positivo.
- Siendo $\mathbb{Q}$ Hilbertiano y $\mathbb{Q}(X)^G|\mathbb{Q}$ es racional, los elementos de G pueden ser vistos como automorfismos de $\mathbb{Q}(X)^G$, entonces resulta factible encontrar mediante el Teorema de irreducibilidad de Hilbert, un polinomio irreducible f' con coeficientes en $\mathbb{Q}$ (a partir de un $f \in \mathbb{Q}[w_1, \ldots, w_n][y]$, donde $\mathbb{Q}(w_1, \ldots, w_n) \cong \mathbb{Q}(X)^G$) cuyo campo de descomposición E' es la extensión de $\mathbb{Q}$ que tiene grupo de Galois isomorfo a G. (Enfoque de Noether), por lo cual el problema inverso de Galois tiene solución positiva.

5.3. Limitaciones y desafíos

1. **Casos no resolubles:**
   - Se evidenció que hay grupos finitos que no satisfacen las condiciones de Noether, sin embargo se cuenta con otro resultado, el teorema de Kronecker-Weber, que para grupos abelianos da solución afirmativa al problema inverso de Galois.
   - $G = S_3$ es un grupo no abeliano para el cual $\mathbb{Q}(X)|\mathbb{Q}(X)^G$ no es racional, por lo que no fue posible aplicar los teorema de Noether y Kronecker–Weber, sin embargo con otros resultados se mostró que es grupo de Galois de una extensión de $\mathbb{Q}$ (el problema inverso de Galois tiene respuesta afirmativa).
   - Los métodos existentes para extender los resultados a estos grupos requieren técnicas más avanzadas, como el uso de teoría de invariantes.
2. **Dependencia del campo base:**
   - Se presentó el teorema de Miyata como opción para dar respuesta afirmativa al problema inverso de Galois general (grupos no finitos), ya que proporciona una clase de grupos que satisfacen las hipótesis del teorema de Noether.
   - La racionalidad de de $K(G)$ depende críticamente del campo base K. Aunque los resultados fueron positivos para $K = \mathbb{Q}$, persisten desafíos de campos más generales o característicos distintos de cero.

5.4. Impacto del enfoque elemental

El tratamiento elemental del problema inverso de Galois permitió:

- Facilitar la comprensión de los resultados para audiencias con conocimiento básico en teoría de campos y álgebra.
- Dar condicionas específicas y construibles para una respuesta afirmativa al problema de Galois.

- Propiciar una mejor divulgación y exposición del problema inverso de Galois a la comunidad matemática y una mayor facilidad de estudio para todo aquel que quiera explorar ese teorema u otros relacionados con él.
- Brindar ejemplos concretos que ilustran el uso práctico de los teoremas presentados.
- Identificar áreas donde los enfoques clásicos necesitan ser complementados con técnicas más modernas.

Capítulo 6

Discusión

En el presente proyecto, se analizó la definición de campo Hilbertiano y se presentó la demostración del Teorema de irreducibilidad de Hilbert, lo cual nos permitió concluir que $\mathbb{Q}$ es Hilbertiano; hecho que, como se muestra en (Coleman y Zwald, 2018), se usa para obtener distintos resultados, uno de los cuales da pie al planteamiento de Noether para dar una solución positiva al problema inverso de Galois.

Como se plantea en (Ranjbar y Ranjbar, 2015), el problema inverso de Galois se puede plantear para cualquier campo, pero nos hemos enfocado, como los autores de la bibliografía, en el problema clásico, que considera extensiones de $\mathbb{Q}$. Una solución parcial es la que proporciona el enfoque de Noether presentada en (Blue, s.f.), el cual requiere que $Q(X)^G$ sea puramente trascendente sobre $\mathbb{Q}$. Con todo el análisis recabado en este proyecto, a futuro nos gustaría abordar extensiones obtenidas de una manera distinta a la descrita en el enfoque de Noether, para contemplar grupos no incluidos en el enfoque de Noether, y desde luego, considerar la interrogante del problema inverso de Galois para otros campos K.
Algunas de las preguntas a examinar serían

- ¿Cuales serían otras técnicas que nos permitan construir extensiones de Galois de $\mathbb{Q}$ con grupo de Galois isomorfo a un grupo dado?.
- El enfoque de Noether, ¿puede usarse para otros campos Hilbertianos en el problema inverso de Galois?
- ¿Cuándo un grupo finito puede verse como grupo de Galois de una extensión de un campo? (distinto de $\mathbb{Q}$).

Capítulo 7

Conclusión y recomendaciones

El objetivo principal de esta tesis fue dar un tratamiento elemental, que permitiera la comprensión del problema inverso de Galois (general y clásico) y los resultados que lo sustentan, mismo que fue llevado a campo en los primeros tres capítulos. Dicho problema se ha ido estudiando con distintos enfoques (ramas de la matemáticas), pero hemos seguido el guiado por la teoría de campos para lograr el estudio y comprensión de la solución parcial desde el enfoque de Noether, ejemplificando soluciones afirmativas y negativas, como se exhibió en el capítulo 4.

En la búsqueda de los resultados que sustentan el problema inverso de Galois, encontramos que el teorema de irreducibilidad de Hilbert, es relevante para dar una solución positiva, su estudio nos permite determinar campos Hilbertianos, la ventaja de estos bajo el enfoque de Noether es que nos permiten encontrar la forma de la extensión buscada para $\mathbb{Q}$, como se mostró en el ejemplo para G de orden 2. El enfoque de Noether necesita que la extensión $\mathbb{Q}(X)^G/\mathbb{Q}$ sea puramente trascendente, lo cual puede llegar a ser tan complicado como encontrar solución al Problema inverso de Galois.

Otro objetivo fue, que ante estas limitantes esperadas, se pudo encontrar una alternativa para llegar a la solución, así como en el ejemplo para $G = \mathbb{Z}_8$, donde se recurrió al Teorema de Kronecker–Weber, para dar sí como respuesta al Problema inverso de Galois. Gracias a este ejemplo se concluyó que no en todos los casos puede aplicarse el Teorema de Noether, para grupos abelianos es recomendable aplicar el teorema de Kronecker–Weber, pero de manera similar, este excluye situaciones por sus hipótesis, como se mostró para $G = Q_8$ no abeliano, en el cual se resaltó la relevancia del Teorema de Noether para asegurar que tendríamos una respuesta afirmativa y después, se implementó el uso de un polinomio genérico obtenido como se describe en (Gröbner, 1934) para encontrar dicha extensión.

Aún más, vimos que es posible guiarse con el enfoque de Noether para grupos no finitos con las condiciones del Teorema de Miyata, ya que dicho resultado nos proporciona extensiones puramente trascendentes para ciertos grupos; si bien dicho resultado nos asegura de manera más directa que la extensión $\mathbb{Q}(x)^G|\mathbb{Q}$ es racional (para ciertos grupos), el encontrar cuál es la forma de $\mathbb{Q}(w_i)$ con estos w_i algebraicamente independientes, sigue siendo complicado. Más aún, en estos casos es necesario trabajar con operadores de Reynolds y la teoría de invariantes (y por supuesto el uso de un software matemático), ya que puede ser un camino

que permita encontrar dicha forma.

Como se plasmó en los ejemplos incluidos, en su mayoría no es sencillo probar las condiciones para asegurar que el problema inverso de Galois tiene respuesta positiva o encontrar dicha extensión. No obstante el problema inverso de Galois permanece sin resolver (con solución completa), hay grupos para los cuales no se ha podido probar si es respuesta positiva o negativa al problema inverso de Galois, como es el caso para $G = Q_{16}$ (el grupo de cuaterniones generalizado de orden 16), que es el grupo de orden menor para el cual no se sabe si es posible aplicar el Teorema de Noether y en consecuencia responder a la pregunta del problema inverso de Galois ((Jensen, Ledet, y Yui, 2002)); desde luego se torna más complicado en cuanto se consideran grupos de orden mayor, como es este caso. Se puede interpretar que mucho tiene que ver las propiedades del grupo a tratar, de acuerdo a (Futorny y Schwarz, 2021) en p. 13, considerando las características de K un campo algebraicamente cerrado y G soluble conexo (topológicamente), los teoremas de Lie-Kolchin y Miyata respectivamente nos aseguran la racionalidad, por lo que podríamos seguir el enfoque de Noether para obtener una respuesta afirmativa al problema inverso de Galois.

De igual manera, aterrizamos que quedan muchas cuestiones interesantes por tratar, oportunidades de extensión de este y otros trabajos pueden comenzar con las preguntas:

1. Para G un grupo finito no abeliano tal que $\mathbb{Q}(X)^G|\mathbb{Q}$ es no racional, ¿G puede verse como grupo de Galois de una extensión de $\mathbb{Q}$?

2. ¿Qué forma tienen dichas extensiones y cómo podemos obtenerlas?

Además, profundizar en el estudio del problema inverso de Galois para grupos no finitos.

Referencias

Blue, M. (s.f.). Galois theory and noether's problem.

Böhning, C. (2009). The rationality problem in invariant theory. *arXiv preprint arXiv:0904.0899*.

Coleman, R., y Zwald, L. (2018). Hilbertian fields and hilbert's irreducibility theorem. *arXiv preprint arXiv:1809.10977*.

Cox, D., Little, J., y O'Shea, D. (2018). *Ideals, varieties, and algorithms: An introduction to computational algebraic geometry and commutative algebra, corrected fourth edition.* Springer Science & Business Media, Berlin.

Fulton Arrufat, D. (2018). *The kronecker-weber theorem* (B.S. thesis). Universitat Politècnica de Catalunya.

Futorny, V., y Schwarz, J. (2021). Noether's problems. *Ensaios Matemáticos*, *37*, 1–99.

Gröbner, W. (1934). Minimalbasis der quaternionengruppe. *Monatshefte für Mathematik und Physik*, *41*, 78–84.

Hungerford, T. W. (2012). *Algebra* (Vol. 73). Springer Science & Business Media.

Jensen, C. U., Ledet, A., y Yui, N. (2002). *Generic polynomials: constructive aspects of the inverse galois problem* (Vol. 45). Cambridge University Press.

Lenstra, H. W. (1972). *Rational functions invariant under a finite abelian group.* Universiteit van Amsterdam, Mathematisch Instituut.

Morandi, P. (2012). *Field and galois theory* (Vol. 167). Springer Science & Business Media.

Ranjbar, F., y Ranjbar, S. (2015). Inverse galois problem and significant methods. *arXiv preprint arXiv:1512.08708*.

Stewart, I. (2022). *Galois theory.* Chapman and Hall/CRC.

Sturmfels, B. (2008). *Algorithms in invariant theory.* Springer Science & Business Media.

Alojamiento de la Tesis en el Repositorio Institucional	
Título de Tesis:	Un tratamiento elemental al problema inverso de Galois a través del problema de Noether
Autora:	Karen De La Cruz Ramos
ORCID	https://orcid.org/0009-0001-7798-9262
Resumen de la Tesis:	El problema inverso de Galois, planteado en los primeros años del siglo XIX examina cuándo un grupo finito G surge como grupo de Galois de una extensión de Galois de $\mathbb{Q}$, dicho problema no cuenta con solución completa. En este trabajo se procedió con un un tratamiento y análisis elemental tanto para el problema inverso de Galois como para el enfoque de Noether que permite una solución parcial, como es el caso de los ejemplos presentados. Así mismo, se expone una alternativa para algunos casos donde no es posible aplicar la solución de Noether.
Palabras claves de la Tesis:	Problema inverso de Galois, Teorema de irreducibilidad de Hilbert, Teorema de Noether, Polinomios, Extensiones.

Referencias citadas:

Blue, M. (s.f.). Galois theory and noether's problem

Böhning, C. (2009). The rationality problem in invariant theory. *arXiv preprint arXiv:0904.0899*.

Coleman, R., y Zwald, L. (2018). Hilbertian fields and hilbert's irreducibility theorem. *arXivpreprint arXiv:1809.10977*.

Cox, D., Little, J., y O'Shea, D. (2018). *Ideals, varieties, and algorithms: An introduction to computational algebraic geometry and commutative algebra, corrected fourth edition*. Springer Science & Business Media, Berlin.

Fulton Arrufat, D. (2018). *The kronecker-weber theorem* (B.S. thesis). Universitat Polit'ecnica de Catalunya.

Futorny, V., y Schwarz, J. (2021). Noether's problems. *Ensaios Matemáticos, 37,* 1–99.

Gröbner, W. (1934). Minimalbasis der quaternionengruppe. *Monatshefte für Mathematik und Physik, 41,* 78–84.

Hungerford, T. W. (2012). *Algebra* (Vol. 73). Springer Science & Business Media.

Jensen, C. U., Ledet, A., y Yui, N. (2002). *Generic polynomials: constructive aspects of the inverse galois problem* (Vol. 45). Cambridge University Press.

Lenstra, H. W. (1972). *Rational functions invariant under a finite abelian group*. Universiteitvan Amsterdam, Mathematisch Instituut.

Morandi, P. (2012). *Field and galois theory* (Vol. 167). Springer Science & Business Media.

Ranjbar, F., y Ranjbar, S. (2015). Inverse galois problem and significant methods. *arXiv preprint arXiv:1512.08708*.

Stewart, I. (2022). *Galois theory*. Chapman and Hall/CRC.

Sturmfels, B. (2008). *Algorithms in invariant theory*. Springer Science & Business Media.