



ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO
FACULTAD DE CIENCIAS
CARRERA MATEMÁTICA

**INSOLUBILIDAD DE ECUACIONES ALGEBRAICAS DE GRADO
MAYOR O IGUAL A CINCO MEDIANTE RADICALES**

Trabajo de Integración Curricular

Tipo: Proyecto de Investigación

Presentado para optar al grado académico de:

MATEMÁTICA

AUTORA: LAURA JANETH ARCENTALES NARVAEZ

DIRECTOR: Dr. LEONIDAS ANTONIO CERDA ROMERO

Riobamba – Ecuador

2024

©2024, Laura Janeth Arcentales Narvaez

Se autoriza la reproducción total o parcial, con fines académicos, por cualquier medio o procedimiento, incluyendo la cita bibliográfica del documento, siempre y cuando se reconozca el Derecho de Autor.

Yo, Laura Janeth Arcentales Narvaez, declaro que el presente Trabajo de Integración Curricular es de mi autoría y los resultados del mismo son auténticos. Los textos en el documento que provienen de otras fuentes están debidamente citados y referenciados.

Como autor asumo la responsabilidad legal y académica de los contenidos de este trabajo de titulación; el patrimonio intelectual pertenece a la Escuela Superior Politécnica de Chimborazo.

Riobamba, 13 de mayo de 2024



Laura Janeth Arcentales Narvaez

030294954-0

ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO
FACULTAD DE CIENCIAS
CARRERA MATEMÁTICA

El Tribunal del Trabajo de Integración Curricular certifica que: el Trabajo de Integración Curricular; Tipo: Proyecto de Investigación. **INSOLUBILIDAD DE ECUACIONES ALGEBRAICAS DE GRADO MAYOR O IGUAL A CINCO MEDIANTE RADICALES**, realizado por la señorita: **LAURA JANETH ARCENTALES NARVAEZ**, ha sido minuciosamente revisado por los Miembros del Tribunal del Trabajo de Integración Curricular, el mismo que cumple con los requisitos científicos, técnicos, legales, en tal virtud el Tribunal Autoriza su presentación.

	FIRMA	FECHA
Mgs. Ramón Antonio Abancín Ospina PRESIDENTE DEL TRIBUNAL		2024-05-13
Dr. Leonidas Antonio Cerda Romero DIRECTOR DEL TRABAJO DE INTEGRACIÓN CURRICULAR		2024-05-13
Mgs. Alex Eduardo Pozo Valdiviezo ASESOR DEL TRABAJO DE INTEGRACIÓN CURRICULAR		2024-05-13

DEDICATORIA

Este logro no habría sido posible sin el apoyo incondicional de cada uno de ustedes. A mis padres, Aurelia y Xavier, quienes siempre creyeron en mí y me brindaron su amor y aliento en cada paso del camino, les dedico este trabajo con profundo agradecimiento. A mis queridos hermanos, Cristian y Fabian, por el apoyo incondicional.

A mi querida abuela Laura, cuya sabiduría y amor han sido luz en mi vida, le dedico este logro con todo mi corazón. Sus consejos y palabras han sido mi guía a lo largo de esta travesía académica. A todos ustedes, mi familia, les debo más de lo que las palabras pueden expresar. Su amor, apoyo y sacrificio han sido la fuerza impulsora detrás de cada página escrita en esta tesis. Gracias por estar siempre a mi lado, por creer en mí y por ser mi mayor fuente de inspiración.

Laura

AGRADECIMIENTO

Quiero expresar mi sincero agradecimiento a todas las personas que contribuyeron de alguna manera en la realización de esta tesis. En primer lugar, agradezco a mi director de tesis, Dr. Leonidas Cerda, por su orientación experta, paciencia y dedicación a lo largo de este proceso. Sus comentarios han sido invaluable para mejorar este trabajo.

A mis docentes quienes ayudaron en mi formación como Matemática, y que aportaron con sus conocimiento para poder cumplir esta etapa en mi vida.

Quiero expresar mi gratitud a mi persona especial quien me ha acompañado en este proceso y ha sido un pilar fundamental en toda esta etapa, mis amigos, y familiares por su constante apoyo emocional y motivación durante este período. En particular, quiero agradecer a mis padres, Aurelia y Xavier, por su amor incondicional, aliento y sacrificio. Su apoyo inquebrantable ha sido mi mayor fortaleza.

Este logro no solo es mío, sino de todos aquellos que me han acompañado en este viaje académico. Gracias a todos por su invaluable ayuda y apoyo.

Laura

ÍNDICE DE CONTENIDO

ÍNDICE DE ANEXOS	ix
RESUMEN	x
ABSTRACT	xi
INTRODUCCIÓN	1
CAPÍTULO I	
2. PROBLEMA DE INVESTIGACIÓN	2
1.1. Planteamiento del problema	2
1.2. Objetivos	2
1.2.1. <i>Objetivo general</i>	2
1.2.2. <i>Objetivos específicos</i>	2
1.3. Justificación	3
CAPÍTULO II	
3. MARCO TEÓRICO	4
2.1. Referencias teóricas	4
CAPÍTULO III	
4. MARCO METODOLÓGICO	6
3.1. Descripción de enfoque, alcance, diseño, tipo, métodos, técnica e instrumentos de investigación.	6
CAPÍTULO IV	
5. MARCO DE ANÁLISIS E INTERPRETACIÓN DE RESULTADOS	8
4.1. Resultado	8
4.2. Estructura de la monografía	8

CAPÍTULO V

6. CONCLUSIONES Y RECOMENDACIONES 9

BIBLIOGRAFÍA

ANEXOS

ÍNDICE DE ANEXOS

ANEXO A: MONOGRAFÍA “INSOLUBILIDAD DE ECUACIONES ALGEBRAICAS DE GRADO MAYOR O IGUAL A CINCO POR MEDIO DE RADICALES”

RESUMEN

En la Escuela Superior Politécnica de Chimborazo no hay indicios de la presencia de información bibliográfica sobre la Teoría de Galois, aplicada a la insolubilidad de ecuaciones algebraicas de grado mayor o igual a cinco por medio de radicales, lo que impide que estudiantes interesados en el tema puedan realizar sus investigaciones. Por lo que a partir de esto, el objetivo de este trabajo es analizar la teoría de Galois, mediante la revisión de material bibliográfico especializado, para así generar una monografía sobre la insolubilidad de ecuaciones algebraicas de grado mayor o igual a cinco por medio de radicales; la cual se desarrolló mediante el uso del editor de texto \LaTeX . Para la elaboración de este se tomó en cuenta una investigación con un enfoque cualitativo, nivel descriptivo y de tipo documental. Finalmente como resultado se obtuvo una monografía titulada: Insolubilidad de ecuaciones algebraicas de grado mayor o igual a cinco por medio de radicales. La monografía se apoya en cuatro capítulos: el primer capítulo consiste en los temas de anillos y campos; el segundo capítulo trata el tema de anillos de polinomios; tercer capítulo estudia extensiones de campos y el cuarto capítulo se enfoca en la teoría de Galois, donde se abarca la demostración de la insolubilidad de las ecuaciones de grado mayor o igual a cinco por medio de radicales. Por lo tanto, a partir del análisis de la teoría de anillos y extensiones de campos se pudo determinar la demostración de la insolubilidad de ecuaciones algebraicas por medio de radicales de grado mayor o igual a cinco.

Palabras clave:<ANILLOS>, <EXTENSIONES DE CAMPOS>, <GRUPO DE GALOIS>, <SOLUBLE POR RADICALES>, <ECUACIONES ALGEBRAICAS>, <INSOLUBILIDAD>

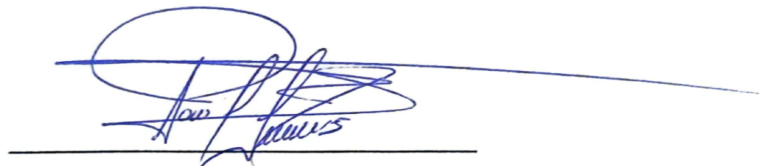
0532-DBRA-UPT-2025



ABSTRACT

The Escuela Superior Politécnica de Chimborazo does not have evidence on the existence of bibliographic information about the Galois Theory, applied to the insolubility of algebraic equations with a degree greater than or equal to five by means of radicals, this impedes students interested in the subject to carry out their research. Therefore, the aim of this research is to analyze the Galois theory, through the review of specialized bibliographic material, in order to generate a monograph on the insolubility of algebraic equations with a degree greater than or equal to five by means of radicals, which was developed using the LATEX text editor. The development of this work was based on a qualitative approach, descriptive level and documentary type research. Finally, the result was a monograph entitled: Insolubility of algebraic equations with a degree greater than or equal to five by means of radicals. The monograph has four chapters: the first chapter has to do with the study of rings and fields; the second chapter deals with the rings of polynomials topic; the third chapter studies extensions of fields and the fourth chapter focuses on the Galois theory, where the demonstration of the insolubility of equations with degree greater than or equal to five by means of radicals is covered. Therefore, from the analysis of the theory of rings and field extensions it was possible to determine the demonstration of the insolubility of algebraic equations by means of radicals with a degree greater than or equal to five.

Keywords: <RINGS>, <EXTENSIONS OF FIELDS>, <GALOIS GROUP>, <SOLVABILITY BY RADICALS>, <ALGEBRAIC EQUATIONS>, <INSOLUBILITY>.



Lic. Paul Rolando Armas Pesántez. Mgs

060328987-7

INTRODUCCIÓN

El conocimiento matemático es demasiado extenso para ser cubierto por una carrera de Matemática de pregrado. Por esta razón, muchas teorías importantes no son consideradas en sus mallas curriculares; de ahí surge la necesidad de dejar plasmada en una monografía una parte de la matemática que no haya sido estudiada en el pregrado. En efecto, en la carrera de Matemática de la Escuela Superior Politécnica de Chimborazo (ESPOCH), en las asignaturas, Álgebra abstracta I y Álgebra abstracta II, se abarca la teoría de grupos, la teoría de anillos, y una introducción muy somera a la teoría de campos.

El motivo para el desarrollo de la monografía surgió por la idea de que, la teoría de Galois es una rama de la matemática compleja y dificultosa para estudiantes con poca experiencia en teorías abstractas, pero que ha generado conceptos valiosos para el crecimiento de la matemática. Además, es una teoría usada en diferentes áreas y permite muchos avances en cada una de ellas; de hecho uno de los grandes logros de la teoría de Galois ha sido establecer la insolubilidad, por medio de radicales, de las ecuaciones algebraicas de grado mayor o igual a cinco.

El propósito de esta Trabajo de Integración Curricular fue explorar y comprender en profundidad la demostración de la insolubilidad de ecuaciones algebraicas de grado mayor o igual a cinco por medio de radicales.

La resolución de ecuaciones algebraicas ha sido un enigma a lo largo de la historia de la matemática. Por un lado, se ha logrado la resolución de ecuaciones de segundo, tercer y cuarto grado por medio de fórmulas algebraicas. Por otro lado, muchas generaciones de matemáticos han fracasado al intentar hallar una fórmula algebraica que permita la resolución de ecuaciones de grado mayor o igual a cinco; en efecto, uno de los mayores éxitos de la teoría de Galois es demostrar que tales fórmulas no existen.

Este proyecto de investigación deja como resultado una monografía, que facilite la comprensión de los estudiantes con lo que respecta a teoría de Galois aplicada a la insolubilidad de ecuaciones algebraicas. La monografía ofrece 4 capítulos, cada uno consta de conceptos básicos, lemas, ejemplos, teoremas y sus demostraciones. El primer capítulo estudia teoría de anillos, sus propiedades y mas definiciones relacionadas; el segundo capítulo trata sobre anillos de polinomios; el tercero se enfoca en lo que es extensiones de campos; estos tres capítulos facilitarán la comprensión de la teoría de Galois aplicada a la insolubilidad de ecuaciones algebraicas por medio de radicales, tema que se trata en el cuarto capítulo titulado Teoría de Galois.

CAPÍTULO I

1. PROBLEMA DE INVESTIGACIÓN

1.1. Planteamiento del problema

La teoría de Galois es una rama del álgebra abstracta que ha servido para el desarrollo de la matemática. Desde su inicio ha proporcionado diferentes métodos y conceptos que proporcionan beneficiosas e importantes aplicaciones en diversos campos de la matemática; por ejemplo, esta se utiliza para demostrar la insolubilidad, por radicales, de ecuaciones algebraicas de grado mayor o igual a cinco.

En la ESPOCH no hay evidencia de la existencia de material bibliográfico sobre teoría de Galois aplicada a la demostración de la insolubilidad de ecuaciones algebraicas, lo cual dificulta que estudiantes interesados en entender y expandir sus conocimientos matemáticos puedan iniciar sus investigaciones.

1.2. Objetivos

1.2.1. *Objetivo general*

Analizar la teoría de Galois, a través de la revisión de material bibliográfico especializado, con la finalidad de generar una monografía sobre la insolubilidad por radicales de las ecuaciones algebraicas de grado mayor o igual a cinco.

1.2.2. *Objetivos específicos*

- Examinar documentos especializados sobre la teoría de Galois, mediante estrategias eficaces para la búsqueda de información, para la comprensión de la teoría de Galois.
- Estudiar la aplicación de la teoría de Galois, a través de definiciones y la demostración de teoremas, para determinar la insolubilidad por medio de radicales de las ecuaciones algebraicas de grado mayor o igual a cinco.
- Redactar un documento sobre la insolubilidad, de las ecuaciones algebraicas de grado mayor o igual a cinco, por medio de radicales, con la utilización del editor de texto \LaTeX , para futuros usos del documento.

1.3. Justificación

En la carrera de matemática de la ESPOCH, no se estudia la Teoría de Galois como un curso regular pero, su conocimiento es importante no solo para potencializar la formación académica de los futuros matemáticos de la ESPOCH, sino también que facilitaría estudios conducentes a obtener un título de cuarto nivel.

Este Trabajo de Integración Curricular explora la teoría de Galois a través de su aplicación en la insolubilidad de ecuaciones algebraicas de grado mayor o igual a cinco por medio de radicales; ofreciendo una importante contribución a los estudiantes de la Carrera de Matemática de la ESPOCH, para que exploren y comprendan esta importante rama de la matemática.

CAPÍTULO II

2. MARCO TEÓRICO

2.1. Referencias teóricas

En el transcurso del crecimiento de hallazgos matemáticos hasta la actualidad se escribieron documentos en los que se encuentran procedimientos para la resolución de ecuaciones cuadráticas, cúbicas y de cuarto grado, las cuales son desarrolladas mediante radicales. Las ecuaciones de grado dos tienen la forma $ax^2 + bx + c = 0$, donde sus coeficientes son número reales con $a \neq 0$, fueron resueltas por la civilización babilónica. De manera similar, la resolución de las ecuaciones cúbicas por medio de radicales se le atribuye a Cardano-Tartaglia (Chavarría, 2014, pág. 42). Cardano en su obra *El Ars Magna* atribuye a Ludovico Ferrari, quien fue secretario de Cardano, el descubrimiento de la resolución por medio de radicales de las ecuaciones de grado cuatro.

A inicios del siglo XIX, el matemático noruego Abel probó que no hay ninguna fórmula para encontrar las raíces de los polinomios de grado mayor o igual a cinco en términos de sus coeficientes (Aceff y Puebla, 2016 pág. 5), Galois también contribuyó con la teoría de la resolución de ecuaciones por medio de radicales en su memoria sobre la teoría de ecuaciones, donde se describe lo que se conoce en la actualidad como grupo de Galois de una ecuación, y cómo dicho grupo influye en si una ecuación es soluble o no por radicales (Muñoz, 2016, pág. 78).

En la bibliografía hallada, se menciona que las ecuaciones de grado mayor o igual a cinco no son solubles por medio de radicales, indicando algunos de los teoremas a usar para el desarrollo de su demostración. Por ejemplo, en el libro titulado “Elementos de la teoría de cuerpos” de Labra y Suazo, se menciona un teorema que influye directamente en tal desarrollo, el cual expresa que: si el polinomio $p(x) \in F[x]$, donde F es un campo, es soluble por radicales, entonces su grupo de Galois es soluble (Labra y Suazo, 2011 pág. 119), este teorema no consta de su demostración, lo que impide el desarrollo y entendimiento de la insolubilidad de ecuaciones de grado mayor o igual a cinco.

En el documento “Teoría de Galois y ecuaciones algebraicas” de Riquelme también se afirma que el polinomio general de grado $n \geq 5$ no es soluble por radicales, pero no presenta su demostración a detalle para el entendimiento por parte de estudiantes recién iniciados en el tema, de hecho presenta la demostración de que un grupo de Galois de un polinomio es isomorfo al grupo de permutaciones S_n , pero no prueba que el grupo S_n no es soluble para $n \geq 5$, un hecho importante para la demostración de la primera afirmación (Riquelme, 2007, pág.48).

El libro “*Galois Theory*” de Ian Stewart trata el tema de solubilidad por radicales, ofreciendo

definiciones básicas y teoremas que posibiliten la demostración de que una ecuación de grado cinco no es soluble, pero su demostración no está desarrollada; además, no considera las ecuaciones de grado mayor a cinco; este hecho podría confundir a un público inexperto en el tema, creyendo que quizás las ecuaciones polinomiales de grado seis sí son solubles por medio de radicales (Stewart, 2015, pág. 176). De manera similar sucede con el libro “*Contemporary Abstract Algebra* ” de Joseph Gallian, que afirma la insolubilidad de las ecuaciones quinticas, y para apoyar este enunciado considera un polinomio de grado 5 y prueba que en esencia no es soluble por radicales (Gallian, 2015, pág. 542).

Otra referencia que trata la insolubilidad de una ecuación quintica, es el libro “Algebra Abstracta Teoría y Aplicaciones” del autor Thomas Judson, donde se asegura que la ecuación de grado cinco no es soluble, y para probar esto menciona que solo es necesario encontrar un polinomio con un grupo de Galois S_5 (Judson y Beezer, 2017, pág. 429), al igual que los libros previos ya mencionados, no proporciona su demostración y tampoco considera las ecuaciones de grado $n > 5$.

Finalmente, el libro “*Álgebra Moderna*” de Herstein es uno de los libros que ha proporcionado la demostración de los teoremas a usar para mostrar que las ecuaciones de grado mayor o igual a cinco no son solubles, pero algo que impide su entendimiento es su notación y su escritura altamente sofisticada que, lamentablemente, pueden resultar incomprensibles para estudiantes novatos en el tema (Herstein, 1980, pág. 249).

CAPÍTULO III

3. MARCO METODOLÓGICO

3.1. Descripción de enfoque, alcance, diseño, tipo, métodos, técnica e instrumentos de investigación.

Este trabajo de investigación se desarrolló con el uso de una metodología de enfoque cualitativo, dado que los temas de la monografía se detallan a través del análisis y la interpretación subjetiva del material bibliográfico seleccionado para la comprensión de la insolubilidad de las ecuaciones algebraicas.

Dicha investigación responde a un alcance descriptivo, ya que la monografía describe los aspectos más importantes de cada tema que se encuentra plasmado en cada capítulo de la misma, contenido que es relevante para el entendimiento de la teoría de Galois aplicada a la demostración de la insolubilidad de ecuaciones algebraicas..

La investigación es de tipo documental, debido al uso de material bibliográfico especializado enfocado en el tema de teoría de Galois, en su mayoría se incluyeron: libros, tesis, monografías, etc. Para el desarrollo de este documento, se siguieron los siguientes lineamientos:

- **Búsqueda de material bibliográfico:** Con el tema de investigación establecido, se procedió a indagar fuentes de información confiables, es decir, libros, tesis y monografías, en su mayoría digitales, en los cuales se considera el estudio de la teoría de Galois.
- **Seleccionar y organizar el material recolectado:** A través de una lectura selectiva de las fuentes bibliográficas recolectadas, se procedió a destacar aquellos documentos que permita el desarrollo y la interpretación de los tópicos a tratar en la monografía.
- **Redacción de la monografía:** Este documento esta dirigido a estudiantes de la carrera de matemática recién iniciados en el tema, debido a esto el documento se redactó con una estructura lógica y coherente, además de detallar de manera clara y sencilla cada uno de los tópicos, donde cada teorema consta de su demostración; también se realizan ejemplos para una mejor comprensión.
- Finalmente se realizó una revisión profunda de la monografía, permitiendo así corregir ciertos errores gramaticales y detalles de forma. Además, se verificó que las demostraciones sigan una estructura lógica, sean precisas y comprensibles, dado que la monografía esta dirigida para los estudiantes de la carrera de Matemática de la ESPOCH.

Para la escritura de dicho documento se hizo uso del editor de texto \LaTeX , debido a que nos permite desarrollar documentos que involucren fórmulas matemáticas, generando así un documento de alta calidad.

CAPÍTULO IV

4. MARCO DE ANÁLISIS E INTERPRETACIÓN DE RESULTADOS

4.1. Resultado

Este Trabajo de Integración Curricular deja como resultado una monografía que tiene como título: “Insolubilidad de ecuaciones algebraicas de grado mayor o igual a cinco por medio de radicales”. Su propósito es facilitar al lector la comprensión de conceptos básicos relacionados con la Teoría de Galois aplicada a la demostración de la insolubilidad de ecuaciones algebraicas de grado mayor o igual a cinco.

4.2. Estructura de la monografía

La monografía consta de cuatro capítulos, cada uno de ellos con sus respectivas definiciones, proposiciones, teoremas y ejemplos, los cuales permiten resaltar los aspectos importantes de cada uno de los temas.

Capítulo 1 (Anillos y Campos): En esta sección se contempla el estudio elemental vinculado a la Teoría de Anillos y Campos, los cuales fueron: anillos, subanillos, ideales, anillo cociente, campos, subcampos, campos finitos y homomorfismos de anillos.

Capítulo 2 (Anillos de Polinomios): Este capítulo abarcó el estudio de lo que es un anillo de polinomios, sus temas fueron: estructura algebraica $F[x]$, algoritmo de Euclides, máximo común divisor y polinomios irreducibles.

Capítulo 3 (Extensiones de campos): De igual manera trata el estudio de conceptos básicos de lo que es una extensión de campo, y los temas a considerar fueron: extensiones finitas y algebraicas, raíces de polinomio irreducibles, clausuras algebraicas, derivada de un polinomio y campos finitos.

Capítulo 4 (Teoría de Galois): En este capítulo se llega a estudiar lo que es un Monomorfismo, extensión de Galois, el Teorema Fundamental de la teoría de Galois, el grupo de Galois, la raíz primitiva n -ésima de la unidad, para así finalmente llegar a determinar lo que es la solubilidad por radicales, donde se da una pequeña introducción de lo que son grupos solubles y extensiones de radicales, lo que nos permitió demostrar cuando una ecuación es soluble o no por radicales.

CAPÍTULO V

5. CONCLUSIONES Y RECOMENDACIONES

Conclusiones

Al culminar este proyecto de investigación, se derivan las siguientes conclusiones:

- A partir del análisis de la teoría de Galois, mediante la revisión de material bibliográfica especializado, se logró generar una monografía sobre la insolubilidad de ecuaciones algebraicas de grado mayor o igual a cinco por medio de radicales.
- El análisis crítico de los documentos especializados sobre la teoría de Galois, permitió la comprensión de dicha teoría.
- El estudio de la Teoría de Galois aplicada a la insolubilidad de ecuaciones algebraicas de grado mayor o igual a cinco por medio de radicales, ofrece a los estudiantes la oportunidad de explorar y comprender un tema específico que no se ve en los cursos regulares de pregrado.
- La monografía, resultado de este trabajo servirá como fuente de conocimiento valioso para los estudiantes, sobre lo que es la teoría de Galois aplicada a la insolubilidad de ecuaciones algebraicas de grado mayor o igual a cinco por medio de radicales.

Recomendaciones

En lo que respecta a las recomendaciones, se proponen las siguientes:

- Debido a que la monografía “Insolubilidad de ecuaciones algebraicas de grado mayor o igual a cinco por medio de radicales”, va dirigida a los estudiantes de la carrera de matemática de la ESPOCH, se recomienda que dicho documento se encuentre al alcance de los estudiantes, permitiendo así que ellos puedan explorar y expandir sus conocimientos sobre el tema.
- Indagar nuevos problemas matemáticos donde se refleje la aplicación de la teoría de Galois, permitiendo así potencializar las capacidades para afrontar enigmas matemáticos sofisticados, además de fortalecer y ampliar sus conocimientos sobre el tema.
- Plantear la posibilidad de la realización de futuros trabajos donde se vea reflejada la aplicación de la teoría de Galois, permitiendo así explorar nuevas aplicaciones de la teoría ya mencionada.

BIBLIOGRAFÍA

1. **ACEFF, Flor & PUEBLA, Emilio.** "Teoría de Galois, un primer curso". *Publicaciones electrónicas Sociedad matemática Mexicana*, 2016, vol.14. Disponible en: http://pesmm.org.mx/Serie%20Textos_archivos/T14.pdf
2. **CHAVARRIA, Sandra.** De las ecuaciones a la teoría de grupos, algunos obstáculos epistemológicos. (Trabajo de titulación) (Pregrado). Universidad del valle, Instituto de educación y pedagogía. Cali-Colombia. 2014 [Consulta: 18 enero 2024]. Disponible en: <http://funes.uniandes.edu.co/10891/1/Chavarr%C3%ADa2014De.pdf>
3. **GARCÍA, Hugo.** Teoría de los grupos-anillos y sus aplicaciones. [en línea]. (Trabajo de titulación) (Pregrado). Universidad de San Carlos de Guatemala, Facultad de ingeniería, Escuela de Ciencias (Guatemala-Guatemala). 2014. pp 41-108. [Consulta: 2023-07-12]. Disponible en: https://ecfm.usac.edu.gt/sites/default/files/2016-09/08_0011_MA.pdf
4. **GALLIAN, Joseph.** *Contemporary Abstract Algebra* [en línea]. 9ª ed. Minnesota-USA: Cengage Learning, 2015. [Consulta: 17 abril 2023]. Disponible en: <https://github.com/dtbinh/OpenCourse/blob/master/AbstractAlgebra/Contemporary%20Abstract%20Algebra%209th%20Joseph%20A.%20Gallian.pdf>
5. **HERSTEIN, I.N.** *Álgebra Moderna* [en línea]. Ciudad de México-México: Trillas, 1980. [Consulta: 10 de abril 2023]. Disponible en: https://www.academia.edu/14931038/Algebra_Moderna_Herstein
6. **HERNANDEZ, I.; et al.** "Diofanto, Hilbert y Robinson:¿Alguna relación entre ellos?". *Números. Revista de Didáctica de las Matemáticas* [en línea], 2009, (España), vol. 70, p. 75-87. [Consulta: 17 abril 2009]. ISSN: 1887-1984. Disponible en: <http://funes.uniandes.edu.co/3501/1/Hern%C3%ADandez2009DiofantoNumeros70.pdf>
7. **JUDSON, Thomas & BEEZER, Robert.** *Algebra Abstracta Teoría y aplicaciones* [en línea]. Texas: Anual Edition 2017. [Consulta: 12 de noviembre 2023]. Disponible en: https://www.academia.edu/40352218/Algebra_Abtracta_Teor%C3%ADa_y_Aplicaciones

8. **LABRA, Alicia & SUAZO, Avelino.** *Elementos de la teoría de cuerpos* [en línea]. Chile: Jc Sáez Editor, 2011. [Consulta: 15 de marzo 2023]. Disponible en: <https://cmmedu.uchile.cl/repositorio/Instructional%20design%20%28of%20materiales%20or%20pedagogical%20models%29./Herramientas%20para%20la%20formaci%C3%B3n%20de%20profesores%20de%20matem%C3%A1tica/12%20-%20Elementos%20de%20Teor%C3%ADa%20de%20Cuerpos.pdf>
9. **MUÑOZ, Adrian.** De Las matemáticas clásicas a las matemáticas modernas y contemporáneas: El caso de la teoría de Galois como una adjunción [en línea] (Trabajo de Titulación) (Pregrado) Universidad del Valle, 2016. pp 80-99. [Consulta: 19 marzo 2023]. Disponible en: <http://funes.uniandes.edu.co/11035/1/Orozco2016de.pdf>
10. **RIQUELME, Edgardo.** "Teoría de Galois y ecuaciones algebraicas". Universidad del BÍO-BÍO, 2007. Disponible en: http://repobib.ubiobio.cl/jspui/bitstream/123456789/1996/3/Riquelme_Faundez_Edgardo.pdf
11. **RODRIGUEZ, Yanina & FRANCO, Angela.** "Paolo Ruffini y la Solubilidad de la Ecuación de Quinto Grado" *Revista Visión Antataura*, 2019,(Panamá), col. 3, no 1. Disponible en: <http://portal.amelica.org/ameli/jatsRepo/225/2251081005/html/>
12. **SANCHEZ, José.** "Historias de Matemáticas Abel y la imposibilidad de resolver la "quintica" por radicales". *Revista de Investogación Pensamient Matemátic*, 2011. Disponible en: http://www2.camino.upm.es/Departamentos/matematicas/revistapm/revista_impresa/numero_1/abel_y_la_quintica.pdf
13. **SERRES, Yolanda.** "Iniciación del aprendizaje del álgebra y sus consecuencias para la enseñanza". SAPIENS Revista Universitaria de investigación [en línea], 2011, (Venezuela) vol.12 (1), pp.122-142 [Consulta: 12 de julio 2023]. ISSN: 1317-5815. Disponible en: <https://www.redalyc.org/pdf/410/41030367007.pdf>
14. **STEWART, Ian.** *GALOIS THEORY*. 3ª ed. [en línea]. Reino Unido: Chapman & Hall/CRCR mathematics, 2015. [Consulta: 10 de abril 2023]. Disponible en: https://math.illinoisstate.edu/schebol/teaching/407-14-files/Stewart-galois_theory.pdf



ANEXOS

ANEXO A: MONOGRAFÍA “INSOLUBILIDAD DE ECUACIONES ALGEBRAICAS DE GRADO MAYOR O IGUAL A CINCO POR MEDIO DE RADICALES”



ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

INSOLUBILIDAD DE ECUACIONES ALGEBRAICAS DE GRADO MAYOR O IGUAL A CINCO POR MEDIO DE RADICALES

COMPILADO POR
LAURA ARCENTALES

RIOBAMBA, 2024

Contenidos

Introducción	1
1 Anillos y campos	2
1.1 Anillos	2
2 Anillos de polinomios	26
2.1 Estructura algebraica $F[x]$	26
2.2 Algoritmo de Euclides	31
2.3 Máximo Común Divisor	36
2.4 Polinomios irreducibles	42
3 Extensiones de campos	50
3.1 Definiciones preliminares	50
3.2 Extensiones Finitas y Algebraicas	51
3.3 Raíces de polinomios irreducibles	67
3.4 Clausuras Algebraicas	71
3.5 Derivada de un polinomio	72
3.6 Campos Finitos	76
4 Teoría de Galois	79
4.1 Introducción	80
4.2 Monomorfismo	83
4.3 Extensión de Galois	97

4.4	Teorema Fundamental de la Teoría de Galois	101
4.5	El grupo de Galois de un polinomio de Grado 3	109
4.6	El Grupo de Galois del Polinomio $x^n - 1$	113
4.7	Solubilidad por Radicales	118
4.7.1	Grupos Solubles	121
4.7.2	Extensiones radicales	126
	Bibliografía	129

Introducción

El conocimiento matemático es demasiado extenso para ser cubierto por una carrera de matemática de pregrado. Por esta razón, muchas teorías importantes no son consideradas en sus mallas curriculares; de ahí, surge la necesidad de dejar plasmada en una monografía una parte de la matemática que no haya sido estudiada en el pregrado. En efecto, en la carrera de matemática de la Escuela Superior Politécnica de Chimborazo (ESPOCH), en las asignaturas de álgebra abstracta 1 y 2, se abarca la teoría de grupos, la teoría de anillos, y una introducción muy somera a la teoría de campos.

La teoría de Galois es una rama de la matemática compleja y difícil para estudiantes con poca experiencia en teorías abstractas, pero que ha generado conceptos valiosos para el crecimiento de la matemática. Además, es una teoría usada en diferentes áreas y permite muchos avances en cada una de ellas; de hecho, uno de los grandes logros de la teoría de Galois ha sido establecer la insolubilidad, por medio de radicales, de las ecuaciones algebraicas de grado mayor o igual a cinco.

La monografía ofrece 4 capítulos, cada uno consta de conceptos básicos, lemas, ejemplos, teoremas y sus demostraciones. El primer capítulo estudia teoría de anillos, sus propiedades y más definiciones relacionadas; el segundo capítulo trata sobre anillos de polinomios; el tercero se enfoca en lo que es extensiones de campos; estos tres capítulos facilitarán la comprensión de la teoría de Galois aplicada a la insolubilidad de ecuaciones algebraicas por medio de radicales, tema que se trata en el cuarto capítulo titulado Teoría de Galois.

1

Anillos y campos

En el apasionante y abstracto mundo del álgebra, los anillos se consideran estructuras fundamentales que representan la naturaleza de las operaciones algebraicas. El presente capítulo nos sumerge en el estudio de los anillos, el cual proporciona la bases necesarias para comprender la insolubilidad de las ecuaciones algebraicas. Se tratará propiedades, operaciones y ejemplos, que nos guiarán a entender definiciones como: homomorfismo de anillos, dominios integros, campos, etc. Todas estas definiciones serán útiles en el entendimiento de temas presentes en capítulos posteriores.

1.1 Anillos

Definición 1.1

Sea A un conjunto diferente del vacío, en el cual se encuentra definidas dos operaciones, que se denotan de la siguiente manera $(+)$ como el operador suma y (\cdot) como el operador del producto. Decimos que $(A, +, \cdot)$ es un **anillo** si y sólo si:

1. $(A, +)$ es un grupo abeliano.
2. (A, \cdot) es un semigrupo.
3. **Distributiva** : $a \cdot (b + c) = a \cdot b + a \cdot c$ y $(b + c) \cdot a = b \cdot a + c \cdot a$

Ejemplo 1.1. Consideramos \mathbb{Z} el conjunto de los números enteros, probaremos que es un anillo.

Por consecuencia de teoría de grupos sabemos que el conjunto de los enteros bajo

la operación $(+)$ es un grupo abeliano, y bajo el producto (\cdot) es un semigrupo, es decir, es cerrado y cumple con ser asociativa bajo el producto. Por lo tanto, finalmente demostraremos que la operación (\cdot) sea distributiva respecto a la $(+)$:

Sea $a, b, c \in \mathbb{Z}$

$$a(b + c) = ab + ac$$

$$(b + c)a = ba + bc,$$

sabemos que ab y ac siguen perteneciendo al conjunto de \mathbb{Z} , de igual manera para ba y ca .

Nota. A partir de lo anterior podemos ver que (A, \cdot) cumple con ser asociativo y cerrado. En el caso de que exista un elemento denotado por 1, y cumpla con $1 \cdot a = a \cdot 1 = a$, se le conoce como **anillo unitario**. Luego, si $a \cdot b = b \cdot a$ para todo $a, b \in A$, se dice que es un **anillo conmutativo o abeliano**.

Definición 1.2

Sean los elementos a, b no nulos del anillo conmutativo con unidad $(A, +, \cdot)$, es un **divisor de cero** si y sólo si, $a \cdot b = 0$.

Definición 1.3

Sea $(A, +, \cdot)$ un anillo conmutativo con unidad, se dice que es un **dominio integral** si el anillo no tiene divisores de cero.

A continuación daremos un ejemplo de dominio integral.

Ejemplo 1.2. El conjunto $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$ es un dominio integral, para verificar esto, supongamos que $\mathbb{Z}[i]$ tiene divisores de cero, entonces existe $x, y \in \mathbb{Z}[i]$ definidos de la siguiente manera,

$$x = a_1 + b_1i$$

$$y = a_2 + b_2i,$$

de los cuales al menos uno de a_1, b_1 es diferente de cero, de igual manera para a_2, b_2 . Luego,

$$\begin{aligned}
 xy &= (a_1 + b_1i)(a_2 + b_2i) \\
 &= (a_1a_2 - b_1b_2) + (a_1b_2 + a_2b_1)i \\
 &= 0 + 0i \\
 &\begin{cases} a_1a_2 - b_1b_2 = 0 & (b_2) \\ a_1b_2 + a_2b_1 = 0 & (-a_2) \end{cases} \tag{1.1}
 \end{aligned}$$

Luego, resolvemos el sistema de ecuaciones obteniendo lo siguiente:

$$\begin{array}{rcl}
 a_1a_2b_2 - b_1b_2^2 & = & 0 \\
 + & & \\
 a_1a_2b_2 + a_2^2b_1 & = & 0 \\
 \hline
 -b_1(a_2^2 + b_2^2) & = & 0
 \end{array} \tag{1.2}$$

A partir de lo obtenido tenemos lo siguiente, $b_1 = 0$ ó $(a_2^2 + b_2^2) = 0$.

Considerando la primera opción, $b_1 = 0$ entonces, $a_1 \neq 0$. Por lo tanto,

$$a_1a_2 = 0$$

$$a_2 = 0$$

y

$$a_1b_2 = 0$$

$$b_2 = 0$$

Luego de esto tenemos el caso $(a_2^2 + b_2^2) = 0$, para que esto suceda, a_2 y b_2 deben ser cero. Por lo tanto, es un dominio integro.

Definición 1.4

Un campo es un anillo A conmutativo con el elemento unidad $1 \neq 0$, tal que todos los elementos no nulos de A admiten inversos multiplicativos en A , es decir,

- sea $a \in A$, con $a \neq 0$, existe $a^{-1} \in A$ tal que, $(a \cdot a^{-1}) = 1$.

Nota. Dado un campo F . De la definición de campo los grupos $(F, +)$ y (F^*, \cdot) son abelianos, donde $F^* = F - \{0\}$.

Definición 1.5

Si B un subconjunto del anillo A es un anillo bajo las mismas operaciones de producto y suma de A , entonces decimos que B es un **subanillo** de A .

Lema 1.1

El subconjunto B del anillo A es un subanillo de A , si y sólo si:

1. $0 \in B$,
2. para todo $a, b \in B : a - b \in B$,
3. para todo $a, b \in B : ab \in B$.

Demostración. \Rightarrow) Si B es un subanillo, implica que cumple con las mismas propiedades que un anillo, es decir, que $(B, +)$ es un semigrupo. Por lo tanto, $0 \in B$ y el elemento inverso de la suma existe. Luego, cumple con que (B, \cdot) es un semigrupo, por lo tanto, $a - b \in B$.

\Leftarrow)

1. Sabemos que A es un anillo, por lo que los elementos de A son conmutativos bajo la adición, y B es cerrado bajo la substracción, por teoría de grupos se tiene que, $(B, +)$ es un grupo abeliano.
2. Ya que (A, \cdot) es un semigrupo, cumple con ser asociativo. Además, $a \cdot b \in B$, entonces (B, \cdot) es un semigrupo.
3. Finalmente, ya que el anillo $(A, +, \cdot)$ cumple con que el producto es distributiva con respecto a la suma, entonces los elemento de B de igual manera cumple con la propiedad distributiva.

□

Ejemplo 1.3. Sea el anillo $(\mathbb{R}, +, \cdot)$, probaremos que $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\} \geq \mathbb{R}$.

Sean $x, y \in \mathbb{Z}[\sqrt{2}]$ definidos de la siguiente manera:

$$x = a_1 + b_1\sqrt{2}$$

$$y = a_2 + b_2\sqrt{2}$$

- Cerrado bajo la substracción,

$$\begin{aligned}x - y &= (a_1 + b_1\sqrt{2}) - (a_2 + b_2\sqrt{2}) \\ &= (a_1 - a_2) + (b_1 - b_2)\sqrt{2},\end{aligned}$$

de donde $(a_1 - a_2) \in \mathbb{Z}$, de igual manera $(b_1 - b_2) \in \mathbb{Z}$, entonces $(a_1 - a_2) + (b_1 - b_2)\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$.

- Cerrado bajo el producto,

$$\begin{aligned}x \cdot y &= (a_1 + b_1\sqrt{2})(a_2 + b_2\sqrt{2}) \\ &= a_1a_2 + 2b_1b_2 + a_2b_1\sqrt{2} + a_1b_2\sqrt{2} \\ &= (a_1a_2 + 2b_1b_2) + (a_2b_2 + a_1b_2)\sqrt{2},\end{aligned}$$

de donde $(a_1a_2 + 2b_1b_2) \in \mathbb{Z}$, y de manera similar $(a_2b_2 + a_1b_2) \in \mathbb{Z}$. Por lo tanto, $(a_1a_2 + 2b_1b_2) + (a_2b_2 + a_1b_2)\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$.

Definición 1.6

Sea I un subconjunto del anillo R , es un **ideal** si:

1. $0 \in I$,
2. $a - b \in I$: para todo $a, b \in I$,
3. para todo $a \in I$ y $r \in R$: $ar \in I$ y $ra \in I$.

Nota. Podemos darnos cuenta que todo ideal de un anillo R es un subanillo del mismo, pero no todo subanillo de R es un ideal de R .

Teorema 1.1

Sea R un anillo abeliano con elemento unidad y $a_1, \dots, a_k \in R$, entonces $I = \{a_1x_1 + \dots + a_kx_k / x_1, \dots, x_k \in R\}$ es un ideal de R . Se dice que I es el ideal de R generado por los elementos a_1, \dots, a_k , y se denota como $I = \langle a_1, \dots, a_k \rangle$.

Demostración. Para su demostración, debemos verificar que cumple con las propiedades de un ideal:

1. $0 \in I$

Ya que R es un anillo, sabemos que $0 \in R$, por lo tanto, $0 = (a_10 + \dots + a_k0)$, es decir, $0 \in I$.

2. $a - b \in I$ para todo $a, b \in I$.

Definimos $a = (a_1x_1 + \dots + a_kx_k)$ y $b = (a_1y_1 + \dots + a_ky_k)$, con $a_n, x_n, y_n \in R$, donde $n = 1, \dots, k$.

$$\begin{aligned} a - b &= (a_1x_1 + \dots + a_kx_k) - (a_1y_1 + \dots + a_ky_k) \\ &= (a_1x_1 - a_1y_1) + \dots + (a_kx_k - a_ky_k) \\ &= a_1 \underbrace{(x_1 - y_1)}_{\in R} + \dots + a_k \underbrace{(x_k - y_k)}_{\in R} \in I, \end{aligned}$$

por lo tanto, $a - b \in I$.

3. $ar \in I$ y $ra \in I$ para todo $a \in I$ y $r \in R$,

$$\begin{aligned} ar &= (a_1x_1 + \dots + a_kx_k)r \\ &= ra_1x_1 + \dots + ra_kx_k \\ &= a_1 \underbrace{(rx_1)}_{\in R} + \dots + a_k \underbrace{(rx_k)}_{\in R} \in I, \end{aligned}$$

por lo tanto, $ar \in R$. Ya que R es conmutativo $ar = ra$. Finalmente, podemos decir que I es un ideal.

□

Definición 1.7

Dado el anillo R con elemento unidad. Decimos que R es un **anillo de ideales principales**, si para cada ideal I de R existe un elemento $a \in R$ tal que, $I = \langle a \rangle = \{ax/x \in R\}$.

Lema 1.2

Sea I, J ideales de un anillo R , entonces $I + J = \{i + j \mid i \in I, j \in J\}$ es un ideal de R .

Demostración. 1. Sabemos que I y J son ideales, por lo que cumplen con ser diferente del vacío. Por lo tanto, $0 \in I$.

2. Sea $x, y \in I + J$ donde,

$$x = i_1 + j_1 : i_1 \in I, j_1 \in J,$$

$$y = i_2 + j_2 : i_2 \in I, j_2 \in J,$$

entonces verificaremos que $x - y \in I + J$,

$$\begin{aligned} x - y &= (i_1 + j_1) - (i_2 + j_2) \\ &= \underbrace{(i_1 - i_2)}_{\in I} + \underbrace{(j_1 - j_2)}_{\in J}. \end{aligned}$$

Por lo tanto, $x - y \in I + J$.

3. Sea $x \in I + J$ y $r \in R$, entonces $xr \in I + J$ y $rx \in I + J$

$$xr = (i_1 + j_1)r = i_1r + j_1r$$

$$xr = \underbrace{i_1r}_{\in I} + \underbrace{j_1r}_{\in I}.$$

Por lo tanto, $xr \in I + J$. Luego,

$$rx = r(i_1 + j_1) = ri_1 + rj_1$$

$$rx = \underbrace{ri_1}_{\in I} + \underbrace{rj_1}_{\in I},$$

de igual manera $rx \in I + J$.

□

Definición 1.8

Si el subconjunto F de un campo K , con las operaciones de suma y producto de K es un campo, entonces F es un **subcampo** de K (denotado como $F \leq K$).

Nota. Si un subconjunto F de un campo K es un subanillo de K , para que F sea un campo solo hace falta de que 1 sea un elemento en F , y que todo elemento no nulo en F admita inverso multiplicativo.

Lema 1.3

Sea K un campo y F subconjunto de K , entonces F es subcampo de K , si y sólo si:

1. $0 \in F$,
2. $a - b \in F$ y $ab \in F$, para todo $a, b \in F$,
3. $1 \in K$ es un elemento en F ,
4. para todo elemento no nulo en F el inverso multiplicativo está en F .

Demostración. \Rightarrow) F es un subcampo, lo que implica que cumple con las mismas propiedades de un campo, es decir, que F es un anillo conmutativo con el elemento unidad. $(F, +)$ cumple con ser un grupo abeliano, entonces a es elemento de F y además, el elemento inverso de la suma pertenece a F . Por lo tanto, $a - b \in F$.

Luego, (F, \cdot) es un semigrupo debido a que es cerrado bajo el producto, entonces $a \cdot b \in F$. Finalmente $1 \in F$ y F admite elementos inversos.

\Leftarrow) Sabemos que K es un campo, esto en consecuencia de que K es un anillo conmutativo y unitario, también sabemos que $0 \in F$, $a - b \in F$ y $a \cdot b \in F$, entonces F es un anillo conmutativo. Luego, $1 \in F$, entonces prueba que es un anillo unitario, por último F admite inversos multiplicativos, entonces F es un subcampo.

□

Ejemplo 1.4. Consideremos el conjunto $\mathbb{Q}[i] = \{a + bi / a, b \in \mathbb{Q}\}$, de donde i es el número complejo tal que $i^2 = -1$, a continuación probaremos que es un campo,

para esto basta demostrar que $\mathbb{Q}[i]$ es un subcampo de \mathbb{C} , para esto haremos uso del lema anterior.

1. $0 = 0 + 0i \in \mathbb{Q}[i]$.

2. Sea $x, y \in \mathbb{Q}[i]$ tal que

$$x = a_1 + b_1i | a, b \in \mathbb{Q}$$

$$y = a_2 + b_2i | a, b \in \mathbb{Q},$$

entonces

$$(a_1 + b_1i) - (a_2 + b_2i) = (a_1 - a_2) + (b_1 - b_2)i \in \mathbb{Q}[i]$$

y

$$(a_1 + b_1i)(a_2 + b_2i) = (a_1a_2 - b_1b_2) + (a_1b_2 + b_1a_2)i \in \mathbb{Q}[i].$$

3. $1 = 1 + 0i \in \mathbb{Q}[i]$.

4. Sea el elemento no nulo, $a + bi \neq 0$, con $a, b \in \mathbb{Q}$, entonces podemos decir que $a \neq 0$ ó $b \neq 0$, de donde $a^2 + b^2 > 0$.

El inverso multiplicativo de $a + bi$ es

$$(a + bi)^{-1} = \frac{(a - bi)}{(a - bi)} \frac{1}{(a + bi)} = \frac{a - bi}{(a - bi)(a + bi)} = \frac{a - bi}{a^2 + b^2},$$

de donde

$$= \frac{a}{a^2 + b^2} - \frac{b}{a^2 + b^2}i \in \mathbb{Q}(i).$$

Definición 1.9

Sea I el ideal del anillo $(R, +, \cdot)$, debido a que todo ideal I de un anillo R es un subanillo podemos decir que, $(I, +)$ es un subgrupo abeliano de $(R, +)$, de esta manera podemos definir el conjunto $R/I = \{a + I/a \in R\}$ de todas las clases laterales de I en R , por tanto $(R/I, +)$ es un grupo, donde

$$(a + I) + (b + I) = (a + b) + I,$$

para todo $a, b \in R$, para que R/I tenga la estructura de un anillo, necesitamos

definir un producto en R/I , el cual este bien definido y verifique las propiedades 3 y 4 de la definición 1.1.

$$(a + I)(b + I) = ab + I,$$

a continuación verificaremos las propiedades previamente indicadas. De esta manera decimos que el anillo $(R/I, +, \cdot)$ es el **anillo cociente** de R por I .

Consecuentemente probaremos las propiedades anteriormente mencionadas, y que el producto este bien definido.

Demostración. • Sabemos por la teoría de grupos, que el conjunto R/I es un grupo bajo la adición. Además,

$$(a + I) + (b + I) = (a + b) + I = (b + a) + I \quad \text{ya que } R \text{ es un anillo,}$$

por lo tanto, $(R/I, +)$ es un grupo conmutativo.

- Probemos que $(a + I)(b + I) = (ab) + I$ está bien definido. Es decir, debemos mostrar que

$$(a + I)(b + I) = (a' + I)(b' + I) \implies (ab) + I = (a'b') + I.$$

Sea $a + I = a' + I$ y $b + I = b' + I$, entonces $a - a' \in I$ y $b - b' \in I$. Luego, existen $s, t \in I$ tales que $a - a' = s$ y $b - b' = t$. De donde $a = a' + s$ y $b = b' + t$.

$$\begin{aligned} ab + I &= (a' + s)(b' + t) + I \\ &= a'b' + (a't + sb' + st) + I \\ &\in a'b' + I \quad \text{ya que } a't + sb' + st \in I. \end{aligned}$$

Por lo tanto, el producto esta bien definido.

- Asociatividad del producto en R/I

Probemos que el producto es asociativo. Sea $a, b, c \in R/I$ tales que $a = x + I$, $b = y + I$, $c = z + I$.

$$\begin{aligned}a(bc) &= (x + I)[(y + I)(z + I)] \\ &= (x(yz)) + I \\ &= ((xy)z) + I \\ &= (xy + I)(z + I) \\ &= [(x + I)(y + I)](z + I) \\ &= (ab)c.\end{aligned}$$

- Distributividad del producto respecto a la suma en R/I .

Caso $a(b + c) = ab + ac$.

Sea $a, b, c \in R/I$, donde $a = x + I, b = y + I, c = z + I$.

$$\begin{aligned}a(b + c) &= (x + I)[(y + I) + (z + I)] \\ &= (x + I)[(y + z) + I] \\ &= (x(y + z)) + I \\ &= (xy + xz) + I \\ &= (xy + I) + (xz + I) \\ &= (x + I)(y + I) + (x + I)(z + I) \\ &= ab + ac.\end{aligned}$$

Luego en el caso de $(b + c)a = ba + ca$ tenemos:

Sea $a, b, c \in R/I$, donde $a = x + I, b = y + I, c = z + I$.

$$\begin{aligned}(b + c)a &= [(y + I) + (z + I)](x + I) \\ &= [(y + z) + I](x + I) \\ &= ((y + z)x) + I \\ &= (yx + zx) + I \\ &= (yx + I) + (zx + I) \\ &= (y + I)(x + I) + (z + I)(x + I) \\ &= ba + ca.\end{aligned}$$

Así, R/I es un anillo.

□

Definición 1.10

Sea R un anillo y un ideal I de R con $I \neq R$ se dice que es un **ideal maximal** de R , si dado un ideal J de R tal que $I \subset J \subset R$, entonces $I = J$ ó $I = R$, es decir, no existe un ideal J de R tal que $I \subsetneq J \neq R$.

Ejemplo 1.5. Demostraremos que el ideal $\langle 2 \rangle = 2\mathbb{Z}$ de \mathbb{Z} es un ideal maximal de \mathbb{Z} .

Sea J un ideal de \mathbb{Z} tal que $2\mathbb{Z} \subset J \subset \mathbb{Z}$. Debido a que \mathbb{Z} es un anillo de ideales principales y $J \neq 0$ esto por consecuencia de que $2 \in J$, por lo tanto existe $n \in \mathbb{Z}^+$, de donde $J = n\mathbb{Z}$, y ya que $2\mathbb{Z} \subset n\mathbb{Z}$, entonces existe un $m \in \mathbb{Z}^+$ tal que $2 = nm$, de donde deducimos que $n = 2$ ó $n = 1$, en el caso de que $n = 2$, entonces $2\mathbb{Z} = J$ y si $n = 1$, entonces $J = \mathbb{Z}$. Por lo tanto, $2\mathbb{Z}$ es un ideal maximal de \mathbb{Z} .

Teorema 1.2

Sea R un anillo abeliano con elemento unidad $1 \neq 0$ e I un ideal de R . Por lo tanto, I es un ideal maximal de R , si y sólo si, R/I es un campo.

Demostración. \Rightarrow) Supongamos que I es un ideal maximal de R .

Probar que R/I es un campo.

Por la definición 1.4 de campo debemos probar que R/I es un anillo conmutativo, y admite inversos multiplicativos para elementos no nulos. Por hipótesis sabemos que R/I es conmutativo con elemento unidad $1 \neq 0$, lo que implica que $1 + I \neq 0 + I$. A continuación probaremos que $a + I \neq 0 + I$, lo que nos lleva a decir que $a \notin I$, entonces $a + I$ tiene un inverso multiplicativo en R/I .

Ahora $\langle a \rangle$ y el ideal I son ideales de R , por el Lema 1.1 $\langle a \rangle + I$ es un ideal de R . Ya que $a \notin I$ y $a = 0 + a \notin I + \langle a \rangle$, entonces $I \subsetneq I + \langle a \rangle$, por hipótesis I es un ideal maximal de R , por lo que $I + \langle a \rangle = R$.

Capítulo 1. Anillos y campos

Sabemos que el anillo R contiene al elemento unidad, es decir, $1 \in R$, por lo que existe $m \in I$ y $b \in R$ tal que, $1 = m + ab$ así,

$$1 + I = m + ab + I \in I$$

$$1 + I = ab + I.$$

Por lo tanto,

$$(a + I)(b + I) = 1 + I$$

y así, $(a + I) = (b + I)^{-1}$ demostrando que R/I admite inversos multiplicativos.

\Leftrightarrow Suponemos que R/I es un campo debemos probar que I es un ideal maximal de R .

Sea J un ideal de R tal que $I \subsetneq J \subset R$, primero probaremos que $J = R$, para esto definimos $J/I = \{j + i/j \in J\}$ es un ideal de R/I . Luego, haciendo uso de la definición 1.6 tenemos:

- Sea $s, t \in J/I$ tal que,

$$s = j_1 + I$$

$$t = j_2 + I,$$

entonces

$$s - t = (j_1 + I) - (j_2 + I) = \underbrace{(j_1 - j_2)}_{\in J} + I \in J/I.$$

- Sea $(r + I) \in R/I$,

$$(r + I)(j_1 + I) = \underbrace{rj_1}_{\in J} + \underbrace{rI + Ij_1 + I}_I \in J/I,$$

ya que $I \subsetneq J$ existe un $j \in J$ tal que $j \notin I$. Luego, $j + I \in J/I$ y $j + I \neq 0 + I$, lo que prueba que $J/I \neq 0 + I$, por hipótesis R/I es un campo, por lo tanto sus únicos ideales son $0 + I$ y R/I . Finalmente concluimos que $J/I = R/I$.

Consideremos $x \in R$, entonces existe $j \in J$ tal que $x + I = j + I$, de donde $x - j \in i \subset J$ y así, $x \in J$. Por lo tanto, $R = J$ lo que prueba que I es un ideal maximal.

□

Lema 1.4

Si p es un primo, entonces $\mathbb{Z}/p\mathbb{Z}$ es un campo con p elementos.

Demostración. Para llegar a demostrar que $\mathbb{Z}/p\mathbb{Z}$ es un campo, solo se necesita probar que $p\mathbb{Z}$ es un ideal maximal. Consideramos el ideal J de \mathbb{Z} , tal que $p\mathbb{Z} \subset J \subset \mathbb{Z}$, debido a que \mathbb{Z} es un anillo de ideales principales y claramente vemos que $J \neq 0$, por lo tanto existe un $n \in \mathbb{Z}^+$, de donde $J = n\mathbb{Z}$, además sabemos que $m\mathbb{Z} \subset n\mathbb{Z}$, entonces existe un $m \in \mathbb{Z}^+$ tal que $p = nm$, si p es un número primo, implica que p puede ser solo dividido por si mismo y por 1, entonces decimos que $n = p$ ó $n = 1$, para el primer caso $I = J$ y para el segundo caso $J = \mathbb{Z}$. Por lo tanto, $p\mathbb{Z}$ es un ideal maximal.

Ya que hemos probado que $p\mathbb{Z}$ es un ideal, aplicando el teorema anterior podemos decir que es un campo.

A continuación probaremos que $\mathbb{Z}/m\mathbb{Z} = \{a + p\mathbb{Z} / 0 \leq a < p\}$. Ahora, definimos el siguiente elemento de $\mathbb{Z}/p\mathbb{Z}$ como $b + p\mathbb{Z}$, ya que $0 \leq b < p$, entonces por el algoritmo de Euclides existen $q, r \in \mathbb{Z}$, tales que $b = pq + r$, con $0 \leq r < p$, de esta manera podemos decir que $b - r = pq \in m\mathbb{Z}$, por lo que podemos afirmar que $b + p\mathbb{Z} = r + p\mathbb{Z}$ con $0 \leq r < p$.

Finalmente demostraremos que $\mathbb{Z}/p\mathbb{Z}$ tiene p elementos. Supongamos que tenemos dos elementos $x, y \in \mathbb{Z}/p\mathbb{Z}$, de donde $x = a + p\mathbb{Z}$ y $y = c + p\mathbb{Z}$, con $0 \leq a < c < p$, tales que $x = y$, desarrollando esto tenemos lo siguiente:

$$\begin{aligned} a + p\mathbb{Z} &= c + p\mathbb{Z} \\ c - a &= p\mathbb{Z} + p\mathbb{Z} \in p\mathbb{Z}, \end{aligned}$$

lo que implica que $c - a \in p\mathbb{Z}$ y $0 < c - a < p$, por lo que llegamos a una contradicción, demostrando así, que $\mathbb{Z}/p\mathbb{Z}$ es un campo con p elementos. □

Definición 1.11

Sean los anillos A, B y sea una función $f : A \rightarrow B$ se dice que es un **homomorfismo de anillos**, si y sólo si,

1. $f(x + y) = f(x) + f(y)$ para todo $x, y \in A$
2. $f(xy) = f(x)f(y)$ para todo $x, y \in A$.

Nota. $f : A \rightarrow B$ es un homomorfismo inyectivo, si y sólo si, $\ker(f) = \{0\}$.

Definición 1.12

Sean A y B anillos.

- Si $f : A \rightarrow B$ es un homomorfismo biyectivo de anillos, denominamos a f un **isomorfismo de anillos** denotado por $A \approx B$.
- Si $f : A \rightarrow A$ es un isomorfismo de anillos, diremos que f es un **automorfismo de A** .
- Si $f : A \rightarrow B$ es un homomorfismo inyectivo de anillos, decimos que f es un **monomorfismo de anillos**.

Ejemplo 1.6. Para $n \in \mathbb{Z}$ definimos un homomorfismo de anillos

$$\phi : \mathbb{Z} \rightarrow \mathbb{Z}_n$$

$$a \longmapsto a \pmod{n}.$$

Probaremos que es un homomorfismo de anillos.

Sea $a, b \in \mathbb{Z}$,

- $\phi(a + b) = \phi(a) + \phi(b)$

$$\begin{aligned}\phi(a + b) &= (a + b) \pmod{n} \\ &= a \pmod{n} + b \pmod{n} \\ &= \phi(a) + \phi(b),\end{aligned}$$

- $\phi(ab) = \phi(a)\phi(b)$

$$\begin{aligned}\phi(ab) &= ab \pmod{n} \\ &= a \pmod{n} b \pmod{n} \\ &= \phi(a)\phi(b)\end{aligned}$$

Teorema 1.3 (Primer teorema de isomorfismo de anillos)

Sean A, B anillos, y la función $f : A \rightarrow B$ un homomorfismo de anillos, entonces los anillos A/K y $f(A)$ son isomorfos, donde $K = \text{Ker}(f)$.

Demostración. Sea $K = \text{ker}(f)$, por el primer Teorema de Isomorfia para grupos, existe un homomorfismo de grupos bien definido $\eta : A/K \rightarrow f(A)$ definido por $\eta(r + K) = f(r)$ para los grupos abelianos aditivos A y A/K . Para probar que este es un homomorfismo de anillos, solo debemos mostrar que $\eta((r + K)(s + K)) = \eta(r + K)\eta(s + K)$; pero

$$\begin{aligned}\eta((r + K)(s + K)) &= \eta(rs + K) \\ &= f(rs) \\ &= f(r)f(s) \\ &= \eta(r + K)\eta(s + K)\end{aligned}$$

□

Teorema 1.4

Sean A, B, D anillos:

- Si $\phi : A \rightarrow B$ es un isomorfismo de anillos, entonces $\phi^{-1} : B \rightarrow A$ también es un isomorfismo de anillos.
- Si $\phi : A \rightarrow B$ y $\sigma : B \rightarrow D$ son homomorfismos de anillos, entonces $\sigma \circ \phi : A \rightarrow D$ es un homomorfismo de anillos.

Demostración. • Por hipótesis tenemos que ϕ es biyectivo, es decir, que de igual manera tenemos para ϕ^{-1} es biyectivo por lo que solo falta probar que ϕ^{-1} sea un homomorfismo.

Sea $a, b \in A$ tal que $\phi(a) = x$ y $\phi(b) = y$ de donde $x, y \in B$.

- $\phi(\phi^{-1}(x + y)) = x + y$

$$\begin{aligned}x + y &= \phi(a) + \phi(b) \\ &= \phi(a + b)\end{aligned}$$

$$\phi^{-1}(x + y) = a + b$$

$$\begin{aligned}a + b &= \phi^{-1}(x) + \phi^{-1}(y) \\ &= \phi^{-1}(x + y)\end{aligned}$$

- $\phi(\phi^{-1}(xy)) = xy$

$$\begin{aligned}xy &= \phi(a)\phi(b) \\ &= \phi(ab)\end{aligned}$$

$$\phi^{-1}(xy) = ab$$

$$\begin{aligned}ab &= \phi^{-1}(x)\phi^{-1}(y) \\ &= \phi^{-1}(xy)\end{aligned}$$

Entonces $\phi^{-1} : B \rightarrow A$ es un isomorfismo.

- Sabemos que los homomorfismo $\phi : A \rightarrow B$ y $\sigma : B \rightarrow D$, entonces consideramos $\sigma(x) = r$ y $\sigma(y) = s$ con $x, y \in B$ y $r, s \in D$,

-

$$\begin{aligned}\sigma \circ \phi(a + b) &= \sigma(\phi(a + b)) \\ &= \sigma(\phi(a) + \phi(b)) \\ &= \sigma \circ \phi(a) + \sigma \circ \phi(b)\end{aligned}$$

-

$$\begin{aligned}\sigma \circ \phi(ab) &= \sigma(\phi(ab)) \\ &= \sigma(\phi(a)\phi(b)) \\ &= \sigma \circ \phi(a)\sigma \circ \phi(b).\end{aligned}$$

□

Lema 1.5

Sean D, D' dominios de integridad. Si $\phi : D \rightarrow D'$ es un monomorfismo de anillos, por lo tanto $\phi(1) = 1'$, donde $1'$ es el elemento unidad de D' .

Demostración. Sabemos por hipótesis que D, D' son dominios integros lo que implica que no tienen divisores de cero. Sabemos que $\phi(0) = 0'$ por hipótesis $\phi(1) \neq 0'$, además sabemos que ϕ es un homomorfismo, es decir, $\phi(1)\phi(1) = \phi(1 \cdot 1) = \phi(1)$, entonces $\phi(1)(\phi(1) - 1') = 0'$, y ya que D' es un dominio integro y $\phi(1) \neq 0'$, entonces $\phi(1) = 1'$. \square

Lema 1.6

Sea un subcampo K de los números complejos y sea la función $\phi : \mathbb{Z} \rightarrow K$ un monomorfismo de anillos. Entonces $\phi(x) = x$ para todo $x \in \mathbb{Z}$.

Demostración. Sabemos por el lema previo que $\phi(1) = 1$. Partiremos probando esto por inducción considerando $n \in \mathbb{Z}^+$, ahora consideramos para el caso n , entonces $\phi(n) = n$; en el caso de $n + 1$, entonces $\phi(n + 1) = \phi(n) + \phi(1) = n + 1$. Por lo tanto, hemos probado que $\phi(m) = m$ para todo $m \in \mathbb{Z}^+$. Ahora tomaremos un $n \in \mathbb{Z}^-$ entonces $\phi(-n) = -\phi(n) = -n$. Dado que $\phi(0) = 0$ concluimos que $\phi(x) = x$. \square

Corolario 1.1

Sea K un subcampo de los números complejos y $\phi : \mathbb{Q} \rightarrow K$ un monomorfismo de anillos. Entonces $\phi(x) = x$ para todo $x \in \mathbb{Q}$.

Demostración. Primero partiremos probando que $\phi_{\mathbb{Z}} : \mathbb{Z} \rightarrow K$ definido como $\phi_{\mathbb{Z}}(n) = \phi(n)$ para todo $n \in \mathbb{Z}$, entonces $\phi : \mathbb{Z} \rightarrow K$ sigue siendo un monomorfismo de anillos. Por lo tanto, $\phi(x) = x$, para todo $x \in \mathbb{Z}$. Habiendo probado esto podemos continuar la demostración para $\phi : \mathbb{Q} \rightarrow K$, ϕ es inyectiva por definición de monomorfismo, por lo que si tomamos $x \in \mathbb{Q}^* = \mathbb{Q} - \{0\}$ tenemos que $\phi(x) \in K^* = K - \{0\}$, lo que implica que $\phi : \mathbb{Q}^* \rightarrow K^*$ es un homomorfismo inyectivo de grupos. Luego, consideramos los elementos no nulos $a, b \in \mathbb{Z}$. Entonces $\phi\left(\frac{a}{b}\right) = \phi(ab^{-1}) = \phi(a)\phi(b^{-1}) = \phi(a)\phi(b)^{-1} = ab^{-1} = \frac{a}{b}$, entonces $\phi(x) = x$ tal que $x \in \mathbb{Q}$. \square

Teorema 1.5

Sea D un dominio integro, entonces existe el campo K tal que $D \subset K$.

Demostración. Consideramos D como un dominio integro, por lo que construiremos un campo K que contenga al conjunto D . Luego, el conjunto $M = \{(a, b) / a \cdot b \in D \text{ y } b \neq 0\}$ y \sim una relación de equivalencia definida como, $(a, b) \sim (c, d)$ si y sólo si $ab = cd$ sobre M , por lo que existe la clase de equivalencia $[(a, b)] = \{(x, y) \in M / (x, y) \sim (a, b)\}$, para todo $(a, b) \in M$. Como es sabido, las clases de equivalencia forma una partición del conjunto M . Sea K el conjunto de todas las clases de equivalencia $[(a, b)]$, con $a, b \in D$ y $b \neq 0$. Sabemos que para que K sea un campo debe incluirse las operaciones suma (+) y el producto (\cdot), de donde las definimos como:

$$[(a, b)] + [(c, d)] = [(ad + bc, bd)]$$

$$[(a, b)][(c, d)] = [(ab, bd)].$$

Suponemos que

$$[(a, b)] = [(a', b')] \Rightarrow ab' = ba'$$

$$[(c, d)] = [(c', d')] \Rightarrow cd' = dc'$$

luego multiplicamos dd' y bb' respectivamemnete, entonces

$$dd'ab' = dd'ba'$$

$$bb'cd' = bb'dc'$$

al sumar esto tenemos,

$$dd'ab + bb'cd' = dd'ba' + bb'dc$$

$$(ad + bc)b'd' = (a'd' + b'c')bd,$$

lo que implica que,

$$[(ad + bc), bd] = [(a'd' + b'c'), b'd']$$

verificando así, que la suma esta bien definida.

Ahora demostraremos de manera similar para el producto

$$[(a, b)] = [(a', b')] \Rightarrow ab' = ba'$$

$$[(c, d)] = [(c', d')] \Rightarrow cd' = dc'$$

multiplicando tenemos

$$ab'cd' = ba'dc'$$

$$acb'd' = a'c'bd$$

$$[(ac, bd)] = [a'c', b'd'],$$

de esta manera probamos que en K el producto también está bien definido.

Probamos ahora que K es un campo, para esto debemos empezar con:

- $(K, +)$ es un grupo abeliano.

- Sea $x = [a, b]$; $y = [c, d]$ y $z = [e, f]$

$$\begin{aligned} x + (y + z) &= [a, b] + ([c, d] + [e, f]) \\ &= [a, b] + [cf + de, df] \\ &= [adf + bcf + bde, bdf] \\ &= [ad + bc, bd] + [e, f] \\ &= ([a, b] + [c, d]) + [e, f]. \end{aligned}$$

- Sea $x = [a, b]$; $y = [c, d]$

$$\begin{aligned} x + y &= [a, b] + [c, d] \\ &= [ad + bc, bd] \\ &= [da + cb, db] \\ &= [cb + ad, db] \\ &= [c, d] + [a, b]. \end{aligned}$$

- $[a, b] + [0, 1] = [a \cdot 1 + b \cdot 0, b \cdot 1] = [a, b]$, entonces $[0, 1]$ es el elemento neutro.

- Como $[a, b] + [-a, b] = [ab + b(-a), b^2] = [0, b^2] = [0, 1]$.

- (K, \cdot) es un semigrupo con identidad.

- Asociativa bajo el producto

$$\begin{aligned}x \cdot (y \cdot z) &= [a, b]([c, d] \cdot [e, f]) \\ &= [a, b] \cdot [ce, df] \\ &= [ace, bdf] \\ &= [ac, bd] \cdot [e, f] \\ &= (x \cdot y) \cdot z.\end{aligned}$$

- Conmutativa bajo la adición

$$\begin{aligned}x \cdot y &= [a, b] \cdot [c, d] \\ &= [ac, bd] \\ &= [ca, db] \\ &= [c, d] \cdot [a, b].\end{aligned}$$

- Como $[a, b] \cdot [1, 1] = [a, b] \Rightarrow [1, 1]$ es el elemento identidad.

- Sea $a, b \in D$

$$\begin{aligned}[a, b][b, a] &= [ab, ba] \\ &= [1, 1].\end{aligned}$$

- Distributiva

$$\begin{aligned}x \cdot (y + z) &= [a, b] \cdot [cf + de, df] \\ &= [acf + ade, bdf] \\ &= [ac, bd] + [ae, df] \\ &= [abcf + abde, b^2df] \\ &= [b(acf, ade), b(bdf)] \\ &= [acf + ade, bdf].\end{aligned}$$

Finalmente denotaremos $[(a, b)] = \frac{a}{b}$ obteniendo así el campo $K = \{\frac{a}{b} / a, b \in D \text{ y } b \neq 0\}$, de tal manera que si tomamos dos elementos de K lo denotaremos como $\frac{a}{b}, \frac{c}{d} \in K$, entonces

$$\frac{a}{b} + \frac{c}{d} = [(a, b)] + [(c, d)] = [(ad + bc, bd)] = \frac{ad + bc}{bd}$$

$$\frac{a}{b} \cdot \frac{c}{d} = [(a, b)][(c, d)] = [(ac, bd)] = \frac{ac}{bd}.$$

De esta manera podemos observar que la función $h : D \rightarrow K$ definida como $h(a) = \frac{a}{1}$ para cualquier $a \in D$ es un monomorfismo de anillos. Ya que $a \in D$ con $h(a) = \frac{a}{1} \in K$ y escribir $a = \frac{a}{1}$. Por lo tanto, $D \subset K$.

Observación 1.1. El campo K construido a partir del dominio integro D , se le denomina **campo de fracciones del dominio integro** D . Además, resulta que K es el campo mas pequeño que contiene a D , lo que implica que si F es un campo que contiene a D , entonces $K \subset F$.

□

Lema 1.7

Si F es un subcampo de \mathbb{C} , entonces $\mathbb{Q} \subset F$.

Demostración. Por hipótesis sabemos que F es un subcampo de \mathbb{C} lo que implica que contiene a los elementos 0 y 1. De esta manera $1 + 1 \in F$ y por inducción $n \in F$ para todo $n \in \mathbb{Z}^+$. Luego, para $n \in \mathbb{Z}^+$, $-n \in F$ y finalmente $\mathbb{Z} \subset F$ y por la observación antes mencionada, el campo de fracciones de \mathbb{Z} está contenida en F , entonces $\mathbb{Q} \subset F$.

□

Definición 1.13

Sea R un anillo con unidad 1 y sea $n \in \mathbb{Z}^+$, denotaremos $n \cdot 1$ como n sumandos, es decir, $1 + 1 + 1 + 1 + \dots + 1 \in R$, y denotaremos a $(-n)$ sumandos como $(-1) + (-1) + \dots + (-1) = (-n) \cdot (1)$ y $0_{\mathbb{Z}} \cdot 1 = 0$. El menor entero positivo n en el caso de existir tal que $n \cdot 1 = 0$, se dice que es la **característica del anillo** R , en el caso de no existir se dice que la característica de R es cero.

Ejemplo 1.7. Los anillos $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ tienen característica cero y el anillo \mathbb{Z}_n tiene característica n .

Teorema 1.6

Sea K un campo

- Si la característica de K es $n > 1$, entonces $n = p$ es un número primo y K contiene un subcampo isomorfo a $\mathbb{Z}/p\mathbb{Z}$.
- Si la característica de K es $n = 0$, entonces K contiene un subcampo isomorfo a \mathbb{Q} y luego K es infinito.
- Si K es un conjunto finito, entonces $\text{char}(K) = p$ con p primo y luego, K contiene un subcampo isomorfo a $\mathbb{Z}/p\mathbb{Z}$.

Demostración. a) Supongamos que la característica de K es $n > 1$. Definimos la función ϕ como $\phi(m) = m \cdot 1_K$ para todo $m \in \mathbb{Z}$. Dado que $\phi(n) = n \cdot 1_K = 0$, entonces $\text{Ker}(\phi) \neq 0$. Debido a que $\text{Ker}(\phi)$ es un ideal de \mathbb{Z} y \mathbb{Z} es un anillo de ideales principales, existe $n_0 \in \mathbb{Z}^+$ tal que $\text{Ker}(\phi) = n_0\mathbb{Z}$. Como $\phi(n_0) = n_0 \cdot 1_K = 0$ y n es el menor entero positivo tal que $n \cdot 1_K = 0$, entonces $n \leq n_0$. Como $n \in \text{Ker}(\phi) = n_0\mathbb{Z}$, entonces $n_0 \leq n$. Por lo tanto, $n = n_0$. Utilizando el primer teorema de isomorfismo de anillos, $\mathbb{Z}/n\mathbb{Z}$ y $\phi(\mathbb{Z})$ son anillos isomorfos. Pero $\phi(\mathbb{Z})$ es un subanillo del campo K , y luego, no existen divisores del cero en $\phi(\mathbb{Z})$. Concluimos que necesariamente $n = p$ es un número primo.

b) Si la característica de K es cero, entonces $\text{Ker}(\phi) = 0$. En efecto, si suponemos que $\text{ker}(\phi) \neq 0$, entonces existe $m \in \mathbb{Z}^+$ tal que $\phi(m) = 0$, lo que contradice nuestra hipótesis. Así, $\phi : \mathbb{Z} \rightarrow K$ es inyectiva y, por lo tanto, existe un subanillo $\phi(\mathbb{Z})$ contenido en K , el cual resulta ser isomorfo a \mathbb{Z} . Los campos de fracciones de \mathbb{Z} y de $\phi(\mathbb{Z})$ son isomorfos. De acuerdo con la observación ??, el campo de fracciones de $\phi(\mathbb{Z})$ está contenido en el campo K .

c) Si K tiene m elementos, entonces $(K, +)$ es un grupo finito con m elementos. Por la teoría de grupos, tenemos que, para $a \in K$, $m \cdot a = 0$ (donde $m \cdot a$ denota la suma repetida $a + a + \dots + a$), y, por lo tanto, $m \cdot 1_K = 0$. Existe un menor

entero positivo p tal que $p \cdot 1_K = 0$, que es la característica de K . Por el ítem (a), p es un número primo y K contiene un subcampo isomorfo a $\mathbb{Z}/p\mathbb{Z}$.

□

Definición 1.14

Un campo con un número finito de elementos se le denomina **campo finito** se le denota como F_q a un campo finito con q elementos.

Observación 1.2. Los campos $\mathbb{Z}/p\mathbb{Z}$ y \mathbb{Z} resultan ser iguales, es decir, si $a \in \mathbb{Z}$, entonces

$$\bar{a} = \{x \in \mathbb{Z}/x \equiv a \pmod{p}\} = \{a + pt/t \in \mathbb{Z}\} = a + p\mathbb{Z}$$

Teorema 1.7

Si p es un número primo y $a \in \mathbb{Z}$ tal que $p \nmid a$, entonces $a^{p-1} \equiv 1 \pmod{p}$.

Demostración. Ya que \mathbb{Z}_p es un campo con p elementos, entonces (\mathbb{Z}_p^*, \cdot) es un grupo con $p - 1$ elementos, donde $\mathbb{Z}_p^* = \mathbb{Z}_p - \{\bar{0}\}$. Dado que $\bar{a} \in \mathbb{Z}_p$ y $p \nmid a$, entonces $\bar{a} \in \mathbb{Z}_p^*$. Luego, $\bar{a}^{p-1} = a^{p-1} \equiv 1 \pmod{p}$. □

Teorema 1.8

Sea p primo $\mathbb{Z}_p = \{0, 1, \dots, p - 1\}$ es un dominio íntegro.

Demostración. Sabemos que \mathbb{Z}_p es un anillo conmutativo y unitario, por lo que falta probar que $(\mathbb{Z}_p, +, \cdot)$ no tiene divisores de cero.

Sean $[a], [b] \in \mathbb{Z}_p$

$$[a][b] = [0]$$

$$[ab] = [0]$$

$$[ab] = 0 \pmod{p}$$

lo que implica que $p|ab$ entonces por el Lema de Euclides $p|a$ ó $p|b$, es decir $a \equiv 0 \pmod{p}$ ó $b \equiv 0 \pmod{p}$, es decir, $[a] = [0]$ ó $[b] = [0]$. □

Teorema 1.9

Todo campo F es un dominio integro.

Demostración. Al ser F un anillo, entonces F es un anillo conmutativo y unitario, por lo que falta probar que no tiene divisores de cero, y que al tener los elementos $a, b \in F$ con $a \neq 0$ tal que $ab = 0$, entonces $b = 0$.

$$\begin{aligned} ab &= 0 \\ aa^{-1}b &= 0a^{-1} \\ 1b &= 0 \\ b &= 0 \end{aligned}$$

ya que $b = 0$, entonces contradice la definición de divisor de cero. \square

2

Anillos de polinomios

Este capítulo profundiza en la importante sección de anillos de polinomios. Aquí exploramos cómo los polinomios (objetos comunes en matemáticas elementales) pueden formalizarse y manipularse como elementos de anillos. Es decir, se dedica a un estudio en profundidad del tema anillos de polinomios, un espacio matemático donde las herramientas algebraicas encuentran sus expresiones más importantes y diversas. Estudiaremos la factorización de polinomios, la división de polinomios y las propiedades que hacen que los anillos polinomiales sean una parte importante de nuestro estudio de la insolubilidad de ecuaciones algebraicas.

2.1 Estructura algebraica $F[x]$

Definición 2.1

Sea F un campo. Una expresión de la forma $\sum_{i=0}^n a_i x^i = a_0 + a_1 x + \dots + a_n x^n$, donde $n \in \mathbb{Z}^+$ y a_0, a_1, \dots, a_n son elementos de F , a esto se le conoce como un **polinomio con coeficientes en F** en la indeterminada x .

Nota. Al conjunto formado por todos los polinomios con coeficientes en el campo F se lo denota como, $F[x]$, y sus elementos se lo denotan como $f(x), g(x), \dots, etc.$

Definición 2.2

Sean $f(x) = \sum_{i=0}^n a_i x^i$ y $g(x) = \sum_{i=0}^n b_i x^i$, donde $f(x), g(x) \in F[x]$

- $f(x) = g(x)$ si y sólo si, $a_i = b_i$ para cada $i \geq 0$.
- Definimos $(f + g)(x) = \sum_{i=0}^n (a_i + b_i) x^i$. Entonces $(f + g)(x) \in F[x]$.

Definición 2.3

Sean $f(x) = \sum_{i=0}^n a_i x^i$ y $g(x) = \sum_{i=0}^m b_i x^i$ elementos en $F[x]$. Definimos $(f \cdot g)(x) = \sum_{i=0}^{n+m} c_i x^i$, donde $c_k = \sum_{i=0}^k a_i b_{k-i}$. Entonces $f \cdot g(x)$ es elemento de $F[x]$.

Nota. • $(f + g)(x) = f(x) + g(x)$

• $(f \cdot g)(x) = f(x)g(x)$

Lema 2.1

El conjunto $F[x]$ es un anillo conmutativo con elemento unidad bajo las operaciones de suma y producto de polinomios, definidas anteriormente.

Demostración. Sea $f(x), g(x), h(x) \in F[x]$, para probar que es un anillo conmutativo vamos a empezar probando que:

• $(F[x], +)$ sea un grupo abeliano.

• Asociativa Sea $f(x), g(x), h(x) \in F[x]$ con $n \leq m \leq k$

$$\begin{aligned}
 f(x) + (g(x) + h(x)) &= \sum_{i=0}^n a_i x^i + \left(\sum_{i=0}^m b_i x^i + \sum_{i=0}^k c_i x^i \right) \\
 &= \left(\sum_{i=0}^n a_i x^i + \sum_{i=0}^m b_i x^i \right) + \sum_{i=0}^k c_i x^i \\
 &= \sum_{i=0}^m (a_i + b_i) x^i + \sum_{i=0}^k c_i x^i \\
 &= \sum_{i=0}^k (a_i + b_i + c_i) x^i \\
 &= \sum_{i=0}^n a_i x^i + \sum_{i=0}^k (b_i + c_i) x^i \\
 &= \sum_{i=0}^n a_i x^i + \left(\sum_{i=0}^m b_i x^i + \sum_{i=0}^k c_i x^i \right) \\
 &= (f(x) + g(x)) + h(x).
 \end{aligned}$$

- Elemento neutro: Para todo $f(x) \in F[x]$ existe $0(x) \in F[x]$,

$$\begin{aligned}
 f(x) + 0(x) &= 0(x) + f(x) = f(x) \\
 0(x) + f(x) &= f(x) \\
 &= \sum_{i=0}^n 0x^i + \sum_{i=0}^n a_i x^i \\
 &= \sum_{i=0}^n (0 + a_i) x^i \\
 &= \sum_{i=0}^n a_i x^i.
 \end{aligned}$$

- Elemento inverso: Para todo $f(x) \in F[x]$ existe $-f(x) \in F[x]$,

$$\begin{aligned}
 f(x) + (-f(x)) &= 0(x) \\
 &= \sum_{i=0}^n a_i x^i + \sum_{i=0}^n -a_i x^i \\
 &= \sum_{i=0}^n (a_i - a_i) x^i \\
 &= \sum_{i=0}^n 0 x^i = 0^n(0) x^i \\
 &= 0(x).
 \end{aligned}$$

- Conmutativa: $f(x) + g(x) = g(x) + f(x)$,

$$\begin{aligned}
 f(x) + g(x) &= \sum_{i=0}^n a_i x^i + \sum_{i=0}^m b_i x^i \\
 &= \sum_{i=0}^m (a_i + b_i) x^i \\
 &= \sum_{i=0}^m (b_i + a_i) x^i \\
 &= \sum_{i=0}^m b_i x^i + \sum_{i=0}^n a_i x^i.
 \end{aligned}$$

- $(F[x], \cdot)$ sea un semigrupo.

- Asociativa

$$\begin{aligned}
 (f(x)g(x))h(x) &= \left(\sum_{i=0}^n a_i x^i \sum_{i=0}^m b_i x^i \right) \sum_{i=0}^p c_i x^i \\
 &= \sum_{i=0}^{n+m} \left(\sum_{j=0}^i a_j b_{i-j} \right) x^i \sum_{i=0}^p c_i x^i \\
 &= \sum_{i=0}^{n+m+p} \left(\sum_{k=0}^i \sum_{j=0}^k a_j b_{k-j} c_{i-k} \right) x^i \\
 &= \sum_{i=0}^{n+m+p} \left(\sum_{k=0}^i \sum_{j=0}^{i-k} a_j b_{i-k-j} c_k \right) x^i \\
 &= \sum_{i=0}^{n+m+p} \left(\sum_{k=0}^i \sum_{j=0}^{i-k} a_k b_{i-k-j} c_j \right) x^i \\
 &= \sum_{i=0}^{n+m+p} \left(\sum_{k=0}^i a_k \sum_{j=0}^{i-k} b_j c_{i-k-j} \right) x^i \\
 &= \sum_{i=0}^n a_i x^i \left(\sum_{i=0}^{m+p} \sum_{j=0}^i b_j c_{k-j} \right) x^i \\
 &= \sum_{i=0}^n a_i x^i \left(\sum_{i=0}^m b_i x^i \sum_{i=0}^p c_i x^i \right).
 \end{aligned}$$

- Conmutativa

$$\begin{aligned}
 f(x)g(x) &= \sum_{i=0}^n a_i x^i \sum_{i=0}^m b_i x^i \\
 &= \sum_{i=0}^{n+m} \left(\sum_{j=0}^i a_j b_{i-j} \right) x^i \\
 &= \sum_{i=0}^{n+m} \left(\sum_{j=0}^i a_{i-j} b_j \right) x^i \\
 &= \sum_{i=0}^{m+n} \left(\sum_{j=0}^i a_{i-j} b_j \right) x^i \\
 &= \sum_{i=0}^m b_i x^i \sum_{i=0}^n a_i x^i.
 \end{aligned}$$

□

Definición 2.4

Sea $f(x) = \sum_{i=0}^n a_i x^i$ elemento de $F[x]$, con $a_n \neq 0$, entonces diremos que n es el grado de $f(x)$. Denotaremos $n = \deg(f)$ ó $n = \deg(f(x))$.

Observación 2.1. Sea $f(x) \in F[x]$ se tiene la equivalencia:

$$f(x) \neq 0 \Leftrightarrow \deg(f(x)) \geq 0.$$

Los polinomios de grado cero en $F[x]$ son los elementos no nulos del campo F .

Teorema 2.1

Sean $f(x), h(x)$ elementos distintos de cero en $F[x]$, entonces

$$\deg(f(x)h(x)) = \deg(f(x)) + \deg(h(x)).$$

Demostración. Sabemos que

$$f(x) = \sum_{i=0}^n a_i x^i$$

$$h(x) = \sum_{i=0}^m b_i x^i,$$

con $a_n \neq 0$ y $b_m \neq 0$ por definición de producto sabemos que

$$\begin{aligned} (f \cdot h)(x) &= \sum_{i=0}^{n+m} c_i x^i \\ &= c_0 + c_1 x + \dots + c_{n+m} x^{n+m}, \end{aligned}$$

donde $c_{n+m} = a_n b_m \neq 0$, entonces $\deg(f(x)h(x)) = \deg(f(x)) + \deg(h(x))$. \square

Corolario 2.1

El anillo $F[x]$ no tiene divisores de cero, entonces $F[x]$ es un dominio de integridad.

Demostración. Al ser divisores de cero significa que tomamos dos elementos no nulos, es decir, $f(x) \neq 0$ y $h(x) \neq 0$, entonces $f(x)h(x) \neq 0$. Por el Teorema 2.1 tenemos que $\deg(f(x)h(x)) = \deg(f(x)) + \deg(h(x)) \geq 0$, luego $\deg(f(x)h(x)) \geq 0$ así $f(x)h(x) \neq 0$. \square

Observación 2.2. Como $F[x]$ es un dominio integro, existe el campo de fracciones de $F[x]$ denotado también como $F(x)$. Por lo tanto,

$$F(x) = \left\{ \frac{f(x)}{g(x)} / f(x), g(x) \in F[x] \text{ y } g(x) \neq 0 \right\}.$$

2.2 Algoritmo de Euclides

Definición 2.5

El **algoritmo de Euclides** para números enteros afirma que, sea $a, b \in \mathbb{Z}$ con $b > 0$, existen únicos enteros q, r tal que $a = bq + r$, donde $0 \leq r < b$.

Teorema 2.2

Sean $f(x), h(x)$ polinomios en $F[x]$ con $h(x) \neq 0$, entonces existen $q(x)$ y $r(x)$ polinomios en $F[x]$ tales que $f(x) = h(x)q(x) + r(x)$, donde $r(x) = 0$ ó $\deg(r) < \deg(h)$.

Nota. Al polinomio $r(x)$ se lo llama resto y al polinomio $q(x)$ se lo conoce como el cociente de la división de $f(x)$ por $h(x)$.

Demostración. Para esta demostración partiremos por inducción.

Notemos que si $f(x) = 0$ ó $\deg(f) < \deg(h)$ consideramos que $q(x) = 0$ y $r(x) = f(x)$.

Podemos suponer que

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

$$h(x) = b_0 + b_1x + \dots + b_mx^m$$

con $a_n \neq 0$ y $b_m \neq 0$ y $n \geq m$.

Empezamos definiendo un polinomio, el cual es menor a n y suponiendo por hipótesis inductiva que este polinomio cumple con el teorema, es decir, el polinomio

$$f_1(x) = f(x) - a_nb_m^{-1}x^{n-m}(h(x))$$

tiene grado menor que n , por hipótesis de inducción, existen polinomios $q_1(x)$ y $r(x)$ en $F[x]$, tales que $f_1(x) = q_1(x)h(x) + r(x)$, donde $r(x) = 0$ o $\deg(r) < \deg(h)$. Así,

$$f(x) - a_nb_m^{-1}x^{n-m}(h(x)) = h(x)q_1(x) + r(x)$$

$$f(x) = a_n b_m^{-1} x^{n-m} h(x) + h(x) q_1(x) + r(x)$$

$$f(x) = (a_n b_m^{-1} x^{n-m} + q_1(x)) h(x) + r(x).$$

Por lo tanto, consideramos

$$q(x) = a_n b_m^{-1} x^{n-m} + q_1(x)$$

$$f(x) = h(x)q(x) + r(x),$$

donde $r(x) = 0$ ó $\deg(r) < \deg(h)$, lo que demuestra la existencia de polinomios $q(x)$ y $r(x) \in F[x]$.

Finalmente probaremos la unicidad de $q(x)$ y $r(x)$ en $F[x]$. Empezamos suponiendo que $f(x) = h(x)q(x) + r(x)$ y $f(x) = h(x)q_0(x) + r_0(x)$ con $q_0(x)$ y $r_0(x)$ en $F[x]$, es decir,

$$r(x) = 0 \quad \text{ó} \quad \deg(r) < \deg(h)$$

$$r_0(x) = 0 \quad \text{ó} \quad \deg(r_0) < \deg(h).$$

Entonces

$$h(x)q(x) + r(x) = h(x)q_0(x) + r_0(x)$$

$$r(x) - r_0(x) = h(x)(q_0(x) - q(x)),$$

si suponemos que $r(x) + r_0(x) \neq 0$, entonces

$$\deg(r(x) - r_0(x)) = \deg(q_0(x) + q(x)) + \deg(h(x)) \geq \deg(h(x)),$$

por otro lado concluimos que

$$\deg(r(x) - r_0(x)) < \deg(h(x))$$

lo que nos lleva a una contradicción. Por lo tanto, $r(x) = r_0(x)$ y así

$$(q_0(x) - q(x))h(x) = 0 \Rightarrow q(x) = q_0(x). \quad \square$$

Ejemplo 2.1. Sean $f(x) = x^4 - 3x^3 + 2x^2 + 4x - 1$ y $g(x) = x^2 - 2x + 3$ en $\mathbb{Z}_5[x]$. Encontrar el cociente $q(x)$ y el resto $r(x)$ de la división de $f(x)$ por $g(x)$.

$$\begin{array}{r}
 \left(\begin{array}{l} x^4 - 3x^3 + 2x^2 + 4x - 1 \\ -x^4 + 2x^3 - 3x^2 \\ \hline -x^3 - x^2 + 4x \\ x^3 - 2x^2 + 3x \\ \hline -3x^2 + 7x - 1 \\ 3x^2 - 6x + 9 \\ \hline x + 8 \end{array} \right) \div (x^2 - 2x + 3) = x^2 - x - 3 + \frac{x + 8}{x^2 - 2x + 3}
 \end{array}$$

de donde sabemos que en \mathbb{Z}_5 el valor $[8] = [3]$, entonces podemos observar que $q(x) = x^2 - x - 3$ y el resto es $r(x) = x + 3$.

Ejemplo 2.2. Sean $f(x) = x^4 - 3x^3 + x^2 + 4$ y $g(x) = x - 2$ en $\mathbb{Z}_7[x]$. Encontrar el cociente $q(x)$ y el resto $r(x)$ de la división de $f(x)$ por $g(x)$.

$$\begin{array}{r}
 \left(\begin{array}{l} x^4 - 3x^3 + x^2 + 4 \\ -x^4 + 2x^3 \\ \hline -x^3 + x^2 \\ x^3 - 2x^2 \\ \hline -x^2 \\ x^2 - 2x \\ \hline -2x + 4 \\ 2x - 4 \\ \hline 0 \end{array} \right) \div (x - 2) = x^3 - x^2 - x - 2
 \end{array}$$

Definición 2.6

Sea $f(x)$ un polinomio no nulo con coeficientes en F y $\alpha \in F$, se dice que α es una **raíz de $f(x)$** si $f(\alpha) = 0$.

Corolario 2.2

Sea $f(x)$ un polinomio no nulo con coeficientes en F y $\alpha \in F$. Entonces α es una raíz de $f(x)$ si y sólo si, existe un polinomio $q(x)$ en $F[x]$ tal que $f(x) = (x - \alpha)q(x)$.

Demostración. \Rightarrow) Supongamos que α es una raíz de $f(x)$. Sabemos que un polinomio $f(x) = q(x)g(x) + r(x)$. Luego, $f(x) = (x - \alpha)q(x) + r(x)$, donde $r(x) = 0$ ó $\deg(r) < \deg(x - \alpha) = 1$. Así $r(x) = 0$ ó $\deg(r) = 0$, de donde $r(x) = a_0 \in F$.

Ya que α es una raíz de $f(x)$, obtenemos que

$$0 = f(\alpha) = (\alpha - \alpha)q(\alpha) + r(\alpha) = r(\alpha)$$

por lo tanto, $a_0 = 0$ y $f(x) = (x - \alpha)q(x)$.

\Leftarrow) Existe un polinomio $q(x) \in F[x]$, tal que $f(x) = (x - \alpha)g(x)$. Además, $\alpha \in F$ por lo tanto al evaluar en $f(x)$ tenemos que:

$$f(\alpha) = (\alpha - \alpha)g(\alpha)$$

$$f(\alpha) = 0.$$

□

Definición 2.7

Sea F un campo se dice que es **algebraicamente cerrado**, si todo polinomio no constante en $F[x]$ tiene al menos una raíz en F .

Observación 2.3. Un polinomio no constante es aquel polinomio con *grado* ≥ 1 .

Corolario 2.3

Sea $f(x) \in F[x]$ y $\deg(f) = n \geq 1$, donde F es un campo algebraicamente cerrado, entonces existen elementos $d, \alpha_1, \alpha_2, \dots, \alpha_n$ en F tales que,

$$f(x) = d(x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n).$$

Capítulo 2. Anillos de polinomios

Demostración. Para esta demostración nos apoyamos en la demostración por inducción, sobre el grado de $f(x)$.

- Si $\deg(f) = 1$.

$$f(x) = ax + b \text{ con } a, b \in F \text{ y } a \neq 0$$

$$f(x) = ax + aa^{-1}b$$

$$f(x) = a(x - (-a^{-1}b)).$$

- Si $\deg(f) = n > 1$.

Ya que F es algebraicamente cerrado, existe $\alpha_n \in F$ raíz de $f(x)$ por el corolario ??, existe $q(x) \in F[x]$ tal que $f(x) = (x - \alpha_n)q(x)$.

Dado que $\deg(q) = n - 1$, entonces por la hipótesis de inducción existe $d, \alpha_1, \alpha_2, \dots, \alpha_{n-1}$ en F tales que,

$$q(x) = d(x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_{n-1}).$$

Por lo tanto, $f(x) = (x - \alpha_n)d(x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_{n-1})$

$$f(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_{n-1})(x - \alpha_n).$$

□

Teorema 2.3

El polinomio $f(x) \in F[x]$ de grado $n \geq 1$ tiene a lo más n raíces en F .

Demostración. Para la demostración de este teorema lo haremos por inducción sobre el grado de $f(x)$.

- Si $\deg(f) = 1$, entonces $f(x) = ax + b$ con $a, b \in F$ y $a \neq 0$,

$-a^{-1}b \in F$ es la única raíz de $f(x)$.

- Si $\deg(f) = n > 1$.

Si $f(x)$ tiene una raíz $\alpha \in F$, entonces por el Corolario 2.3 existe un polinomio $q(x) \in F[x]$ tal que $f(x) = (x - \alpha)q(x)$, donde $\deg(q) = n - 1$. Cualquier raíz $\beta \in F$ de $f(x)$ distinta de α es una raíz de $q(x)$.

Por lo tanto,

$$f(\beta) = (\beta - \alpha)q(\beta) = 0$$

entonces $q(\beta) = 0$.

Por hipótesis de inducción $q(x)$ tiene a lo más $n - 1$ raíces, dado que las raíces de $f(x)$ son α y β las raíces de $q(x)$, concluimos que $f(x)$ tiene a lo más n raíces en F .

□

Definición 2.8

Sea $f(x)$ un polinomio con coeficientes en F y $\alpha \in F$. Se dice que α como raíz de $f(x)$ tiene **multiplicidad** $m \geq 1$, si existe $q(x) \in F[x]$ tal que $f(x) = (x - \alpha)^m q(x)$ con $q(x) \neq 0$.

Teorema 2.4 (Teorema Fundamental del Álgebra)

Sea $f(x)$ un polinomio no constante con coeficientes en el campo de los complejos \mathbb{C} , entonces $f(x)$ tiene al menos una raíz en \mathbb{C} . Por lo tanto, \mathbb{C} es un campo algebraicamente cerrado.

Demostración. La demostración del teorema fundamental del algebra se la puede encontrar en la siguiente referencia [3]. □

2.3 Máximo Común Divisor

Teorema 2.5

Sea $F[x]$ un anillo de ideales principales. Es decir, si I es un ideal de $F[x]$, entonces existe un polinomio $g(x) \in F[x]$ que es un generador de I .

Capítulo 2. Anillos de polinomios

Demostración. Si $I = \{0\}$, entonces $I = \langle 0 \rangle$, supongamos que $I \neq \{0\}$. Consideramos el polinomio no nulo $g(x) \in I$ con la propiedad: si $h(x) \in I$ y $h(x) \neq 0$, entonces $\deg(g) \leq \deg(h)$.

Por consiguiente, demostraremos que

$$I = \langle g(x) \rangle.$$

Sea $f(x) \in I$ por el algoritmo de Euclides

$$f(x) = g(x)q(x) + r(x),$$

de donde $r(x) = 0$ ó $\deg(r) < \deg(g)$.

Debido a que I es un ideal de $F[x]$, entonces $r(x) = f(x) - g(x)q(x)$ es un elemento en I , ya que $g(x) \in I$ obtenemos que $r(x) = 0$. Así $f(x) = g(x)q(x)$ por lo tanto $I = \langle g(x) \rangle$. \square

Nota. Un polinomio mónico es de la forma $f(x) = c_0 + c_1x + \dots + c_{n-1}x^{n-1} + x^n$.

Definición 2.9

Sean los polinomios $f(x), g(x)$ en $F[x]$ con $f(x)g(x) \neq 0$. Diremos que $g(x)$ divide a $f(x)$, que se denota como $g(x)|f(x)$, si existe un polinomio $h(x) \in F[x]$ tal que $f(x) = g(x)h(x)$.

Definición 2.10

Sean $f_1(x), f_2(x) \in F[x]$ con $f_1(x)f_2(x) \neq 0$. Diremos que $g(x) \in F[x]$ es un máximo común divisor de $f_1(x)$ y $f_2(x)$, si y sólo si

1. $g(x)|f_1(x)$ y $g(x)|f_2(x)$,
2. $h(x) \in F[x]$ y $h(x)|f_1(x)$ y $h(x)|f_2(x)$, entonces $h(x)|g(x)$.

Teorema 2.6

Sean $f_1(x), f_2(x)$ en $F[x]$ con $f_1(x)f_2(x) \neq 0$. Entonces existe un máximo común divisor $g(x) \in F[x]$ de $f_1(x)$ y $f_2(x)$. Además existen polinomios $q(x), t(x)$ en $F[x]$ tales que $g(x) = f_1(x)q(x) + f_2(x)t(x)$.

Demostración. Sabemos que $F[x]$ es un anillo de ideales principales entonces existe un polinomio $g(x) \in F[x]$ el cual es un generador del idea $\langle f_1(x), f_2(x) \rangle$ de $F[x]$.

Probaremos ahora que $g(x)$ es un máximo común divisor de $f_1(x)$ y $f_2(x)$ tenemos que $\langle g(x) \rangle = \langle f_1(x), f_2(x) \rangle$, entonces $f_1(x) \in \langle g(x) \rangle$ de igual manera sucede con $f_2(x) \in \langle g(x) \rangle$, es decir, existen los polinomios $q(x), t(x) \in F[x]$ tales que $f_1(x) = g(x)q(x)$ y $f_2(x) = g(x)t(x)$. Por lo tanto, $g(x)|f_1(x)$ y $g(x)|f_2(x)$. Ya que $g(x) \in \langle f_1(x), f_2(x) \rangle$, existen $q(x)$ y $t(x)$ en $F[x]$ tales que $g(x) = f_1(x)q(x) + f_2(x)t(x)$. Para nuestro segundo punto ha demostrar consideramos $h(x) \in F[x]$ tal que $h(x)|f_1(x)$ y $h(x)|f_2(x)$, existen polinomios $q_0(x), t_0(x)$ en $F[x]$ tales que

$$f_1(x) = h(x)q_0(x) \quad y \quad f_2(x) = h(x)t_0(x).$$

Ahora,

$$f_1(x)q(x) = h(x)q_0(x)q(x) \quad y \quad f_2(x)t(x) = h(x)t_0(x)t(x),$$

de donde

$$\begin{aligned} f_1(x)q(x) + f_2(x)t(x) &= h(x)q_0(x)q(x) + h(x)t_0(x)t(x) \\ &= h(x)(q_0(x)q(x) + t_0(x)t(x)). \end{aligned}$$

Por lo tanto, $h(x)|f_1(x)q(x) + f_2(x)t(x)$, es decir, $h(x)|g(x)$.

□

Observación 2.4. Si consideramos $g(x) = a_0 + a_1x + \dots + a_nx^n$ para la demostración anterior con $a_n \neq 0$, entonces $a_n^{-1}g(x)$ es también un generador de I y en consecuencia el polinomio monico $a_n^{-1}g(x)$, también es el máximo común divisor de $f_1(x)$ y $f_2(x)$. Diremos que un máximo común divisor mónico es el máximo común divisor de $f_1(x)$ y $f_2(x)$ y lo denotaremos como $(f_1(x), f_2(x))$.

Nota. Si $(f_1(x), f_2(x)) = 1$, diremos que $f_1(x), f_2(x)$ son polinomios primos relativos en $F[x]$.

Lema 2.2

Sean $f(x), g(x)$ en $F[x]$ no nulos. Utilizando el algoritmo de Euclides sucesivamente tenemos que,

$$f(x) = g(x)q_1(x) + r_1(x), \text{ donde } r_1(x) = 0 \text{ ó } \deg(r_1) < \deg(g)$$

$$g(x) = r_1(x)q_2(x) + r_2(x), \text{ donde } r_2(x) = 0 \text{ ó } \deg(r_2) < \deg(r_1)$$

$r_1(x) = r_2(x)q_3(x) + r_3(x)$, donde $r_3(x) = 0$ ó $\deg(r_3) < \deg(r_2)$ y así sucesivamente hasta $r_{n-1}(x) = r_n(x)q_{n+1}(x) + r_{n+1}(x)$, donde $r_{n+1}(x) = 0$ ó $\deg(r_{n+1}) < \deg(r_n)$.

Existe un menor entero positivo n para el cual $r_{n+1}(x) = a \in F$. Si $a = 0$ entonces $r_n(x)$ es un máximo común divisor de $f(x)$ y $g(x)$. Si $a \neq 0$, entonces $r_{n+1}(x) = a$ es un máximo común divisor de $f(x)$ y $g(x)$.

Ejemplo 2.3. Calcularemos el máximo común divisor de los polinomios

$$f(x) = x^5 + 4x^4 + 4x^3 + 2x^2 - 5x - 6 \text{ y } g(x) = x^3 - x^2 - 4$$

$$\begin{array}{r} \left(\begin{array}{r} x^5 + 4x^4 + 4x^3 + 2x^2 - 5x - 6 \\ -x^5 + x^4 - 6 \end{array} \right) \div \left(x^3 - x^2 - 4 \right) = x^2 + 5x + 9 + \frac{15x^2 + 15x + 30}{x^3 - x^2 - 4} \\ \hline \begin{array}{r} 5x^4 + 4x^3 + 6x^2 - 5x \\ -5x^4 + 5x^3 + 20x \end{array} \\ \hline \begin{array}{r} 9x^3 + 6x^2 + 15x - 6 \\ -9x^3 + 9x^2 + 36 \end{array} \\ \hline 15x^2 + 15x + 30 \end{array}$$

por lo tanto

$$x^5 + 4x^4 + 4x^3 + 2x^2 - 5x - 6 = (x^3 - x^2 - 4)(x^2 + 5x + 9) + (15x^2 + 15x + 30)$$

por consiguiente

$$\begin{array}{r} \left(\begin{array}{r} x^3 - x^2 - 4 \\ -x^3 - x^2 - 2x \\ \hline -2x^2 - 2x - 4 \\ 2x^2 + 2x + 4 \\ \hline 0 \end{array} \right) \div (15x^2 + 15x + 30) = \frac{1}{15}x - \frac{2}{15} \end{array}$$

por lo tanto

$$x^3 - x^2 - 4 = (15x^2 + 15x + 30) \left(\frac{1}{15}x - \frac{2}{15} \right)$$

,

de esta manera $15x^2 + 15x + 30$ es un máximo común divisor de $f(x)$ y $g(x)$.

Ejemplo 2.4. Calcularemos el máximo común divisor de los polinomios

$$f(x) = x^5 + 4x^4 - 3x^3 - 5x^2 + 10x - 10 \text{ y } g(x) = x^3 - 9$$

sobre el campo \mathbb{Z}_{11} de los enteros módulo 11. Encontraremos polinomios $u(x)$, $v(x)$ en $\mathbb{Z}_{11}[x]$ tales que $f(x)u(x) + g(x)v(x) = d(x)$.

$$\begin{array}{r} \left(\begin{array}{r} x^5 - 4x^4 - 3x^3 - 5x^2 + 10x - 10 \\ -x^5 \qquad \qquad \qquad + 9x^2 \\ \hline -4x^4 - 3x^3 + 4x^2 + 10x \\ 4x^4 \qquad \qquad \qquad - 36x \\ \hline -3x^3 + 4x^2 - 26x - 10 \\ 3x^3 \qquad \qquad \qquad - 27 \\ \hline 4x^2 - 26x - 37 \end{array} \right) \div (x^3 - 9) = x^2 - 4x - 3 + \frac{4x^2 - 26x - 37}{x^3 - 9} \end{array}$$

ya que estamos en el campo \mathbb{Z}_{11} tenemos que $[-26] = [7]$ y $[-37] = [-4]$, entonces

$$f(x) = g(x)(x^2 - 4x - 3) + (4x^2 + 7x - 4)$$

y $[1] = [12]$, entonces

$$\begin{array}{r} \left(\begin{array}{r} 12x^3 \qquad \qquad - 9 \\ - 12x^3 - 21x^2 + 12x \end{array} \right) \div \left(4x^2 + 7x - 4 \right) = 3x - \frac{21}{4} + \frac{\frac{195}{4}x - 30}{4x^2 + 7x - 4} \\ \hline \qquad \qquad \qquad - 21x^2 + 12x - 9 \\ \qquad \qquad \qquad \underline{21x^2 + \frac{147}{4}x - 21} \\ \qquad \qquad \qquad \qquad \qquad \frac{195}{4}x - 30 \end{array}$$

el valor $[195] = [8]$ en el campo \mathbb{Z}_{11} por lo tanto $\frac{8}{4} = 2$ y $[-30] = [-8]$.

Por lo tanto, $\frac{195}{4}x - 30 = 2x - 8$ de manera análoga $3x - \frac{21}{4} = 3x + 3$

de esta manera,

$$g(x) = (4x^2 + 7x - 4)(3x + 3) + (2x - 8)$$

finalmente

$$\begin{aligned} 2x - 8 &= g(x) - (4x^2 + 7x - 4)(3x + 3) \\ &= g(x) - (f(x) - g(x)(x^2 - 4x - 3))(3x + 3) \\ &= g(x) - f(x)(3x + 3) + g(x)(x^2 - 4x - 3)(3x + 3) \\ &= g(x) - f(x)(3x + 3) + g(x)(3x^3 - 9x^2 + x - 9) \\ &= f(x)(-3x - 3) + g(x)(3x^3 - 9x^2 + x - 8). \end{aligned}$$

Así,

$$f(x)(-3x - 3) + g(x)(3x^3 - 9x^2 + x - 8) = 2x - 8$$

por lo tanto, $2x - 8$ es un máximo común divisor de $f(x)$ y $g(x)$.

2.4 Polinomios irreducibles

Definición 2.11

Sea $f(x) \in F[x]$ con $\deg(f) \geq 1$. Diremos que $f(x)$ es irreducible sobre F o irreducible en $F[x]$, si no existen polinomios $g(x), h(x)$ en $F[x]$ tales que, $f(x) = g(x)h(x)$ con $\deg(g) < \deg(f)$ y $\deg(h) < \deg(f)$. Caso contrario es reducible.

Ejemplo 2.5. Consideremos el polinomio $f(x) = x^2 + 2 \in \mathbb{R}[x]$, donde \mathbb{R} es el campo de los números reales.

Supongamos que $f(x)$ se puede escribir como el producto de dos polinomios $g(x)$ y $h(x)$ en $\mathbb{R}[x]$, con $\deg(g) < 2$ y $\deg(h) < 2$, por lo que es necesario definir los polinomios $g(x) = ax + b$ y $h(x) = cx + d$ con $a, b, c, d \in \mathbb{R}$, $a \neq 0$ y $c \neq 0$. Luego,

$$x^2 + 2 = (ax + b)(cx + d) = ac \left(x + \frac{b}{a} \right) \left(x + \frac{d}{c} \right).$$

Por la igualdad de polinomios $ac = 1$. Sean $\frac{b}{a} = \alpha$ y $\frac{d}{c} = \beta$. Así tenemos que

$$\begin{aligned} x^2 + 2 &= (x + \alpha) \\ &= x^2 + \alpha x + \beta x + \alpha\beta \\ &= x^2 + (\alpha + \beta)x + \alpha\beta. \end{aligned}$$

Observación 2.5. Los polinomios con coeficientes en \mathbb{C} y de grados ≥ 2 son reducibles sobre \mathbb{C} .

Demostración. Sea $f(x) \in \mathbb{C}[x]$ y $\deg(f) = n \geq 2$, entonces por el Teorema fundamental del álgebra existe una raíz $\alpha \in \mathbb{C}$ de $f(x)$. Así, existe un polinomio $q(x) \in \mathbb{C}[x]$ tal que $f(x) = (x - \alpha)q(x)$. Ahora $\deg(x - \alpha) < n$ y $\deg(q) < n - 1 < n$ lo que prueba que $f(x)$ es reducible sobre \mathbb{C} . \square

Lema 2.3

Sea $h(x) \in F[x]$ un polinomio de grado 2 (ó grado 3). Entonces $h(x)$ es reducible en $F[x]$, si y sólo si, $h(x)$ tiene una raíz en F .

Capítulo 2. Anillos de polinomios

Demostración. \Rightarrow) Suponemos que $h(x)$ es reducible en $F[x]$, entonces existe un polinomio de la forma $ax + b \in F[x]$ con $a \neq 0$ y un polinomio $q(x) \in F[x]$ de grado 2 o de grado 3 tal que $h(x) = (ax + b)q(x)$. Ahora, $\alpha = -\frac{b}{a} \in F$ es una raíz de $h(x)$.

\Leftarrow) Suponemos que $h(x)$ tiene una raíz α en F , por lo tanto existe un polinomio $q(x) \in F[x]$ tal que,

$f(x) = (x - \alpha)q(x)$ con $\deg(q) = 1$ ó $\deg(q) = 2$. Por lo tanto, es reducible en $F[x]$. \square

Ejemplo 2.6. El polinomio $g(x) = x^3 + 4x^2 + 4x + 1 \in \mathbb{Z}_5[x]$ es irreducible sobre \mathbb{Z}_5 . Para encontrar la raíz evaluamos el polinomio en cada uno de los valores de \mathbb{Z}_5 .

$$p(0) = (0)^3 + 4(0)^2 + 4(0) + 1 = 1,$$

$$p(1) = (1)^3 + 4(1)^2 + 4(1) + 1 = 0$$

y luego existe un polinomio $q(x) \in \mathbb{Z}_5$ con $\deg(q) = 2$ tal que $g(x) = (x - 1)q(x)$.

Ejemplo 2.7. El polinomio $g(x) = x^3 + 3x + 2 \in \mathbb{Z}_5[x]$ es irreducible sobre \mathbb{Z}_5 .

$$p(0) = (0)^3 + 3(0)^2 + 2 = 2,$$

$$p(1) = (1)^3 + 3(1)^2 + 2 = 1,$$

$$p(2) = (2)^3 + 3(2)^2 + 2 = 1,$$

$$p(3) = (3)^3 + 3(3)^2 + 2 = 3,$$

$$p(4) = (4)^3 + 3(4)^2 + 2 = 3.$$

Ejemplo 2.8. Para determinar si el polinomio $f(x) = 2x^3 + x^2 + 2x + 2$ es irreducible sobre \mathbb{Z}_5 .

Primero, evaluemos $f(x)$ en los elementos de \mathbb{Z}_5 para ver si tiene alguna raíz en \mathbb{Z}_5 :

$$f(0) = 2 \cdot 0^3 + 0^2 + 2 \cdot 0 + 2 = 2$$

$$f(1) = 2 \cdot 1^3 + 1^2 + 2 \cdot 1 + 2 = 7 \equiv 2 \pmod{5}$$

$$f(2) = 2 \cdot 2^3 + 2^2 + 2 \cdot 2 + 2 = 26 \equiv 1 \pmod{5}$$

$$f(3) = 2 \cdot 3^3 + 3^2 + 2 \cdot 3 + 2 = 71 \equiv 1 \pmod{5}$$

$$f(4) = 2 \cdot 4^3 + 4^2 + 2 \cdot 4 + 2 = 154 \equiv 4 \pmod{5}.$$

por lo tanto, es irreducible en \mathbb{Z}_5 .

Teorema 2.7

Sea $p(x) \in F[x]$ con $\deg(p) \geq 1$. Entonces $\langle p(x) \rangle$ es un ideal maximal de $F[x]$ si y sólo si, $p(x)$ es irreducible sobre F .

Demostración. \Rightarrow) Empezamos suponiendo que $\langle p(x) \rangle$ no es un ideal maximal de $F[x]$, si y sólo si, $p(x)$ es reducible sobre F . Si $\langle p(x) \rangle$ no es un ideal maximal de $F[x]$, entonces existe un ideal J de $F[x]$ tal que $\langle p(x) \rangle \subset J$, con $\langle p(x) \rangle \neq J$ y $J \neq F[x]$.

Como $F[x]$ es un dominio de ideales principales, existe un $g(x) \in F[x]$ tal que $J = \langle g(x) \rangle = \{g(x)h(x) | h(x) \in F[x]\}$. Ahora, $\langle p(x) \rangle \subset \langle g(x) \rangle$, de donde $p(x) = g(x)h(x)$ con $h(x) \in F[x]$. Si $g(x)$ es constante, entonces $J = F[x]$ por lo que es una contradicción, ahora si $h(x)$ es constante, entonces $\langle p(x) \rangle = \langle g(x) \rangle = J$ lo que también es una contradicción. Por lo tanto, necesariamente $\deg(g) \geq 1$ y $\deg(h) \geq 1$.

Concluimos que $p(x) = g(x)h(x)$ con $\deg(g) < \deg(p)$ y $\deg(h) < \deg(p)$ por lo tanto, $p(x)$ es reducible sobre F .

\Leftarrow) Supongamos que $p(x)$ es reducible sobre F , entonces existen polinomios $g(x), h(x)$ en $F[x]$ tal que $p(x) = g(x)h(x)$ con $\deg(g) < \deg(p)$ y $\deg(h) < \deg(p)$.

Notemos que $\deg(g) > 0$ y $\deg(h) > 0$ de lo contrario $\deg(g) = \deg(p)$ ó $\deg(h) = \deg(p)$.

Claramente $\langle p(x) \rangle \subset \langle g(x) \rangle$ y $\langle g(x) \rangle \neq F[x]$ esto dado que $1 \notin \langle g(x) \rangle$. Ahora $g(x) \notin \langle p(x) \rangle$. Si suponemos que, $g(x) \in \langle p(x) \rangle$, entonces $g(x) = q(x)p(x)$ con $q(x) \in F[x]$. Así $p(x) = g(x)h(x) = p(x)q(x)h(x)$ lo cual implica que $q(x)h(x) = 1$, dado que $p(x) \neq 0$ y $F[x]$ no tiene divisores de cero, entonces de $q(x)h(x) = 1$ concluimos que $\deg(q) = \deg(h) = 0$ lo que es una contradicción. Por lo tanto, $g(x) \notin \langle p(x) \rangle$ y de esta manera obtenemos que $\langle p(x) \rangle \neq \langle g(x) \rangle$, lo que implica que $\langle p(x) \rangle$ no es un ideal maximal. \square

Corolario 2.4

Sea $p(x) \in F[x]$ con $\deg(p) \geq 1$. Entonces $p(x)$ es irreducible sobre F si y sólo si, $F[x]/\langle p(x) \rangle$ es un campo.

Demostración. \Rightarrow) Suponemos que $p(x)$ con $\deg(p) \geq 1$ es irreducible sobre F , por el teorema anterior $\langle p(x) \rangle$ es un ideal maximal. Si $\langle p(x) \rangle$ es un ideal maximal de $F[x]$, entonces $F[x]/\langle p(x) \rangle$ es un campo.

\Leftarrow) Si $F[x]/\langle p(x) \rangle$ es un campo, entonces $\langle p(x) \rangle$ es un ideal maximal de $F[x]$. Luego, si $\langle p(x) \rangle$ es un ideal maximal de $F[x]$, entonces $p(x)$ es irreducible sobre F . \square

Nota. Dado un elemento $f(x) + \langle p(x) \rangle$ en $F[x]/\langle p(x) \rangle$ siempre existe un polinomio $g(x) \in F[x]$ tal que $f(x) + \langle p(x) \rangle = g(x) + \langle p(x) \rangle$, donde $g(x) = 0$ ó $\deg(g) < \deg(p)$.

Lema 2.4

Sea F un campo, $p(x) \in F[x]$ irreducible sobre F y $\deg(p) = n$. Entonces

$$F[x]/\langle p(x) \rangle = \{a_0 + a_1x + \dots + a_{n-1}x^{n-1} + \langle p(x) \rangle \mid a_0, a_1, \dots, a_{n-1} \in F\}.$$

Demostración. Para la demostración de este lema consideramos $f(x) + \langle p(x) \rangle$, como un elemento en $F[x]/\langle p(x) \rangle$. Por el algoritmo de Euclides existen los polinomios $q(x), r(x)$ en $F[x]$, tales que $f(x) = q(x)p(x) + r(x)$, donde $r(x) = 0$ ó $\deg(r) < \deg(p)$. Luego, $f(x) - r(x) = p(x)q(x) \in \langle p(x) \rangle$, ya que $f(x) + \langle p(x) \rangle = r(x) + \langle p(x) \rangle$ con $r(x) = 0$ ó $\deg(r) < n$, entonces $r(x)$ es un polinomio de la forma,

$$a_0 + a_1x + \dots + a_{n-1}x^{n-1} \in F[x].$$

Por lo tanto, $f(x) + \langle p(x) \rangle = a_0 + a_1x + \dots + a_{n-1}x^{n-1} + \langle p(x) \rangle$. \square

Ejemplo 2.9. Sea $p(x) = x^3 - 2 \in \mathbb{Q}[x]$. Demostraremos que el anillo cociente $\mathbb{Q}[x]/\langle p(x) \rangle$ es un campo, y encontrar el inverso multiplicativo del elemento $2 + 3x - 5x^2 + \langle p(x) \rangle \in \mathbb{Q}[x]/\langle p(x) \rangle$.

Los posibles raíces en \mathbb{Q} de $p(x) = x^3 - 2$ son $\pm 1, \pm 2$, como ninguno de estos enteros es una raíz de $p(x)$, decimos que $p(x)$ es irreducible sobre \mathbb{Q} .

Ahora procedemos a encontrar el inverso multiplicativo del elemento $2 + 3x - 5x^2 + \langle p(x) \rangle \in \mathbb{Q}[x]/\langle p(x) \rangle$ por el Lema 2.4 los elementos del campo $\mathbb{Q}[x]/\langle p(x) \rangle$ son de la forma $a + bx + cx^2 + \langle p(x) \rangle$, donde $a, b, c \in \mathbb{Q}$. Por lo tanto, vamos a encontrar $a, b, c \in \mathbb{Q}$.

$$(a + bx + cx^2 + \langle p(x) \rangle)(2 + 3x - 5x^2 + \langle p(x) \rangle) = 1 + \langle p(x) \rangle,$$

lo que significa que,

$$(a + bx + cx^2)(2 + 3x - 5x^2) - 1 \in \langle p(x) \rangle$$

es decir,

$$2a - 1 + (3a + 2b)x + (-5a + 3b + 2c)x^2 + (3c - 5b)x^3 - 5cx^4 \in \langle p(x) \rangle$$

dividiendo el polinomio

$$2a - 1 + (3a + 2b)x + (-5a + 3b + 2c)x^2 + (3c - 5b)x^3 - 5cx^4$$

por $x^3 - 2$ tenemos como cociente de la división,

$$q(x) = -5cx + 3c - 5b$$

y el resto,

$$r(x) = (-5a + 3b + 2c)x^2 + (3a + 2b - 10c)x + 2a - 10b + 6c - 1$$

deseamos que $r(x) = 0$, por lo tanto resolvemos esto por sistema de ecuaciones

$$-5a + 3b + 2c = 0 \quad 3a + 2b - 10c = 0 \quad 2a - 10b + 6c = 1,$$

de donde $a = \frac{-17}{129}$, $b = \frac{-22}{129}$ y $c = \frac{-19}{258}$ por lo tanto el inverso multiplicativo es

$$(2 + 3x - 5x^2 + \langle p(x) \rangle)^{-1} = \frac{-17}{129} - \frac{22}{129}x - \frac{19}{258}x^2 + \langle p(x) \rangle.$$

Definición 2.12 (Contenido de un polinomio)

El contenido de un polinomio $a_n x^n + a_{n-1} x^{n-1} + \dots + a_0$ donde los coeficientes a son enteros, es el máximo común divisor de sus coeficientes.

Definición 2.13

Un polinomio $f(x) = a_0 + a_1 x + \dots + a_n x^n \in \mathbb{Z}[x]$ es llamado **primitivo** si el máximo común divisor de sus coeficientes es 1.

Lema 2.5

El producto de dos polinomios primitivos $f(x)$ y $g(x)$ es también primitivo.

Demostración. Sean $f(x) = \sum_{i=0}^m a_i x^i$ y $g(x) = \sum_{i=0}^n b_i x^i$. Supongamos que p es un primo que divide a todos los coeficientes de $f(x)g(x)$. Sea r el menor entero tal que $p \nmid a_r$ y s el menor entero tal que $p \nmid b_s$. El coeficiente de x^{r+s} en $f(x)g(x)$ es

$$c_{r+s} = a_0 b_{r+s} + a_1 b_{r+s-1} + \dots + a_{r+s-1} b_1 + a_r b_0.$$

Dado que p divide a a_0, \dots, a_{r-1} y b_0, \dots, b_{s-1} , p divide a cada término de c_{r+s} excepto por el término $a_r b_s$. Sin embargo, como $p \mid c_{r+s}$, debe ser que $p \mid a_r$ o $p \mid b_s$, lo cual es imposible. \square

Teorema 2.8

Sea $f(x) \in \mathbb{Z}[x]$. Si $f(x)$ es irreducible sobre \mathbb{Q} , entonces es irreducible sobre \mathbb{Z} .

Demostración. Supongamos que $f(x) = g(x)h(x)$, donde $g(x)$ y $h(x) \in \mathbb{Q}[x]$. Claramente, podemos suponer que $f(x)$ es primitivo porque podemos dividir tanto $f(x)$ y $g(x)$ por el contenido de $f(x)$. Sea a el mínimo común múltiplo de los denominadores de los coeficientes de $g(x)$, y b es el mínimo común múltiplo de los denominadores de los coeficientes de $h(x)$. Entonces $abf(x) = ag(x) \cdot bh(x)$, donde $ag(x)$ y $bh(x) \in \mathbb{Z}[x]$. Sea c_1 el contenido de $ag(x)$ y c_2 el contenido de $bh(x)$. Entonces $ag(x) = c_1 g_1(x)$ y $bh(x) = c_2 h_1(x)$. Dado que $f(x)$ es primitivo, el contenido de $abf(x)$ es ab . Además, dado el producto de dos polinomios

primitivos, se sigue que el contenido $c_1c_2g_1(x)h_1(x)$ es c_1c_2 . Así $ab = c_1c_2$ y $f(x) = g_1(x)h_1(x)$ donde $g_1(x)$ y $h_1(x) \in \mathbb{Z}[x]$ y $\deg(g_1(x)) = \deg(g(x))$ y $\deg(h_1(x)) = \deg(h(x))$. \square

Teorema 2.9 (El criterio de Eisenstein)

Sea $f(x) = a_0 + a_1x + \dots + a_{n-1}x^{n-1} + a_nx^n \in \mathbb{Z}[x]$. Supongamos que para algún primo p se tiene que $p \nmid a_n$, p es un divisor de a_0, a_1, \dots, a_{n-1} y $p^2 \nmid a_0$. Entonces $f(x)$ es irreducible sobre los racionales.

Demostración. Si $f(x)$ es reducible sobre \mathbb{Q} entonces existe elementos $g(x)$ y $h(x)$ en $\mathbb{Z}[x]$ tal que $f(x) = g(x)h(x)$, $1 \leq \deg(g(x))$ y $1 \leq \deg(h(x)) < n$. Definimos los polinomios $g(x) = b_0 + b_1x + \dots + b_r x^r$ y $h(x) = c_0 + c_1x + \dots + c_s x^s$. Entonces dado que $p \mid a_0$, $p^2 \nmid a_0$, y $a_0 = b_0c_0$, se sigue que p divide a b_0 ó divide c_0 . Si consideramos que $p \mid b_0$ y $p \nmid c_0$, además, como $p \nmid a_n = b_r c_s$ sabemos que $p \nmid b_r$. Por lo tanto, existe un entero t tal que $p \nmid b_t$. Ahora consideramos $a_t = b_t c_0 + b_{t-1} c_1 + \dots + b_0 c_t$, por suposición p divide a_t y por elección de t , cada sumando a la derecha después del primero es divisible por p . Claramente, esto implica que p divide a $b_t c_0$. Sin embargo, esto es imposible ya que p es primo y p no divide a b_t ni a c_0 . \square

Ejemplo 2.10. Sea el polinomio $f(x) = 3x^5 + 15x^4 - 20x^3 + 10x + 20$ es irreducible sobre \mathbb{Q} , tomando el número primo $p = 5$, $5 \nmid 3$ y $25 \nmid 20$ además de que 5 divide a 15, -20 , 10, y 20.

Teorema 2.10 (Teorema de la Factorización única)

Sea $f(x) \in F[x]$ y $\deg(f) \geq 1$

- Existen polinomios $p_1(x), \dots, p_n(x)$ en $F[x]$ irreducible sobre F tales que $f(x) = p_1(x) \dots p_n(x)$.
- Si $f(x) = p_1(x) \dots p_n(x) = q_1(x) \dots q_m(x)$, donde $p_1(x), \dots, p_n(x)$, $q_1(x), \dots, q_m(x)$ en $F[x]$ son irreducibles sobre F , entonces $n = m$, y después, haciendo una posible permutación de $q_1(x), \dots, q_m(x)$, se tiene

que $q_i(x) = a_i p(x)$ con $a_i \in F$ para todo $i \in \{1, \dots, n\}$.

Demostración. a) Empezaremos demostrando por inducción. Si $\deg(f) = 1$, entonces $f(x)$ es irreducible sobre F .

Si $\deg(f) = k \geq 2$ partimos suponiendo que, cualquier polinomio no constante en $F[x]$ con *grado* $< k$, admite una factorización en polinomios irreducibles de $F[x]$. Si $f(x)$ es irreducible sobre F , entonces no hay que demostrar. Si suponemos que $f(x)$ no es irreducible sobre F , entonces existen los polinomios $g(x), h(x) \in F[x]$ tal que,

$$f(x) = h(x)g(x) \quad \deg(g) < \deg(f) \quad \text{y} \quad \deg(h) < \deg(f).$$

Por lo tanto, podemos expresar $g(x)$ y $h(x)$ como un producto de polinomios irreducibles sobre $F[x]$, entonces $f(x) = g(x)h(x)$.

b) Por hipótesis sabemos que,

$$f(x) = p_1(x) \cdots p_n(x) = q_1(x) \cdots q_m(x),$$

donde $p_1(x), \dots, p_n(x), q_1(x), \dots, q_m(x)$ en $F[x]$ son irreducibles sobre F , por lo tanto,

$$p_1(x) | q_1(x) \cdots q_m(x),$$

ya que $p_1(x)$ es irreducible sobre F , entonces $p_1(x) | q_j(x)$ para todo $j \in \{1, \dots, m\}$. Luego de volver a numerar los $q_i(x)$ suponemos que $p_1(x) | q_1(x)$ y así,

$$q_1(x) = a_1 p_1(x), \quad \text{con} \quad a_1 \in F.$$

De esta manera obtenemos que

$$p_1(x) \cdots p_n(x) = a_1 p_1(x) q_2(x) \cdots q_m(x),$$

de donde $p_2(x) \cdots p_n(x) = a_1 q_2(x) \cdots q_m(x)$.

Repetiendo nuestro argumento inductivamente, concluimos que existe $a_i \in F$ tales que $q_i(x) = a_i p_i(x)$ para todo $i \in \{1, \dots, m\}$.

Si suponemos $n < m$, obtenemos $1 = \alpha_1 \alpha_2 \cdots \alpha_n q_{n+1}(x) \cdots q_m(x)$, donde $\deg(q_m) = 0$, lo que es una contradicción. Así, $n = m$.

□

3

Extensiones de campos

Las extensiones de campos son los puentes que conectan las soluciones de ecuaciones algebraicas con los fundamentos de la teoría de Galois. En este tercer capítulo, nos centraremos en el estudio de estas extensiones, esclareciendo sus propiedades y aplicaciones cruciales. Desde las extensiones finitas hasta las algebraicas, abordaremos cómo estas estructuras nos permiten comprender de manera más profunda la insolubilidad de las ecuaciones algebraicas.

3.1 Definiciones preliminares

Definición 3.1

Un conjunto no vacío V se dice que es un **espacio vectorial** sobre un campo F si V es un grupo abeliano respecto a la operación $+$, y si para todo $\alpha \in F$, $v \in V$ está definido un elemento, escrito como αv , con las siguientes propiedades:

1. $\alpha(v + w) = \alpha v + \alpha w$
2. $(\alpha + \beta)v = \alpha v + \beta v$
3. $\alpha(\beta v) = (\alpha\beta)v$
4. $1v = v$

para cada $\alpha, \beta \in F$ y $v, w \in V$, donde el 1 representa el elemento unitario de F en la multiplicación.

Definición 3.2

Un conjunto S de vectores se dice **linealmente dependiente** sobre el campo F si existe los vectores v_1, v_2, \dots, v_n de S y los elementos a_1, a_2, \dots, a_n de F , no todos cero, tal que $a_1v_1 + a_2v_2 + \dots + a_nv_n = 0$. Un conjunto de vectores que no es linealmente dependiente es llamado **linealmente independiente** sobre F .

Definición 3.3

Sea V un espacio vectorial sobre un campo F y sea U un subconjunto de V . Decimos que U es un **subespacio** de V si U es también un espacio vectorial sobre F bajo las operaciones de V .

Definición 3.4

Un sistema de vectores $\{v_1, v_2, \dots, v_n\} \subset V$ de un espacio vectorial V se dice que es un **Sistema de Generadores** de V si para todo $u \in V$ este es una combinación lineal finita de elementos del sistema $\{v_1, v_2, \dots, v_n\}$.

Definición 3.5

Un sistema de generadores de un espacio vectorial V se dice que es una **Base** si los vectores del sistema son linealmente independientes.

Definición 3.6

Un espacio vectorial que tiene una base con n elementos se dice que tiene dimensión n . El espacio vectorial trivial $\{0\}$ se dice que esta abarcado por el conjunto vacío y que tiene dimensión 0.

3.2 Extensiones Finitas y Algebraicas

Definición 3.7

Diremos que H es una extensión de un campo F , si K es un campo y F es un subcampo de K .

Definición 3.8

Sea K una extensión de un campo F . Diremos que la dimensión de K , como espacio vectorial sobre F , es el grado de K sobre F , que denotaremos por $[K : F]$. Además, cuando $[K : F]$ sea finito diremos que K es una extensión finita de F .

Teorema 3.1

Sean E una extensión de un campo K , y K una extensión del campo F .

- a) Si $[E : K]$ y $[K : F]$ son finitos, entonces $[E : F]$ es finito. Además, $[E : F] = [E : K][K : F]$.
- b) Si $[E : K]$ es finito, entonces $[E : K]$ y $[K : F]$ son finitos.

Demostración. a) Consideramos $\{\alpha_1, \dots, \alpha_n\}$ como base de K sobre F , y $\{\beta_1, \dots, \beta_m\}$ base de E sobre K . Debemos demostrar que $\{\alpha_i\beta_j / i \in \{1, \dots, n\}; j \in \{1, \dots, m\}\}$ es una base para E como espacio vectorial sobre F .

i. Desmostraremos que los mn vectores:

$$\alpha_1\beta_1, \dots, \alpha_1\beta_n, \alpha_2\beta_1, \dots, \alpha_2\beta_m, \alpha_n\beta_1, \dots, \alpha_n\beta_m,$$

son linealmente independientes sobre F .

Sea $\sum k_{ij}\alpha_i\beta_j = 0$, donde $k_{ij} \in F$. Entonces

$$\begin{aligned} \sum k_{ij}\alpha_i\beta_j &= (k_{11}\alpha_1\beta_1 + k_{12}\alpha_1\beta_2 + \dots + k_{1m}\alpha_1\beta_m) \\ &\quad + (k_{21}\alpha_1\beta_2 + k_{22}\alpha_2\beta_2 + \dots + k_{2m}\alpha_2\beta_m) + \dots \\ &\quad + (k_{n1}\alpha_n\beta_1 + k_{n2}\alpha_n\beta_2 + \dots + k_{nm}\alpha_n\beta_m) = 0, \end{aligned}$$

lo que implica que

$$\begin{aligned} (k_{11}\alpha_1 + k_{21}\alpha_2 + \dots + k_{n1}\alpha_n)\beta_1 + (k_{12}\alpha_1 + k_{22}\alpha_2 + \dots + k_{n2}\alpha_n)\beta_2 + \dots \\ + (k_{1m}\alpha_1 + k_{2m}\alpha_2 + \dots + k_{nm}\alpha_n)\beta_m, \end{aligned}$$

y esto es igual a lo siguiente,

$$\left(\sum_{i=1}^n k_{i1}\alpha_i \right) \beta_1 + \left(\sum_{i=1}^n k_{i2}\alpha_i \right) \beta_2 + \dots + \left(\sum_{i=1}^n k_{im}\alpha_i \right) \beta_m = 0.$$

Sabemos que β_1, \dots, β_m son linealmente independientes sobre K . Luego, los coeficientes de β_j para $j \in \{1, \dots, m\}$ es cero, es decir, $\sum_{i=1}^n k_{ij}\alpha_i = 0$. Pero $\alpha_1, \alpha_2, \dots, \alpha_n$ también es independiente sobre F , entonces $k_{ij} = 0$ con $i \in \{1, \dots, n\}$ y $j \in \{1, \dots, m\}$.

- ii. Demostraremos que los mn vectores $\alpha_i\beta_j$ con $j \in \{1, \dots, m\}$ y $i \in \{1, \dots, n\}$, son generadores del espacio vectorial E sobre F .

Si tomamos el elemento $\beta \in E$, debemos verificar que β se puede expresar como la combinación lineal de los mn vectores $\alpha_i\beta_j$ con coeficientes en F . Ya que $\{\beta_1, \dots, \beta_m\}$ es una base de E sobre K , existen elementos k_1, \dots, k_m en K , tales que $\beta = \{k_1\beta_1 + k_2\beta_2 + \dots + k_m\beta_m\}$.

Por otro lado sabemos que $\{\alpha_1, \dots, \alpha_n\}$ es una base de K sobre F . Por lo tanto, para cada k_j existen $t_{1j}, t_{2j}, \dots, t_{nj}$ en F tales que, $k_j = t_{1j}\alpha_1, t_{2j}\alpha_2, \dots, t_{nj}\alpha_n$.

Finalmente,

$$\beta = \{k_1\beta_1 + k_2\beta_2 + \dots + k_m\beta_m\},$$

es decir,

$$\begin{aligned} \beta &= (t_{11}\alpha_1, t_{21}\alpha_2, \dots, t_{n1}\alpha_n)\beta_1 + \dots + (t_{1m}\alpha_1, t_{2m}\alpha_2, \dots, t_{nm}\alpha_n)\beta_m \\ \beta &= \sum t_{ij}\alpha_i\beta_j \end{aligned}$$

lo que demuestra lo deseado.

- b) Por hipótesis, $[E : F]$ es finito y K es un subespacio vectorial de E . Luego, $[K : F]$ es finito.

Supongamos que $\{\alpha_1, \dots, \alpha_n\}$ es una base de E como espacio vectorial sobre F , lo que implica que para cada elemento $\alpha \in E$ existen $b_1, b_2, \dots, b_n \in F$ tal que, $\alpha = a_1\alpha_1 + a_2\alpha_2 + \dots + a_n\alpha_n$. Pero F es un subconjunto de K , entonces

$$\alpha = a_1\alpha_1 + a_2\alpha_2 + \dots + a_n\alpha_n \quad \text{con} \quad a_1, a_2, \dots, a_n \in K.$$

Por lo tanto, $\alpha_1, \alpha_2, \dots, \alpha_n$ son generadores de E como espacio vectorial sobre K .

Así, $[E : K] \leq n$.

□

Corolario 3.1

Si F_1, F_2, \dots, F_r son campos tales que cada campo F_{i+1} es una extensión finita de F_i , entonces F_r es una extensión finita de F_1 y además,

$$[F_r : F_1] = [F_r : F_{r-1}][F_{r-1} : F_{r-2}] \cdots [F_2 : F_1].$$

Demostración. Esta demostración la desarrollamos por medio de inducción, partiremos tomando desde $r = 2$ el cual es trivial, $[F_2 : F_1] = [F_2 : F_1]$.

Para $r = 3$

$$[F_3 : F_1] = [F_3 : F_1][F_2 : F_1]$$

esto se verifica por el teorema anterior item a).

Para $r = k$ suponemos que el corolario es válido,

$$[F_k : F_1] = [F_k : F_{k-1}][F_{k-1} : F_{k-2}] \cdots [F_2 : F_1].$$

Para $r = k + 1$ suponemos que el corolario es válido,

$$[F_{k+1} : F_1] = [F_{k+1} : F_k][F_k : F_1]$$

$$[F_{k+1} : F_1] = [F_{k+1} : F_k][F_k : F_{k-1}][F_{k-1} : F_{k-2}] \cdots [F_2 : F_1].$$

□

Definición 3.9

Sea K una extensión de un campo F , y $\alpha \in K$, se dice que es algebraico sobre F , si existe $f(x) \in F[X]$ tal que $f(\alpha) = 0$. Si $\alpha \in K$ no es algebraico sobre F se dice que α es trascendente sobre F .

Ejemplo 3.1. Para el polinomio $f(x) = x^2 - 2 \in \mathbb{Q}[x]$ su raíz es $\alpha = \sqrt{2}$ ya que $f(\alpha) = 0$. Por lo tanto, $\sqrt{2} \in \mathbb{R}$ es algebraico sobre \mathbb{Q} .

Ejemplo 3.2. El elemento $i \in \mathbb{C}$ es algebraico sobre \mathbb{Q} , dado que i es una raíz del

polinomio $f(x) = x^2 + 1 \in \mathbb{Q}$ esto se verifica con lo siguiente,

$$f(x) = x^2 + 1 = 0$$

$$x^2 = -1$$

$$x = \sqrt{-1}$$

$$x = i.$$

Teorema 3.2

Si K es una extensión finita de un campo F , entonces K es una extensión algebraica de F .

Demostración. Sea $[K : F] = n$ y $\alpha \in K$. Se demostrará que α es algebraico sobre F . Notemos que $\alpha, \alpha^2, \dots, \alpha^n, \alpha^{n+1}$ son vectores en K . Debido a que la dimensión de K como espacio vectorial sobre F es n , entonces los $n + 1$ vectores $\alpha, \alpha^2, \dots, \alpha^n, \alpha^{n+1}$ son linealmente dependientes sobre F . Luego, existen elementos a_1, a_2, \dots, a_{n+1} en F , no todos cero, tales que $a_1\alpha + a_2\alpha^2 + \dots + a_n\alpha^n + a_{n+1}\alpha^{n+1} = 0$. Así, α es una raíz de $f(x) = a_1x + a_2x^2 + \dots + a_nx^n + a_{n+1}x^{n+1} = 0 \in F[x]$ y por lo tanto, α es algebraico sobre F . \square

Observación 3.1. El conjunto $\bar{\mathbb{Q}} = \{\alpha \in \mathbb{C} / \alpha \text{ es algebraico sobre } \mathbb{Q}\}$ es un campo.

Lema 3.1

Sea K una extensión de un campo F y $\alpha \in K$ algebraico sobre F . Entonces,

- El conjunto $J = \{f(x) \in F[x] / f(\alpha) = 0\}$ es un ideal del anillo de polinomios $F[x]$, generado por un polinomio mónico $p(x) \in F[x]$ irreducible sobre F .
- Existe un único polinomio mónico $p(x) \in F[x]$ irreducible sobre F tal que $p(\alpha) = 0$.

Demostración. a) Partimos demostrando que el conjunto

$$J = \{f(x) \in F[x] / f(\alpha) = 0\},$$

es ideal del anillo $F[x]$.

Sea $f(\alpha), g(\alpha) \in J$, entonces $f(\alpha) - g(\alpha) \in J$.

$$\begin{aligned} f(\alpha) - g(\alpha) &= 0 - 0 \\ &= 0, \quad \text{donde } 0 \in J. \end{aligned}$$

Entonces $f(\alpha) - g(\alpha) \in J$.

Sea $f(\alpha) \in J$ y $r(x) \in F[x]$, entonces $f(\alpha)r(x) \in J$.

$$\begin{aligned} f(\alpha)r(x) &= 0 \cdot r(x) \\ &= 0 \quad \text{donde } 0 \in J. \end{aligned}$$

Demostrando así, que J es un ideal del anillo $F[x]$.

Luego, ya que $\alpha \in K$ es algebraico sobre F , entonces existe un polinomio no nulo $f(x) \in F[x]$ tal que $f(\alpha) = 0$. Así, $f(x) \in J$ y $J \neq \{0\}$.

Sabemos que $F[x]$ es un anillo de ideales principales, entonces existe un polinomio $q(x) \in F[x]$ generador de J , es decir, $J = \langle q(x) \rangle = \{q(x)r(x)/r(x) \in F[x]\}$. Notemos que $q(x)$ no debe ser un polinomio constante, dado que $q(\alpha) = 0$. Así, $\deg(q(x)) \geq 1$.

Ahora demostraremos que $q(x)$ es irreducible sobre F . Supongamos que $q(x)$ es reducible sobre F , entonces existe $g(x), h(x) \in F[x]$ tales que,

$$q(x) = g(x)h(x) \quad \text{con} \quad \deg(g) < \deg(q) \quad \text{y} \quad \deg(h) < \deg(q).$$

Pero $q(\alpha) = g(\alpha)h(\alpha) = 0$, de donde $g(\alpha) = 0$ ó $h(\alpha) = 0$. Si $g(\alpha) = 0$, entonces $g(x) \in J = \langle q(x) \rangle$. Luego, existe un polinomio $r(x) \in F[x]$ tal que $r(x)q(x) = g(x)$. Ahora,

$$g(x)(1 - h(x)r(x)) = g(x) - (g(x)h(x)r(x)) = g(x) - q(x)r(x) \quad g(x) - g(x) = 0.$$

Dado que $g(x)(1 - h(x)r(x)) = 0$, $g(x) \neq 0$ y $F[x]$ no tiene divisores de cero, concluimos que $h(x)r(x) = 1$, lo que implica que $h(x) = b_0 \in F$ con $b_0 \neq 0$ y $r(x) = b_0^{-1} \in F$

$$q(x) = g(x)b_0$$

por lo tanto,

$$\begin{aligned}\deg(q(x)) &= \deg(g(x)) + \deg(b_0) \\ &= \deg(q(x))\end{aligned}$$

lo que es una contradicción. Se concluye que $q(x)$ es irreducible sobre F .

Ahora si suponemos que $q(x) = a_0 + a_1x + \cdots + a_nx^n$ con $a_n \neq 0$, entonces el polinomio $p(x) = a_n^{-1}q(x) \in F[x]$ es mónico y además, $J = \langle p(x) \rangle$. Claramente $p(x)$ es irreducible sobre F , dado que $q(x)$ es irreducible.

b) Sea $t(x) \in F[x]$ un polinomio irreducible mónico tal que $t(\alpha) = 0$. Entonces $t(x) \in J = \langle p(x) \rangle$, por lo tanto, $t(x) = p(x)r(x)$ con $r(x) \in F[x]$.

Si $\deg(r) \geq 1$, entonces, dado que $\deg(p) = n \geq 1$, se obtiene que $t(x)$ es reducible, una contradicción. Por lo tanto, $\deg(r) = 0$ y así $r(x) = c \in F$. Ya que $t(x) = cp(x)$, entonces $\deg(t) = \deg(p) = n$. Los coeficientes de x^n de los polinomios $t(x)$ y $cp(x)$ son 1 y c respectivamente, pero estos polinomios son iguales, debido a que los polinomios son mónicos lo que implica que $c = 1$, de donde $t(x) = p(x)$. Así, $p(x) \in F[x]$ es único.

□

Definición 3.10

Sea K una extensión de un campo F y $\alpha \in K$ algebraico sobre F . Entonces el único polinomio irreducible mónico $p(x) \in F[x]$ tal que $p(\alpha) = 0$ se llama el polinomio irreducible de α sobre F y $\deg(p)$ es el grado de α sobre F .

Ejemplo 3.3. Encontraremos el polinomio irreducible de $\sqrt{3} + \sqrt{5}$ sobre \mathbb{Q} . Sea $\alpha = \sqrt{3} + \sqrt{5}$. Entonces $\alpha^2 = (\sqrt{3} + \sqrt{5})^2 = 2 + 2\sqrt{3}\sqrt{5} + 5 = 8 + 2\sqrt{15}$ y así, $\alpha^2 - 8 = 2\sqrt{15}$. Ahora, $(\alpha^2 - 8)^2 = 60$, de donde obtenemos $\alpha^4 - 16\alpha^2 + 4 = 0$. Por lo tanto, $\sqrt{3} + \sqrt{5}$ es una raíz del polinomio $p(x) = x^4 - 16x^2 + 4 \in \mathbb{Q}[x]$ y de esta forma, $\sqrt{3} + \sqrt{5}$ es algebraico sobre \mathbb{Q} .

A continuación verificaremos que el polinomio $p(x)$ es irreducible sobre \mathbb{Q} . Notemos que $p(x)$ no tiene raíces en \mathbb{Q} . En efecto $p(1) = p(-1) = -11$, $p(3) = p(-3) = -59$ y $p(9) = p(-9) = 5269$. Luego, $p(x)$ no se puede factorizar

como el producto de un polinomio de grado 1 y de grado 3 sobre \mathbb{Q} . Si suponemos que $p(x)$ se puede factorizar como el producto de dos polinomios de grado 2 sobre \mathbb{Q} , ya que $p(x)$ es mónico, entonces se puede expresar como el producto de dos polinomios mónicos. Así,

$$u(x) = x^2 + ax + b \quad \text{y} \quad v(x) = x^2 + cx + d,$$

entonces $x^4 - 16x^2 + 4 = (x^2 + ax + b)(x^2 + cx + d)$,

$$x^4 - 16x^2 + 4 = x^4 + (a + c)x^3 + (b + d + ac)x^2 + (ad + bc)x + bd,$$

de donde $a + c = 0$, $b + d + ac = -16$, $ad + bc = 0$ y $bd = 4$. Luego $c = -a$, entonces $ad + b(-a) = a(d - b) = 0$, para que esto suceda consideramos $a = 0$ ó $d - b = 0$.

Si consideramos $a = 0$, entonces $b + d + 0c = -16$ así $b + d + 16 = 0$ y $bd = 4$. Ahora,

$$0 = b(b + d + 16)$$

$$0 = b^2 + bd + 16b$$

$$0 = b^2 + 16b + 4 - 60 + 60$$

$$0 = (b^2 + 16b + 69) - 60$$

$$0 = (b + 8)^2 - 60$$

$$60 = (b + 8)^2 \quad \text{con} \quad b \in \mathbb{Z},$$

lo que es una contradicción.

Si $d - b = 0$, entonces $d = b$ por lo que,

$$b^2 = 4$$

$$b = \pm 2.$$

Si $b = d = 2$, entonces $2 + 2 + ac = -16$ obteniendo así $ac = -20$. Luego,

$$a + c = 0$$

$$a(a + c) = 0$$

$$a^2 + ac = 0$$

$$a^2 = 20 \quad \text{con} \quad a \in \mathbb{Z},$$

lo que es una contradicción.

Si $b = d = -2$, entonces $(-2 + (-2)) + ac = -16$ obteniendo así $ac = -12$.

Luego,

$$a + c = 0$$

$$a(a + c) = 0$$

$$a^2 + ac = 0$$

$$a^2 = 12 \quad \text{con } a \in \mathbb{Z},$$

lo que es una contradicción.

De esta forma hemos demostrado que el polinomio irreducible de $\sqrt{3} + \sqrt{5}$ sobre \mathbb{Q} es $p(x) = x^4 - 16x^2 + 4$.

Nota. Sea K una extensión de un campo F y $\alpha \in K$ no necesariamente algebraica. Denotaremos por $F[\alpha]$ al conjunto formado por todos los elementos de la forma $f(\alpha)$, donde $f(x) \in F[x]$. Es decir,

$$F[\alpha] = \{f(\alpha) / f(x) \in F[x]\}.$$

De manera similar a como se demuestra que el conjunto $F[x]$ es un dominio integro, podemos demostrar que $F[\alpha]$ es un dominio integro.

Demostración. Supongamos que $f(\alpha)g(\alpha) = 0$, para $f(\alpha), g(\alpha) \in F[\alpha]$, tomemos en cuenta que $f(x), g(x) \in F[x]$, de donde $F[x]$ también es un dominio integro lo que implica que no tiene divisores de cero, así $f(x)g(x)$ evaluado en α es cero, pero α no es necesariamente algebraico, entonces $f(x)$ ó $g(x)$ es el polinomio nulo. Por lo tanto, $F[\alpha]$ no tiene divisores de cero. \square

Teorema 3.3

Sea K una extensión de un campo F y $\alpha \in K$. Entonces

- $\phi_\alpha : F[x] \rightarrow F[\alpha]$ definida por $\phi_\alpha(f(x)) = f(\alpha)$ para todo $f(x) \in F[x]$, es un homomorfismo de anillos.
- Si $\alpha \in K$ es trascendente sobre F , entonces $F[x]$ y $F[\alpha]$ son dominios de integridad isomorfos.

c) Si $\alpha \in K$ es algebraico sobre F , entonces $F[\alpha]$ es un campo y $F(\alpha) = F[\alpha]$.

Demostración. a) Para demostrar que ϕ_α es un homomorfismo de anillos verificaremos las siguientes condiciones:

i. Sea $f(x), g(x) \in F[x]$, entonces

$$\begin{aligned}\phi_\alpha(f(x) + g(x)) &= \phi_\alpha((f + g)(x)) \\ &= (f + g)(\alpha) \\ &= f(\alpha) + g(\alpha) \\ &= \phi_\alpha(f(x)) + \phi_\alpha(g(x)).\end{aligned}$$

ii. Sea $f(x), g(x) \in F[x]$,

$$\begin{aligned}\phi_\alpha(f(x)g(x)) &= (fg)(x) \\ &= (fg)(\alpha) \\ &= f(\alpha)g(\alpha) \\ &= \phi_\alpha(f(x))\phi_\alpha(g(x)).\end{aligned}$$

b) Si $\alpha \in K$ es trascendente sobre F , lo que implica que no existe un polinomio no nulo $f(x) \in F[x]$ tal que $f(\alpha) = 0$. Luego,

$$\begin{aligned}\ker(\phi_\alpha) &= \{f(x) \in F[x] / \phi_\alpha(f(x)) = 0\} \\ &= \{f(x) \in F[x] / f(\alpha) = 0\} \\ &= \{0\} \text{ dado que } \alpha \text{ es trascendente}\end{aligned}$$

y así, $\phi_\alpha : F[x] \rightarrow F[\alpha]$ es una función inyectiva. Lo que nos queda probar que ϕ_α es sobreyectiva, el recorrido de la función ϕ_α es $F[\alpha] = \{f(\alpha) / f(x) \in F[x]\}$ lo que nos garantiza la sobreyectividad, entonces obtenemos que $F[x]$ y $F[\alpha]$ son dominios de integridad isomorfos.

c) Si $\alpha \in K$ es algebraico sobre F y $p(x)$ es el polinomio irreducible de α sobre F , entonces $p(x)$ es un generador del ideal $J = \{f(x) \in F[x] / f(\alpha) = 0\}$ del anillo $F[x]$. Dado que $J = \ker(\phi_\alpha)$, entonces por el primer Teorema de isomorfía de

anillos, los anillos $F[x]/\langle p(x) \rangle$ e $Im(\phi_\alpha) = F[\alpha]$ son isomorfos. Pero $F[x]/\langle p(x) \rangle$ es campo, dado que $p(x)$ es irreducible sobre F . Por lo tanto, $F[\alpha]$ es un campo. Como $F[\alpha]$ es un campo que contiene a F y α , entonces $F(\alpha) = F[\alpha]$.

□

Ejemplo 3.4. Los campos $\mathbb{R}[x]/\langle x^2 + 1 \rangle$ y \mathbb{C} son isomorfos. Por el teorema anterior, sabemos que la función $\phi_i : \mathbb{R}[x] \rightarrow \mathbb{C}$ para todo $f(x) \in F[x]$ es un homomorfismo de anillos. El núcleo de esta función es el ideal maximal $\langle x^2 + 1 \rangle$ de $\mathbb{R}[x]$ y su recorrido es $\mathbb{R}[i] = \mathbb{R}(i)$. Pero $\mathbb{R}[i] = \mathbb{C}$ por el primer teorema de isomorfismo de anillos, $\mathbb{R}[x]/\langle x^2 + 1 \rangle$ y \mathbb{C} son campos isomorfos.

Teorema 3.4

Sea K una extensión de un campo F , $\alpha \in K$ algebraico sobre F y $p(x) \in F[x]$ el polinomio de α sobre F con $\deg(p) = n$, entonces la extensión $F(\alpha)$ de F es el espacio vectorial sobre F , generado por los vectores $1, \alpha, \dots, \alpha^{n-1}$. Además, $[F(\alpha) : F] = n$.

Demostración. Debemos probar que

$$F(\alpha) = \{a_0 + a_1\alpha + \dots + a_{n-1}\alpha^{n-1} \mid a_0, a_1, \dots, a_{n-1} \in F\}$$

y que los vectores $1, \alpha, \dots, \alpha^{n-1}$ son linealmente independientes sobre F . Definimos por U el conjunto $\{a_0 + a_1\alpha + \dots + a_{n-1}\alpha^{n-1} \mid a_0, a_1, \dots, a_{n-1} \in F\}$. Para demostrar que $F(\alpha) = U$, basta probar que $U = F[\alpha]$. Es evidente que $U \subset F[\alpha]$. Consideremos ahora, $f(\alpha)$ un elemento cualquiera en $F[\alpha]$, donde $f(x) \in F[x]$, por el algoritmo de Euclides $f(x) = q(x)p(x) + r(x)$, donde $r(x) = 0$ ó $\deg(r) < \deg(p) = n$. Luego,

$$r(x) = c_0 + c_1x + \dots + c_{n-1}x^{n-1} \in F[x].$$

Por lo tanto,

$$f(\alpha) = p(\alpha)q(\alpha) + r(\alpha) = r(\alpha) = c_0 + c_1\alpha + \dots + c_{n-1}\alpha^{n-1} \in U,$$

lo que demuestra que $F[\alpha] \subset U$. Así, $F(\alpha) = F[\alpha] = U$.

Para demostrar que $[F(\alpha) : F] = n$, basta probar que $1, \alpha, \dots, \alpha^{n-1}$ son linealmente independientes sobre F . Sea $a_0 + a_1\alpha + \dots + a_{n-1}\alpha^{n-1} = 0$ con $a_0, a_1, \dots, a_{n-1} \in F$. Definiendo el polinomio

$$g(x) = a_0 + a_1x + \dots + a_{n-1}x^{n-1},$$

obtenemos que $g(x)$ es un elemento del ideal J de $F[x]$ tal que $g(x) = p(x)q(x)$. Si suponemos que $g(x) \neq 0$ entonces $\deg(g) \leq n-1$ y además, $\deg(g) = \deg(p) + \deg(q) = n + \deg(p)$, lo cual implica $\deg(g) \geq n$, de donde llegamos a una contradicción. Por lo tanto, $g(x) = a_0 + a_1x + \dots + a_{n-1}x^{n-1} = 0$, de donde $a_0 = a_1 = \dots = a_{n-1} = 0$. Así, los elementos $1, \alpha, \dots, \alpha^{n-1}$ son linealmente independientes sobre F . \square

Nota. Sea K una extensión del campo F y los elementos $\alpha, \beta \in K$ algebraicos sobre F . Entonces del teorema anterior, $F(\alpha)$ es una extensión finita de F y $F(\alpha)(\beta)$ es una extensión finita de $F(\alpha)$. Denotaremos el campo $F(\alpha)(\beta)$ por $F(\alpha, \beta)$.

Teorema 3.5

Sea K una extensión del campo F y $\alpha, \beta \in K$ algebraicos sobre el campo F , entonces $F(\alpha, \beta)$ es una extensión finita de F y además,

$$[F(\alpha, \beta) : F] = [F(\alpha, \beta) : F(\alpha)][F(\alpha) : F].$$

Demostración. $[F(\alpha) : F]$ es finito. Como β es algebraico sobre el campo F , entonces existe un polinomio no nulo $q(x) \in F[x]$ tal que $q(\beta) = 0$. Pero $q(x) \in (F(\alpha))[x]$, luego, β es algebraico sobre $F(\alpha)$ y en consecuencia, $(F(\alpha))(\beta) = F(\alpha, \beta)$ es una extensión finita de $f(\alpha)$. De esta forma tenemos

$$\begin{array}{c} F(\alpha, \beta) \\ | \\ F(\alpha) \\ | \\ F \end{array}$$

Finalmente, dado que $[F(\alpha, \beta) : F(\alpha)]$ y $[F(\alpha) : F]$ son finitos, entonces obtenemos que $[F(\alpha, \beta) : F] = [F(\alpha, \beta) : F(\alpha)][F(\alpha) : F]$ es finito. \square

Observación 3.2. En el caso de que $[F(\alpha) : F] = n$, donde la base de $F(\alpha)$ sobre F es, $\{1, \dots, \alpha^{n-1}\}$, y $\{1, \dots, \beta^{n-1}\}$ es la base de $F(\alpha)(\beta)$ sobre $F(\alpha)$. Así, $\{\beta^i \alpha^j / i \in \{0, \dots, n-1\}, j \in \{0, \dots, n-1\}\}$ es una base de $F(\alpha)(\beta)$ sobre F . Como cada producto $\beta^i \alpha^j \in F(\beta)(\alpha)$, entonces $F(\alpha)(\beta) \subset F(\beta)(\alpha)$. De manera análoga $F(\beta)(\alpha) \subset F(\alpha)(\beta)$. Por lo tanto, $F(\alpha, \beta) = F(\beta, \alpha)$. Ahora, si K es una extensión de un campo F y $\alpha_1, \alpha_2, \dots, \alpha_n \in K$ son algebraicos sobre F , entonces $F(\alpha_1, \alpha_2) = (F(\alpha_1))(\alpha_2)$, $F(\alpha_1, \alpha_2, \alpha_3) = (F(\alpha_1, \alpha_2))(\alpha_3)$ y, en general $F(\alpha_1, \alpha_2, \dots, \alpha_n) = (F(\alpha_1, \alpha_2, \dots, \alpha_{n-1}))(\alpha_n)$. Además, si

$$\sigma : \{1, 2, \dots, n\} \rightarrow \{1, 2, \dots, n\}$$

es una biyección, entonces

$$F(\alpha_1, \alpha_2, \dots, \alpha_n) = F(\alpha_{\sigma(1)}, \alpha_{\sigma(2)}, \dots, \alpha_{\sigma(n)}).$$

Corolario 3.2

Sea K una extensión de un campo F y $\alpha_1, \alpha_2, \dots, \alpha_n \in K$ algebraicos sobre F . Entonces $F(\alpha_1, \alpha_2, \dots, \alpha_n)$ es una extensión finita de F y además, $[F(\alpha_1, \alpha_2, \dots, \alpha_n) : F] = [F(\alpha_1, \alpha_2, \dots, \alpha_n) : F(\alpha_1, \alpha_2, \dots, \alpha_{n-1})] \dots [F(\alpha_1) : F]$.

Demostración. Para su demostración consideramos el método por inducción. Para $n = 1$,

$$[F(\alpha_1) : F] = [F(\alpha_1) : F].$$

Supongamos que el corolario es válido para $n - 1$

$$[F(\alpha_1, \alpha_2, \dots, \alpha_{n-1}) : F] = [F(\alpha_1, \alpha_2, \dots, \alpha_{n-1}) : F(\alpha_1, \alpha_2, \dots, \alpha_{n-2})] \dots [F(\alpha_1) : F].$$

Sabemos que

$$F(\alpha_1, \alpha_2, \dots, \alpha_n) = (F(\alpha_1, \alpha_2, \dots, \alpha_{n-1}))(\alpha_n).$$

Luego, por el Teorema 3.5 tenemos que

$$[F(\alpha_1, \dots, \alpha_{n-1})(\alpha_n) : F] = [F(\alpha_1, \dots, \alpha_{n-1}, \alpha_n) : F(\alpha_1, \dots, \alpha_{n-1})] \dots [F(\alpha_1) : F].$$

□

Teorema 3.6

Si E es una extensión finita de un campo F , entonces existen elementos $\alpha_1, \dots, \alpha_n \in E$ tales que $E = F(\alpha_1, \dots, \alpha_n)$.

Demostración. Si $[E : F] = 1$, entonces $E = F(1) = F$. Si $E \neq F$, entonces existe $\alpha_1 \in E$ tal que $\alpha_1 \notin F$, ya que α_1 es algebraico sobre F , entonces por el teorema anterior $[F(\alpha_1) : F]$ es finito, además los vectores $1, \alpha_1$ son linealmente independientes sobre F , de donde $[F(\alpha_1) : F] > 1$. Si $E = F(\alpha_1)$, entonces existe $\alpha_2 \in E$ tal que $\alpha_2 \notin F(\alpha_1)$ y los vectores $1, \alpha_1, \alpha_2$ son linealmente independientes sobre F y así $[F(\alpha_1, \alpha_2) : F] > 2$, volvemos a considerar que $E = F(\alpha_1, \alpha_2)$ al cumplir esto se obtiene el teorema. Este proceso debe ser finito, caso contrario encontraríamos un conjunto infinito de vectores independientes sobre F , lo que contradice la hipótesis. Finalmente con este proceso, deben existir $\alpha_1, \dots, \alpha_n \in E$ tales que $E = F(\alpha_1, \dots, \alpha_n)$. \square

Teorema 3.7

Si K es una extensión algebraica de un campo E y E es una extensión algebraica de un campo F , entonces K es una extensión algebraica de F .

Demostración. Sea $\alpha \in K$, se pretende demostrar que α es algebraico sobre F . Por hipótesis, K es algebraico sobre E . Luego, existe $g(x)$ en E polinomio no nulo definido como $g(x) = b_0 + b_1x + \dots + b_nx^n$ en E tal que $g(\alpha) = 0$. Como E es algebraico sobre F , los elementos $b_0, b_1, \dots, b_n \in E$ son algebraicos sobre F . Por el Corolario 3.2, $F(b_1, b_2, \dots, b_n)$ es una extensión finita de F . Notemos que $g(x) = b_0 + b_1x + \dots + b_nx^n \in (F(b_1, b_2, \dots, b_n))[x]$ y $g(\alpha) = 0$ por lo tanto, α es algebraico sobre $F(b_1, b_2, \dots, b_n)$. En consecuencia tenemos,

$$\begin{array}{c} F(b_1, b_2, \dots, b_n)(\alpha) \\ | \\ F(b_1, b_2, \dots, b_n) \\ | \\ F \end{array}$$

Finalmente, $[F(b_1, b_2, \dots, b_n)(\alpha) : F(b_1, b_2, \dots, b_n)]$, $[F(b_1, b_2, \dots, b_n) : F]$ finitos, lo que implica que $[F(b_1, b_2, \dots, b_n)(\alpha) : F]$ es finito. Lo que demuestra que α es algebraico sobre F . \square

Ejemplo 3.5. Demostraremos que $[\mathbb{Q}(\sqrt{3}, \sqrt{5}) : \mathbb{Q}] = 4$. Sabemos que $\mathbb{Q}(\sqrt{3}, \sqrt{5}) = (\mathbb{Q}(\sqrt{3}))(\sqrt{5})$. Así tenemos:

$$\begin{array}{c} (\mathbb{Q}(\sqrt{3}))(\sqrt{5}) \\ | \\ \mathbb{Q}(\sqrt{3}) \\ | \\ \mathbb{Q} \end{array}$$

Identificamos el polinomio irreducible de $\sqrt{3}$ sobre \mathbb{Q} es $q(x) = x^2 - 3$. Luego, $\mathbb{Q}(\sqrt{3}) = \{a + b\sqrt{3} / a, b \in \mathbb{Q}\}$.

De manera análoga encontramos el polinomio irreducible de $\sqrt{5}$ es $p(x) = x^2 - 5$. Luego, $\mathbb{Q}(\sqrt{5}) = \{a + b\sqrt{5} / a, b \in \mathbb{Q}\}$.

Para demostrar que $p(x) = x^2 - 5$ es irreducible sobre $\mathbb{Q}(\sqrt{3})$ basta probar que $p(x) = x^2 - 5$ no tiene raíces en $\mathbb{Q}(\sqrt{3})$. Supongamos que $a + b\sqrt{3}$ con $a, b \in \mathbb{Q}$ es una raíz de $p(x) = x^2 - 5$. Entonces

$$\begin{aligned} p(a + b\sqrt{3}) &= (a + b\sqrt{3})^2 - 5 = 0 \\ &(a^2 + 2ab\sqrt{3} + 3b^2 - 5) = 0. \end{aligned}$$

Como $1, \sqrt{3}$ son linealmente independientes sobre \mathbb{Q} , entonces $a^2 + 3b^2 - 5 = 0$ y $2ab = 0$. Ahora, si $a = 0$, entonces $b^2 = \frac{5}{3}$. Si $b = 0$, entonces $a^2 = 5$. En ambos casos se obtiene una contradicción. Por lo tanto, $p(x) = x^2 - 5$ es polinomio irreducible de $\sqrt{5}$ sobre $\mathbb{Q}(\sqrt{3})$ y así, $[(\mathbb{Q}(\sqrt{3}))(\sqrt{5}) : \mathbb{Q}(\sqrt{3})] = 2$.

Dado que $\{1, \sqrt{3}\}$ es una base de $\mathbb{Q}(\sqrt{3})$ como espacio vectorial sobre \mathbb{Q} y $\{1, \sqrt{5}\}$ es una base de $(\mathbb{Q}(\sqrt{3}))(\sqrt{5})$ como espacio vectorial sobre $\mathbb{Q}(\sqrt{3})$. Luego,

$$\begin{aligned} [\mathbb{Q}(\sqrt{3}, \sqrt{5}) : \mathbb{Q}] &= [\mathbb{Q}(\sqrt{3}, \sqrt{5}) : \mathbb{Q}(\sqrt{3})][\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] \\ &= (2)(2) \\ &= 4 \end{aligned}$$

Además, $\{1, \sqrt{3}, \sqrt{5}, \sqrt{15}\}$ es una base de $(\mathbb{Q}(\sqrt{3}))(\sqrt{5})$ como espacio vectorial sobre \mathbb{Q} .

Ejemplo 3.6. Vamos a demostrar a continuación que $[\mathbb{Q}(\sqrt{3}, \sqrt{5}) : \mathbb{Q}\sqrt{15}] = 2$. Debido a que $\sqrt{3}, \sqrt{5}$ son elementos del campo $\mathbb{Q}(\sqrt{3}, \sqrt{5})$, entonces $\sqrt{15} = \sqrt{3}\sqrt{5} \in \mathbb{Q}(\sqrt{3}, \sqrt{5})$. De esta manera $\mathbb{Q}(\sqrt{15})$ es un subcampo de $\mathbb{Q}(\sqrt{3}, \sqrt{5})$. Ahora,

$$\begin{array}{c} (\mathbb{Q}(\sqrt{3}))(\sqrt{5}) \\ | \\ \mathbb{Q}(\sqrt{15}) \\ | \\ \mathbb{Q} \end{array}$$

El polinomio $p(x) = x^2 - 15$ no tiene raíces en \mathbb{Q} y $\deg(p) = 2$, lo que implica que $p(x)$ es el polinomio irreducible de $\sqrt{15}$ sobre \mathbb{Q} . Por lo tanto $[\mathbb{Q}(\sqrt{15}) : \mathbb{Q}] = 2$. Luego, a partir de que

$$[\mathbb{Q}(\sqrt{3}, \sqrt{5}) : \mathbb{Q}(\sqrt{15})][\mathbb{Q}(\sqrt{15}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{3}, \sqrt{5}) : \mathbb{Q}] = 4$$

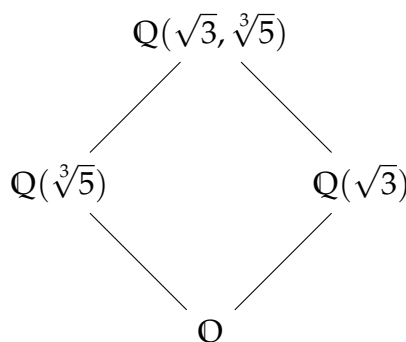
obtenemos que $[\mathbb{Q}(\sqrt{3}, \sqrt{5}) : \mathbb{Q}\sqrt{15}] = 2$.

Ejemplo 3.7. Demostraremos ahora que $\mathbb{Q}(\sqrt{3}, \sqrt{5}) = \mathbb{Q}(\sqrt{3} + \sqrt{5})$. Claramente $\sqrt{3} + \sqrt{5}$ y luego, $\mathbb{Q}(\sqrt{3} + \sqrt{5})$ es un subcampo de $\mathbb{Q}(\sqrt{3}, \sqrt{5})$. Como $[\mathbb{Q}(\sqrt{3} + \sqrt{5}) : \mathbb{Q}] = 4$, y $[\mathbb{Q}(\sqrt{3}, \sqrt{5}) : \mathbb{Q}] = 4$, entonces

$$[\mathbb{Q}(\sqrt{3}, \sqrt{5}) : \mathbb{Q}(\sqrt{3} + \sqrt{5})] = 1.$$

Por lo tanto, $\mathbb{Q}(\sqrt{3}, \sqrt{5}) = \mathbb{Q}(\sqrt{3} + \sqrt{5})$.

Ejemplo 3.8. En este ejemplo demostraremos que $\mathbb{Q}(\sqrt{3}, \sqrt[3]{5})$ es una extensión finita de \mathbb{Q} de grado 6. Sabemos que $\mathbb{Q}(\sqrt{3}, \sqrt[3]{5}) = \mathbb{Q}(\sqrt{3})(\sqrt[3]{5}) = \mathbb{Q}(\sqrt[3]{5})(\sqrt{3})$. Así,



Como ya vimos en los ejemplos anteriores el polinomio irreducible de $\sqrt{3}$ sobre \mathbb{Q} es $q(x) = x^2 - 3$ y el polinomio irreducible de $\sqrt[3]{5}$ sobre \mathbb{Q} es $q(x) = x^3 - 5$. Ya que $\sqrt{2}$ y $\sqrt[3]{5}$ son algebraicos sobre \mathbb{Q} , por el Teorema 3.5, $\mathbb{Q}(\sqrt{3}, \sqrt[3]{5})$ es una extensión finita de \mathbb{Q} . Utilizando el Teorema 3.1, obtenemos que 2 y 3 son divisores de $[\mathbb{Q}(\sqrt{3}, \sqrt[3]{5}) : \mathbb{Q}]$. Por lo tanto, $[\mathbb{Q}(\sqrt{3}, \sqrt[3]{5}) : \mathbb{Q}(\sqrt{3})] \geq 6$.

El polinomio $q(x) = x^3 - 5 \in \mathbb{Q}(\sqrt{3})[x]$ se anula en $\sqrt[3]{5}$. Por lo que el polinomio irreducible de $\sqrt[3]{5}$ sobre $\mathbb{Q}(\sqrt{3})$ es un divisor de $q(x)$. Por lo tanto, $[\mathbb{Q}(\sqrt[3]{5})(\sqrt{3}) : \mathbb{Q}(\sqrt{3})] \leq 3$.

Finalmente a partir del Teorema 3.1 concluimos que

$$[\mathbb{Q}(\sqrt{3}, \sqrt[3]{5}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[3]{5}, \sqrt{3}) : \mathbb{Q}(\sqrt{3})][\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] \leq 6.$$

Por lo tanto, $[\mathbb{Q}(\sqrt{3}, \sqrt[3]{5}) : \mathbb{Q}] = 6$. Además, obtenemos que $q(x) = x^3 - 5$ el cual es el polinomio irreducible de $\sqrt[3]{5}$ sobre $\mathbb{Q}(\sqrt{3})$. Así, $\{1, \sqrt[3]{5}, \sqrt[3]{25}\}$ es una base de $\mathbb{Q}(\sqrt{3}, \sqrt[3]{5})$ sobre $\mathbb{Q}(\sqrt{3})$. Ya que $\{1, \sqrt{3}\}$ es una base de $\mathbb{Q}(\sqrt{3})$ sobre \mathbb{Q} , conseguimos que $\{1, \sqrt[3]{5}, \sqrt[3]{25}, \sqrt{3}, \sqrt{3}\sqrt[3]{5}, \sqrt{3}\sqrt[3]{25}\}$ es una base de $\mathbb{Q}(\sqrt{3}, \sqrt[3]{5})$ sobre \mathbb{Q} .

3.3 Raíces de polinomios irreducibles

Si F es un subcampo de \mathbb{C} y $p(x) \in F[x]$ un polinomio irreducible sobre F de grado n , entonces existe una extensión E de F tal que $[E : F] = n$ y existe $\alpha \in E$ tal que $p(\alpha) = 0$. Por el Teorema fundamental del Álgebra 2.4 sabemos que existe una raíz $\alpha \in \mathbb{C}$ de $p(x)$. Además, $F(\alpha) = E$ es una extensión finita de F de grado n .

Teorema 3.8 (Teorema de Kronecker)

Sea F un campo y $p(x) \in F[x]$ un polinomio irreducible sobre F con $\deg(p) = n$. Entonces el campo $E = F[x]/\langle p(x) \rangle$ es una extensión finita de F tal que $[E : F] = n$ y existe $\alpha \in E$ tal que $p(\alpha) = 0$. Además, $F(\alpha) = E$.

Demostración. Por hipótesis sabemos que el polinomio $p(x)$ es irreducible sobre F , entonces el anillo cociente $E = F[x]/\langle p(x) \rangle$ es un campo. La función $\sigma : F \rightarrow F[x]/\langle p(x) \rangle$ claramente es un monomorfismo de anillos. Para su demostración necesitamos verificar las siguientes propiedades:

- Sea $a, b \in F$ entonces $\sigma(a + b) = \sigma(a) + \sigma(b)$,

$$\begin{aligned}\sigma(a + b) &= a + b + \langle p(x) \rangle \\ &= (a + \langle p(x) \rangle) + (b + \langle p(x) \rangle) \text{ por las propiedades del anillo cociente} \\ &= \sigma(a) + \sigma(b).\end{aligned}$$

- Sea $a, b \in F$ entonces $\sigma(ab) = \sigma(a)\sigma(b)$,

$$\begin{aligned}\sigma(ab) &= ab + \langle p(x) \rangle \\ &= (a + \langle p(x) \rangle)(b + \langle p(x) \rangle) \text{ por las propiedades del anillo cociente} \\ &= \sigma(a)\sigma(b).\end{aligned}$$

- **Iyectividad**

$$\begin{aligned}\ker(\sigma) &= \{a \in F / \sigma(a) = a + \langle p(x) \rangle\} \\ &= \{a \in F / a + \langle p(x) \rangle = \langle p(x) \rangle\} \\ &= \{a \in F / a = p(x)q(x)\}, \text{ donde claramente } q(x) = 0 \\ &= \{0\}.\end{aligned}$$

Verificando ya que σ es un monomorfismo podemos tomar un elemento cualquiera $a \in F$ con $a + \langle p(x) \rangle \in E$ y se puede escribir como $a = a + \langle p(x) \rangle$, lo que nos lleva a decir que E es una extensión de F .

Luego, demostraremos que E es una extensión finita de grado n sobre F . Por el Lema 2.4, sabemos que

$$E = \{a_0 + a_1(x) + \cdots + a_{n-1}x^{n-1} / a_0, \dots, a_{n-1} \in F\}.$$

Es evidente que los vectores $1 + \langle p(x) \rangle, x + \langle p(x) \rangle, \dots, x^{n-1} + \langle p(x) \rangle$ son generadores de E como espacio vectorial sobre F . Además, los vectores antes definidos son linealmente independientes sobre F . Si suponemos que

$$a_0(1 + \langle p(x) \rangle) + a_1(x + \langle p(x) \rangle) \cdots + a_{n-1}(x^{n-1} + \langle p(x) \rangle) = 0 + \langle p(x) \rangle,$$

donde $a_0, a_1, \dots, a_{n-1} \in F$, entonces

$$a_0 + a_1x + \cdots + a_{n-1}x^{n-1} + \langle p(x) \rangle = 0 + \langle p(x) \rangle,$$

de donde $a_0 + a_1x + \cdots + a_{n-1}x^{n-1} \in \langle p(x) \rangle$. Sabemos que el $\deg(p) = n$, necesariamente $a_0 + a_1x + \cdots + a_{n-1}x^{n-1} = 0$, lo cual implica que $a_0 = a_1 = \cdots = a_{n-1} = 0$. Por lo tanto, E es una extensión finita de F y $[E : F] = n$.

Supongamos que $p(x) = b_0 + b_1(x) + \cdots + b_nx^n \in F[x]$. Entonces $\alpha = x + \langle p(x) \rangle$ es una raíz de $p(x)$. En efecto,

$$\begin{aligned} p(\alpha) &= b_0 + b_1(x) + (x + \langle p(x) \rangle) + \cdots + b_n(x + \langle p(x) \rangle)^n \\ &= b_0 + b_1(x) + (x + \langle p(x) \rangle) + \cdots + b_n(x^n + \langle p(x) \rangle) \\ &= b_0 + b_1(x) + \cdots + b_nx^n + \langle p(x) \rangle \\ &= p(x) + \langle p(x) \rangle = 0 + \langle p(x) \rangle = 0. \end{aligned}$$

Finalmente, ya que $[F(\alpha) : F] = n$, $[E : F] = n$ y $F(\alpha)$ es un subcampo de E , entonces $F(\alpha) = E$. □

Corolario 3.3

Sea F un campo y el polinomio $f(x) \in F[x]$ no constante. Entonces existe una extensión finita E de F con $[E : F] \leq \deg(f)$ y $\alpha \in E$ tal que $f(\alpha) = 0$.

Demostración. Sabemos por hipótesis que $f(x)$ es irreducible sobre F o $f(x)$ se puede escribir como el producto de dos polinomios irreducibles sobre F . Sea $p(x)$

un factor irreducible de $f(x)$. Por el teorema previo existe una extensión finita E de F tal que $[E : F] = \deg(p)$ y $\alpha \in E$ tal que $p(\alpha) = 0$. Claramente $\alpha \in E$ es una raíz de $f(x)$ y $[E : F] \leq \deg(f)$. \square

Ejemplo 3.9. Sea $f(x) = x^4 - 9x^2 + 14 \in \mathbb{Q}[x]$. Construiremos una extensión E de \mathbb{Q} , donde $f(x)$ tenga una raíz. Notemos que $f(x) = (x^2 - 7)(x^2 - 2)$ no tiene raíces en \mathbb{Q} . El polinomio $p(x) = x^2 - 7 \in \mathbb{Q}[x]$ es un factor de $f(x)$, irreducible sobre \mathbb{Q} . Luego, por el Corolario 2.4 el cociente $E = \mathbb{Q}[x]/\langle x^2 - 7 \rangle$ es un campo. Además, E es una extensión finita de \mathbb{Q} , $[E : \mathbb{Q}] = \deg(x^2 - 7)$ y $\alpha = x + \langle x^2 - 7 \rangle \in E$ es una raíz del polinomio $x^2 - 7 \in \mathbb{Q}[x]$. Por lo tanto, α también es una raíz de $f(x)$.

Ejemplo 3.10. El polinomio $p(x) = x^2 + 2x + 2 \in \mathbb{Z}_3[x]$ es irreducible sobre \mathbb{Z}_3 . Por lo tanto, $\langle p(x) \rangle$ es un ideal maximal del anillo $\mathbb{Z}_3[x]$ y en consecuencia, el anillo $E = \mathbb{Z}_3[x]/\langle p(x) \rangle$ es un campo. La función $\sigma : \mathbb{Z}_3 \rightarrow E$ definida por $\sigma(a) = a + \langle p(x) \rangle$, es un monomorfismo de anillos. Así, podemos identificar $a \in \mathbb{Z}_3$ con $a + \langle p(x) \rangle \in E$ y escribir $a = a + \langle p(x) \rangle$.

Sabemos que

$$\begin{aligned} E &= \{a + bx + \langle p(x) \rangle \mid a, b \in \mathbb{Z}_3\} \\ &= \{0 + \langle p(x) \rangle, 1 + \langle p(x) \rangle, x + \langle p(x) \rangle, 2 + \langle p(x) \rangle, 2x + \langle p(x) \rangle, 1 + x + \langle p(x) \rangle, \\ &\quad 1 + 2x + \langle p(x) \rangle, x + 2 + \langle p(x) \rangle, 2 + 2x + \langle p(x) \rangle\}. \end{aligned}$$

De acuerdo a la demostración del teorema anterior $\alpha = x + \langle p(x) \rangle$ es raíz de $p(x)$ y por lo tanto $\alpha^2 + 2\alpha + 2 = 0$. Así, $\alpha^2 = -2\alpha - 2 = \alpha + 1$. Luego, $E = \{0, 1, \alpha, 2, 2\alpha, 1 + \alpha, 1 + 2\alpha, \alpha + 2, 2 + 2\alpha\}$. De esta manera hemos construido un campo de 9 elementos,

(+)	0	1	2	α	2α	$\alpha + 1$	$2\alpha + 1$	$\alpha + 2$	$2\alpha + 2$
0	0	1	2	α	2α	$\alpha + 1$	$2\alpha + 1$	$\alpha + 2$	$2\alpha + 2$
1	1	2	0	$\alpha + 1$	$2\alpha + 1$	$\alpha + 2$	$2\alpha + 2$	α	2α
2	2	0	1	$2 + \alpha$	$2\alpha + 2$	α	2α	$\alpha + 1$	$2\alpha + 1$
α	α	$1 + \alpha$	$\alpha + 2$	2α	0	$2\alpha + 1$	1	$2\alpha + 2$	2
2α	2α	$2\alpha + 1$	$2\alpha + 2$	0	α	1	$\alpha + 1$	2	$\alpha + 2$
$\alpha + 1$	$\alpha + 1$	$\alpha + 2$	α	$2\alpha + 1$	1	$2\alpha + 2$	2	2α	0
$2\alpha + 1$	$2\alpha + 1$	$2\alpha + 2$	2α	1	$\alpha + 1$	2	$\alpha + 2$	0	α
$\alpha + 2$	$\alpha + 2$	α	$\alpha + 1$	$2\alpha + 2$	2	α	0	$2\alpha + 1$	1
$2\alpha + 2$	$2\alpha + 2$	2α	$2\alpha + 1$	2	$\alpha + 2$	0	α	1	$\alpha + 1$

De manera análoga sucede con el producto.

3.4 Clausuras Algebraicas

En esta sección demostraremos que el conjunto

$$\bar{\mathbb{Q}} = \{\alpha \in \mathbb{C} \mid \alpha \text{ es algebraico sobre } \mathbb{Q}\}.$$

Teorema 3.9

Sea E una extensión de un campo F . Entonces el conjunto

$$\bar{F}_E = \{\alpha \in E \mid \alpha \text{ es algebraico sobre } F\}$$

es un subcampo de E , llamado la clausura algebraica de F en E .

Demostración. Sean $\alpha, \beta \in \bar{F}_E$. Debido a que α, β son algebraicos sobre F , entonces por el Teorema 3.5 $F(\alpha, \beta)$ es una extensión finita de F , por lo tanto por el Teorema 3.2 $F(\alpha, \beta)$ es una extensión algebraica de F , de donde $F(\alpha, \beta) \subset \bar{F}_E$. Así, $-\alpha, \alpha\beta, \alpha + \beta$ y también α^{-1} para $\alpha \neq 0$, con todos elementos en $F(\alpha, \beta) \subset \bar{F}_E$. De esta manera ya que \bar{F}_E es un campo y subconjunto de E , entonces es un subcampo de E . □

Observación 3.3. Es claro que \bar{F}_E , cuando E es una extensión algebraica de un campo F , esta situación se tiene cada vez que E es una extensión finita.

Teorema 3.10

La clausura algebraica de \mathbb{Q} en \mathbb{C} es un campo algebraicamente cerrado.

Demostración. Debemos probar que el campo $\mathbb{Q}_{\mathbb{C}} = \{\alpha \in \mathbb{C} / \alpha \text{ es algebraico sobre } \mathbb{Q}\}$ es algebraicamente cerrado. Denotemos $\bar{\mathbb{Q}} = \bar{\mathbb{Q}}_{\mathbb{C}}$ y sea $f(x) = a_0 + a_1x + \dots + a_nx^n \in \mathbb{Q}[x]$ con $\deg(f) = n \geq 1$. Por el teorema Fundamental del Álgebra, existe un elemento $\alpha \in \bar{\mathbb{Q}}$. Ya que a_0, a_1, \dots, a_n son algebraicos sobre \mathbb{Q} , entonces $\mathbb{Q}(a_0, a_1, \dots, a_n)$ es una extensión finita sobre \mathbb{Q} y en consecuencia, $\mathbb{Q}(a_0, \dots, a_n)$ es una extensión algebraica sobre \mathbb{Q} . Ahora, $f(x) \in \mathbb{Q}(a_0, \dots, a_n)[x]$ con $F(\alpha) = 0$, es decir, α es algebraico sobre $\mathbb{Q}(a_0, \dots, a_n)$. Luego, $\mathbb{Q}(a_0, \dots, a_n, \alpha)$ es una extensión algebraica sobre $\mathbb{Q}(a_0, \dots, a_n)$, Ya que $\mathbb{Q}(a_0, \dots, a_n, \alpha)$ es una extensión algebraica de $\mathbb{Q}(a_0, \dots, a_n)$ y $\mathbb{Q}(a_0, \dots, a_n)$ es una extensión algebraica sobre \mathbb{Q} , es decir, haciendo uso del Teorema 3.7, entonces $\mathbb{Q}(a_0, \dots, a_n, \alpha)$ es una extensión algebraica sobre \mathbb{Q} de donde α es algebraico sobre \mathbb{Q} . Por lo tanto hemos demostrado que $\alpha \in \bar{\mathbb{Q}}$. \square

3.5 Derivada de un polinomio

Definición 3.11

Sea F un campo y $f(x) = a_0 + a_1x + \dots + a_ix^i + \dots + a_nx^n$ un polinomio $f(x)$, denotado por $f'(x)$ es el polinomio,

$$f'(x) = a_1 + \dots + ia_ix^{i-1} + \dots + na_nx^{n-1}$$

en $F[x]$.

Observación 3.4. Si $f(x)$ es un polinomio con coeficientes reales tal que $f'(x) = 0$, entonces $f(x)$ es una constante. Esto no siempre sucede ya que cuando se considera un polinomio con coeficientes en un campo cualquiera. Por ejemplo, si p es primo y $f(x) = x^p \in \mathbb{Z}_p[x]$, entonces $f'(x) = px^{p-1}$ es el polinomio nulo.

Lema 3.2

Sea F un campo, $f(x), g(x) \in F[x]$ y $\alpha \in F$.

- a) Si $h(x) = f(x) + g(x)$, entonces $h'(x) = f'(x) + g'(x)$.
- b) Si $h(x) = \alpha f(x)$, entonces $h'(x) = \alpha f'(x)$.
- c) Si $h(x) = f(x)g(x)$, entonces $h'(x) = f'(x)g(x) + f(x)g'(x)$.
- d) Si $h(x) = f(x)^m$ para $m \in \mathbb{Z}^+$, entonces $h'(x) = mf(x)^{m-1}f'(x)$.

Demostración. a) Sea $f(x) = a_0 + a_1x + \dots + a_ix^i + \dots + a_nx^n$ y $g(x) = b_0 + b_1x + \dots + b_ix^i + \dots + b_mx^m$ con $n \leq m$. Luego,

$$\begin{aligned} h(x) &= f(x) + g(x) \\ &= (a_0 + a_1 + \dots + a_ix^i + \dots + a_nx^n) + (b_0 + b_1 + \dots + b_ix^i + \dots + b_mx^m) \\ &= (a_0 + b_0) + (a_1 + b_1)x + \dots + (a_i + b_i)x^i + \dots + (a_n + b_n)x^n + \dots + b_mx^m \\ h'(x) &= (a_1 + b_1) + \dots + i(a_i + b_i)x^{i-1} + \dots + n(a_n + b_n)x^{n-1} + \dots + mb_mx^{m-1} \\ &= (a_1 + \dots + ia_ix^{i-1} + \dots + na_nx^{n-1}) + (b_1 + \dots + ib_ix^{i-1} + \dots + mb_mx^{m-1}) \\ &= f'(x) + g'(x) \end{aligned}$$

b)

$$\begin{aligned} h(x) &= \alpha f(x) \\ &= \alpha(a_0 + a_1x + \dots + a_ix^i + \dots + a_nx^n) \\ &= \alpha a_0 + \alpha a_1x + \dots + \alpha a_ix^i + \dots + \alpha a_nx^n \\ h'(x) &= \alpha a_1 + \dots + \alpha ia_ix^{i-1} + \dots + \alpha na_nx^{n-1} \\ &= \alpha(a_1 + \dots + ia_ix^{i-1} + \dots + na_nx^{n-1}) \\ &= \alpha f'(x) \end{aligned}$$

c) Para la demostración de este ítem solo es suficiente demostrar el resultado en el caso muy especial $f(x) = x^n$ y $g(x) = x^m$, donde n, m son enteros positivos.

Entonces $h(x) = x^{n+m}$, de donde $h'(x) = (n+m)x^{n+m-1}$. Por otro lado

$$\begin{aligned}f'(x)g(x) + f(x)g'(x) &= nx^{n-1} + mx^{m-1} \\ &= nx^{n+m-1} + mx^{n+m-1}. \\ &= (n+m)x^{n+m-1}\end{aligned}$$

Por lo tanto, $h'(x) = f'(x)g(x) + f(x)g'(x)$.

d) Partiremos por inducción, consideramos primero para $m = 1$, la función $h(x) = f(x)^1$ es simplemente $h(x) = f(x)$. La derivada de $h(x)$ es entonces $h'(x) = f'(x)$, que coincide con $mf(x)^{m-1}f'(x)$ para $m = 1$.

Supongamos que la regla es válida para $m = k$, es decir, si $h(x) = f(x)^k$, entonces $h'(x) = kf(x)^{k-1}f'(x)$.

Ahora consideremos el caso $m = k + 1$.

$$h(x) = f(x)^{k+1} = f(x)^k \cdot f(x).$$

Aplicando la regla del producto, la derivada de $h(x)$ es:

$$h'(x) = (f(x)^k)' \cdot f(x) + f(x)^k \cdot (f(x))'.$$

Usando la hipótesis de inducción, sabemos que $(f(x)^k)' = kf(x)^{k-1}f'(x)$. Sustituyendo esta expresión en la derivada de $h(x)$, obtenemos:

$$h'(x) = k \cdot f(x)^{k-1} \cdot f'(x) \cdot f(x) + f(x)^k \cdot f'(x).$$

Factorizando $f(x)^{k-1}$ y $f'(x)$, obtenemos:

$$h'(x) = (k \cdot f(x)^{k-1} \cdot f'(x) + f(x)^k \cdot f'(x)).$$

Finalmente, podemos escribir $h'(x)$ en la forma deseada:

$$h'(x) = (k+1) \cdot f(x)^k \cdot f'(x).$$

□

Teorema 3.11

Sea F un campo, \bar{F} la clausura algebraica de F , $f(x)$ un polinomio en $F[x]$ de grado ≥ 1 y $\alpha \in \bar{F}$ una raíz de $f(x)$. Entonces la multiplicidad de α es mayor que 1, si y sólo si $f'(\alpha) = 0$.

Demostración. \Rightarrow) Supongamos que $f(x) = (x - \alpha)^m g(x)$, donde $g(x) \in F[x]$, $g(\alpha) \neq 0$ y $m > 1$. Entonces $f'(x) = m(x - \alpha)^{m-1}g(x) + (x - \alpha)^m g'(x)$ con $m - 1 \geq 1$. Luego, reemplazando x por α tenemos,

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

\Leftarrow) Sea $f(x) = (x - \alpha)^m g(x)$, donde $g(x) \in \bar{F}[x]$, $g(\alpha) \neq 0$ y $f'(\alpha) = 0$. Si $m = 1$, entonces $f'(x) = g(x) + (x - \alpha)g'(x)$. Luego, $f'(\alpha) = g(\alpha) \neq 0$ lo que es una contradicción. Por lo tanto, necesariamente $m > 1$. \square

Corolario 3.4

Dado un subcampo F de los números complejos y $p(x) \in F[x]$ un polinomio mónico irreducible sobre F . Si $\deg(p) = n$, entonces $p(x)$ tiene n raíces distintas en \mathbb{C} .

Demostración. Dado que $p(x) \in \mathbb{C}[x]$, existen n raíces de $p(x)$ en \mathbb{C} . Luego, lo que tenemos que demostrar es que la multiplicidad de cada raíz de $p(x)$ en \mathbb{C} es 1. Ahora, suponemos que $n > 1$. Sea $\alpha \in \mathbb{C}$ una raíz de $p(x)$. Entonces $p(x)$ es el polinomio irreducible de α sobre F . Si suponemos que la multiplicidad de α es $m > 1$, entonces $p'(\alpha) = 0$. Pero $p'(x) \in F[x]$ y $\deg(p') = n - 1 \geq 1$. De esta manera obtenemos que $p'(x) \in \langle p(x) \rangle$, de donde $\deg(p') \geq \deg(p)$, una contradicción. Por lo tanto, $m = 1$. \square

3.6 Campos Finitos

Teorema 3.12

Sea F un campo finito con q elementos y K una extensión finita F de grado n . Entonces K tiene q^n elementos.

Demostración. Sea $\{\alpha_1, \dots, \alpha_n\}$ una base de K como espacio vectorial sobre F . Entonces, todo elemento en K tiene una única representación de la forma $c_1\alpha_1 + \dots + c_n\alpha_n$, donde c_1, \dots, c_n son elementos en F . Como cada coeficiente $c_i \in F$ puede ser cualquiera de los q elementos de F , entonces debe tener q^n elementos. \square

Corolario 3.5

Si K es un campo finito, entonces K tiene p^n elementos, donde p es la característica de K y n es algún entero positivo.

Demostración. Dado que K es un campo finito, entonces la característica de K es un número primo p y K contiene un subcampo F isomorfo a \mathbb{Z}_p . Luego, F tiene p elementos. Como K es una extensión finita de F , existe $n \in \mathbb{Z}^+$ tal que $[K : F] = n$. Por el teorema anterior obtenemos que K tiene p^n elementos. \square

Lema 3.3

Si un campo K tiene p^n elementos, entonces $a^{p^n} = a$ para todo $a \in K$.

Demostración. Si $a = 0$ entonces la afirmación es válida. Ya que el conjunto $F^* = F - 0$ es un grupo con $p^n - 1$ elementos bajo la multiplicación de F , entonces de la teoría de grupos obtenemos que $a^{p^n - 1} = 1$ para todo $a \in F^*$. Multiplicando esta última relación por a , obtenemos $a^{p^n} = a$ \square

Lema 3.6

Si un campo K tiene un p^n elementos, entonces el polinomio $f(x) = x^{p^n} - x \in K[x]$ se factoriza en $K[x]$ como $f(x) = (x - a_1) \cdots (x - a_{p^n})$,

donde $K = \{a_1, \dots, a_{p^n}\}$.

Demostración. Por el Teorema 2.3, $f(x)$ tiene a lo más p^n raíces en K y por el lema anterior, a_1, \dots, a_{p^n} son todas las raíces en K de $f(x)$. Ya que $x - a_1$ es un factor de $f(x)$, entonces existe $q_1(x) \in K[x]$ tal que $f(x) = (x - a_1)q_1(x)$ con $\deg(q_1) = p^n - 1$. Ahora, $q_1(a_i) = 0$ para todo $i \in \{2, \dots, p^n\}$ y además, $q_1(a_1) \neq 0$, de lo contrario $q_1(x)$ tendría p^n raíces en K , contradiciendo el Teorema 2.3. Como $q_1(a_2) = 0$, entonces existe $q_2(x) \in K[x]$ tal que $q_1(x) = (x - a_2)q_2(x)$ con $\deg(q_2) = p^n - 2$, $q_2(a_i) = 0$ para todo $i \in \{3, \dots, p^n\}$ y $q_2(a_2) \neq 0$. Por lo tanto, $f(x) = (x - a_1)(x - a_2)q_2(x)$. Continuando con este proceso, obtenemos que $f(x) = (x - a_1) \cdots (x - a_{p^n})q_{p^n}(x)$, lo cual implica que $q_{p^n}(x) = 1$. \square

Teorema 3.13

Para todo número primo p y todo entero positivo n , existe un campo con p^n elementos.

Demostración. Consideramos el campo \mathbb{Z}_p y el polinomio $f(x) = x^{p^n} - x \in \mathbb{Z}_p[x]$. El polinomio $f(x)$ tiene todas sus raíces en la clausura algebraica $\bar{\mathbb{Z}}_p$ de \mathbb{Z}_p .

Sea $K = \{\alpha \in \bar{\mathbb{Z}}_p \mid \alpha^{p^n} = \alpha\}$. Demostraremos que K es un campo con p^n elementos, para esto haremos uso del Lema 1.3 para probar que K es un subcampo de $\bar{\mathbb{Z}}_p$. Es evidente que 0 y 1 son elementos en K , esto se verifica de la siguiente manera. Para 0 se tiene $0^{p^n} - 0 = 0 - 0 = 0$, además de que cumple con la condición de $\alpha^{p^n} = \alpha$. Por lo tanto, 0 es una raíz de $f(x)$ y $0 \in K$. De manera análoga sucede con 1, se tiene $1^{p^n} - 1 = 1 - 1 = 0$, que también satisface la condición $\alpha^{p^n} = \alpha$. Por lo tanto, 1 es una raíz de $f(x)$ y así verificamos que 0 y 1 están en K .

Sean $\alpha, \beta \in K$. Entonces $\alpha^{p^n} = \alpha$ y $\beta^{p^n} = \beta$. Ahora,

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

Ya que la característica de \mathbb{Z}_p es p y p es un divisor de $\binom{p^n}{k}$ para todo entero k con $1 \leq k < p^n$, entonces

$$\sum_{k=1}^{p^n-1} \binom{p^n}{k} \alpha^{p^n-k} (-\beta)^k = 0$$

y por lo tanto

$$(\alpha - \beta)^{p^n} = \alpha^{p^n} + (-1)^{p^n} \beta^{p^n} = \alpha + (-1)^{p^n} \beta.$$

Si p^n es impar, entonces $(\alpha - \beta)^{p^n} = \alpha - \beta$. Ahora, en el caso de p^n es par, entonces $p = 2$ y ya que $-1 \equiv 1 \pmod{2}$, obtenemos $(\alpha - \beta)^{p^n} = \alpha - \beta$. Por lo tanto, $\alpha - \beta \in K$. Dado que $(\alpha\beta)^{p^n} = \alpha^{p^n} \beta^{p^n} = \alpha\beta$, entonces $\alpha\beta \in K$.

Sea $\alpha \in K$ con $\alpha \neq 0$, entonces $(\alpha^{-1})^{p^n} = (\alpha^{p^n})^{-1} = \alpha^{-1}$, lo cual demuestra que $\alpha^{-1} \in K$. De esta manera, hemos probado que K es un campo. Finalmente, ya que $f'(x) = p^n x^{p^n-1} - 1 = -1$, según el Teorema 3.12, las raíces de $f(x)$ son todas distintas y así, K tiene p^n elementos. \square

4

Teoría de Galois

Al hablar de la teoría de Galois hacemos referencia a una colección de resultados que conectan la teoría de campos con la teoría de grupos. La teoría de Galois fue creada por el matemático Évariste Galois (1811-1832). El nacimiento de dicha teoría surgió como respuesta a la pregunta, ¿por qué no existe una fórmula general para la resolución de ecuaciones algebraicas de grado mayor o igual a cinco en términos de coeficientes del polinomio, usando operaciones algebraicas y la extracción de raíces cuadradas, cúbicas, etc?.

Évariste Galois considerado como un genio matemático, en el transcurso de su corta vida solo pudo ver publicados cinco de sus trabajos matemáticos. Sus inicios en lo que es la teoría de ecuaciones, empezó al presentar dos artículos a la Academia de Ciencias sobre la solución de ecuaciones algebraicas. El interés por esta teoría se reforzó al descubrir que sus trabajos incluían resultados ya demostrados por Abel, a partir de esto, redactó un nuevo artículo, donde plantea las condiciones para que una ecuación sea soluble por radicales. Empezó a trabajar, intentando encontrar una fórmula que diera como resultado las raíces de un polinomio de quinto grado. Galois asoció a un polinomio el grupo de permutaciones de sus raíces, el cual lleva su nombre, grupo de Galois en su honor.

El resultado principal de este capítulo es el Teorema Fundamental de la Teoría de Galois, el cual demuestra la existencia de una estrecha relación entre grupo asociado a $f(x) \in F[x]$ y un grupo asociado llamado el grupo de Galois de $f(x)$.

4.1 Introducción

Para iniciar este capítulo primero empezaremos con un ejemplo el cual será la pequeña iniciativa para el estudio de esta teoría.

Definición 4.1

Sea F un campo y $p(x) = a_0 + a_1x + \dots + a_nx^n \in F[x]$ un polinomio no constante. Una extensión de campos E de F es un campo de descomposición de $p(x)$ si existen $\alpha_1, \dots, \alpha_n$ en E tales que

- $E = F(\alpha_1, \dots, \alpha_n)$
- $f(x) = a \prod (x - \alpha_i), a \in F$

Ejemplo 4.1. Sea $p(x) = x^4 + 2x^2 - 8$ en $\mathbb{Q}[x]$. Entonces al factorizar este polinomio obtenemos que $p(x) = (x^2 - 2)(x^2 + 4)$. Por lo tanto, su campo de descomposición es $\mathbb{Q}(\sqrt{2}, i)$.

Ejemplo 4.2. Encontraremos todos los automorfismos el polinomio $p(x) = x^2 + 1$.

El campo de descomposición de $p(x)$ es $\mathbb{Q}(i, -i) = \mathbb{Q}(i)$. Ya que $p(x) = x^2 + 1$ es el polinomio irreducible de $2i$ sobre \mathbb{Q} , entonces $\mathbb{Q}(i) = \{a + bi \mid a, b \in \mathbb{Q}\}$. Encontraremos a continuación todos los automorfismos del campo $\mathbb{Q}(i)$.

Sea $\sigma : \mathbb{Q}(i) \rightarrow \mathbb{Q}(i)$ un automorfismo. La restricción de σ a \mathbb{Q} , es decir, $\sigma_{\mathbb{Q}} : \mathbb{Q} \rightarrow \mathbb{Q}(i)$ tal que $\sigma_{\mathbb{Q}}(a) = \sigma(a)$ para todo $a \in \mathbb{Q}$, es un monomorfismo. Luego, ya que $\mathbb{Q}(i)$ es un subcampo de los números complejos y $\sigma : \mathbb{Q} \rightarrow \mathbb{Q}(i)$ un monomorfismo de anillos. Entonces, $\sigma(a) = a$ para todo $a \in \mathbb{Q}$. Como $(\sigma(i))^2 = \sigma(i)\sigma(i) = \sigma(i^2) = -1$, entonces $\sigma(i) = i$ ó $\sigma(i) = -i$. Por lo tanto, $\sigma(i) \in \mathbb{Q}(i)$. De esta manera, tenemos dos posibles automorfismos del campo $\mathbb{Q}(i)$:

$$\sigma_1 : \mathbb{Q}(i) \rightarrow \mathbb{Q}(i) \text{ con } \sigma_1(i) = i \text{ y } \sigma_2 : \mathbb{Q}(i) \rightarrow \mathbb{Q}(i) \text{ con } \sigma_2(i) = -i$$

Ahora, si $a + bi \in \mathbb{Q}(i)$, entonces:

$$\sigma_1(a + bi) = \sigma_1(a) + \sigma_1(b)\sigma_1(i) = a + bi \in \mathbb{Q}(i),$$

de donde σ_1 es la función identidad de $\mathbb{Q}(i)$.

$$\sigma_2(a + bi) = \sigma_2(a) + \sigma_2(b)\sigma - 2(i) = a - bi \in \mathbb{Q}(i).$$

Es fácil demostrar que σ_2 es un automorfismo, para esto debemos verificar que σ_2 es un homomorfismo y que sea biyectivo.

1. σ_2 es un homomorfismo:

Sea $x, y \in \mathbb{Q}(i)$, donde $x = a + bi$ y $y = c + di$, consideramos la adición consecuentemente tenemos

$$\begin{aligned}\sigma_2(x + y) &= \sigma_2(a + bi + c + di) \\ &= \sigma_2(a + c + (b + d)i) \\ &= \sigma_2(a + c) + \sigma_2((b + d)i) \\ &= (a + c) - (b + d)i \\ &= a - bi + c + di \\ &= \sigma_2(x) + \sigma_2(y).\end{aligned}$$

Ahora, consideremos la multiplicación

$$\begin{aligned}\sigma_2(xy) &= \sigma_2((a + bi)(c + di)) \\ &= \sigma_2(ac + adi + cbi - db) \\ &= \sigma_2(ac) + \sigma_2((ad)i) + \sigma_2((cb)i) + \sigma(-bd) \\ &= ac - bd - (ad + cb)i \\ &= ac - bd - adi - cbi \\ &= ac + bd(i^2) - adi - cbi \\ &= (a - bi)(c - di) \\ &= \sigma_2(x)\sigma_2(y)\end{aligned}$$

2. σ_2 es biyectivo: Para demostrar que σ_2 es biyectivo, debemos demostrar que es tanto inyectiva como sobreyectiva.

Inyectividad: Supongamos que existen dos elementos $x, y \in \mathbb{Q}(i)$ tales que

$\sigma_2(x) = \sigma_2(y)$. Entonces,

$$\sigma_2(a + bi) = \sigma_2(c + di)$$

$$a - bi = c - di$$

lo que implica que $a = c$ y $d = b$, por lo tanto, $x = y$.

Sobreyectividad: Tomemos $x \in \mathbb{Q}(i)$. Queremos encontrar $y \in \mathbb{Q}(i)$ tal que $\sigma_2(y) = x$. Consideremos $y = x + i$. Luego:

$$\sigma_2(y) = \sigma_2(x + i)$$

$$= x + \sigma_2(i)$$

$$= x + (-i)$$

$$= x - i$$

$$= y.$$

Por lo tanto, σ_2 es sobreyectiva.

Dado que σ_2 es tanto inyectiva como sobreyectiva, podemos concluir que es biyectiva. Además, dado que σ_2 cumple con ambas condiciones, se puede afirmar que es un automorfismo de $\mathbb{Q}(i)$ con $\sigma_2(i) = -i$.

Teorema 4.1

Sea E una extensión de un campo F . Entonces el conjunto

$$G(E/F) = \{\sigma / \sigma : E \rightarrow E \text{ es un automorfismo que fija } F\}$$

es un subgrupo del grado de automorfismo de E .

Demostración. Sea $\sigma, \tau \in G(E/F)$ y $a \in F$. Entonces $\sigma\tau(a) = \sigma(\tau(a)) = \sigma(a) = a$. De este modo, $\sigma\tau \in G(E/F)$. Es evidente que la función identidad de E es un elemento en $G(E/F)$. Si consideramos $\sigma \in G(E/F)$ y $a \in F$, entonces $\sigma(a) = a$. Así, $\sigma^{-1}(a) = \sigma^{-1}\sigma(a) = a$ y por lo tanto, $\sigma^{-1} \in G(E/F)$. \square

Definición 4.2

El grupo $G(E/F)$ se dice que es el grupo de automorfismo de E que fijan F o que es el grupo de E sobre F .

Ejemplo 4.3. Encontraremos el grupo de automorfismos de $\mathbb{Q}(\sqrt[3]{5})$ que fijan \mathbb{Q} . El polinomio irreducible de $\sqrt[3]{5}$ sobre \mathbb{Q} es $p(x) = x^3 - 5$ y la única raíz real de $p(x)$ es $\sqrt[3]{5}$.

Sea $\sigma : \mathbb{Q}(\sqrt[3]{5}) \rightarrow \mathbb{Q}(\sqrt[3]{5})$ un automorfismo que fija \mathbb{Q} . Dado que

$$(\sigma(\sqrt[3]{5}))^3 = \sigma((\sqrt[3]{5})^3) = \sigma(5) = 5$$

y $\sigma(\sqrt[3]{5})$ es un real, entonces $\sigma(\sqrt[3]{5}) = \sqrt[3]{5}$. Un elemento cualquiera de $\mathbb{Q}(\sqrt[3]{5})$ es de la forma $a + b\sqrt[3]{5} + c(\sqrt[3]{5})^2$ con $a, b, c \in \mathbb{Q}$. Luego,

$$\sigma(a + b\sqrt[3]{5} + c(\sqrt[3]{5})^2) = \sigma(a) + \sigma(b)\sigma(\sqrt[3]{5}) + \sigma(c)(\sigma(\sqrt[3]{5}))^2 = a + b\sqrt[3]{5} + c(\sqrt[3]{5})^2,$$

es decir, $\sigma = I$ es la identidad de $\mathbb{Q}(\sqrt[3]{5})$. Por lo tanto, el grupo de automorfismos de $\mathbb{Q}(\sqrt[3]{5})$ que fijan \mathbb{Q} es $G(\mathbb{Q}(\sqrt[3]{5}/\mathbb{Q})) = \{I\}$.

4.2 Monomorfismo

Sea F un campo y $\sigma : F \rightarrow \mathbb{C}$ un monomorfismo. Para el polinomio expresado como $f(x) = a_0 + a_1x + \dots + a_nx^n \in F[x]$, definimos el polinomio

$$\sigma f(x) = \sigma(a_0) + \sigma(a_1)x + \dots + \sigma(a_n)x^n \in \mathbb{C}[x].$$

A partir de esto, es claro que $\sigma(F) = \{\sigma(a) / a \in F\}$ es un campo isomorfo a F y que $\sigma f(x) \in \sigma(F)[x]$.

En virtud de lo anterior se sigue los siguientes resultados:

Lema 4.1

Sea F un campo y $\sigma : F \rightarrow \mathbb{C}$ un monomorfismo. Entonces

- a) Para todo $f(x), g(x) \in F[x] : \sigma(f(x) + g(x)) = \sigma f(x) + \sigma g(x)$ y $\sigma(f(x)g(x)) = \sigma f(x) \cdot \sigma g(x)$.

- b) Si $f(x) \in F[x]$ es no nulo, entonces $\deg(f(x)) = \deg(\sigma f(x))$.
- c) Si $g_0(x) \in \sigma(F)[x]$, entonces existe $g(x) \in F[x]$ tal que $\sigma g(x) = g_0(x)$.
- d) Si $f(x), g(x) \in F[x]$ y $\sigma f(x) = \sigma g(x)$, entonces $f(x) = g(x)$.

Demostración. a) Para todo $f(x), g(x) \in F[x]$, debemos demostrar que $\sigma(f(x) + g(x)) = \sigma f(x) + \sigma g(x)$. Utilizamos la definición de σ y las propiedades del monomorfismo:

$$\begin{aligned}\sigma(f(x) + g(x)) &= \sigma\left(\sum_{i=0}^n (a_i + b_i)x^i\right) \\ &= \sum_{i=0}^n \sigma((a_i + b_i)x^i) \\ &= \sum_{i=0}^n (\sigma(a_i) + \sigma(b_i))\sigma(x^i) \\ &= \sum_{i=0}^n \sigma(a_i)\sigma(x^i) + \sum_{i=0}^n \sigma(b_i)\sigma(x^i) \\ &= \sigma\left(\sum_{i=0}^n a_i x^i\right) + \sigma\left(\sum_{i=0}^n b_i x^i\right) \\ &= \sigma f(x) + \sigma g(x).\end{aligned}$$

Para todo $f(x), g(x) \in F[x]$, la afirmación es $\sigma(f(x)g(x)) = \sigma f(x) \cdot \sigma g(x)$. Nuevamente, aplicamos la definición de σ y las propiedades del monomorfismo:

$$\begin{aligned}
 \sigma(f(x)g(x)) &= \sigma\left(\sum_{i=0}^{m+n} c_i x^i\right) \\
 &= \sum_{i=0}^{m+n} \sigma(c_i x^i) \\
 &= \sum_{i=0}^{m+n} \sigma(c_i) \sigma(x^i) \\
 &= \sum_{i=0}^{m+n} \left(\sum_{j=0}^i a_j b_{i-j}\right) \sigma(x^i) \\
 &= \sum_{i=0}^{m+n} \sum_{j=0}^i \sigma(a_j) \sigma(b_{i-j}) \sigma(x^i) \\
 &= \left(\sum_{i=0}^m \sum_{j=0}^i \sigma(a_j) \sigma(b_{i-j}) \sigma(x^i)\right) + \left(\sum_{i=m+1}^{m+n} \sum_{j=0}^i \sigma(a_j) \sigma(b_{i-j}) \sigma(x^i)\right) \\
 &= \left(\sum_{i=0}^m \sigma\left(\sum_{j=0}^i a_j b_{i-j} x^i\right)\right) + \left(\sum_{i=m+1}^{m+n} \sigma\left(\sum_{j=0}^i a_j b_{i-j} x^i\right)\right) \\
 &= \left(\sum_{i=0}^m \sigma(a(x) \cdot b(x))\right) + \left(\sum_{i=m+1}^{m+n} \sigma(a(x) \cdot b(x))\right) \\
 &= \sigma(a(x) \cdot b(x)).
 \end{aligned}$$

b) Si $f(x)$ es no nulo por lo que $f(x) = a_0 + a_1x + \dots + a_nx^n \in F[x]$ con $a_n \neq 0$. Como σ es inyectivo, entonces $\sigma(a_n) \neq 0$.

c) Sea $g_0(x) = d_0 + d_1x + \dots + d_nx^n \in \sigma(F)[x]$, cada $d_i \in \sigma(F)$, existe $b_i \in F$ tal que $\sigma(b_i) = d_i$. Así,

$$g_0(x) = \sigma(b_0) + \sigma(b_1)x + \dots + \sigma(b_n)x^n = \sigma(b_0 + b_1x + \dots + b_nx^n).$$

Definiendo $g(x) = b_0 + b_1x + \dots + b_nx^n \in F[x]$, entonces $\sigma(g(x)) = g_0(x)$.

d) Si $f(x), g(x) \in F[x]$ y $\sigma f(x) = \sigma g(x)$, entonces $f(x) = g(x)$.

Sabemos que $\sigma f(x) = \sigma g(x)$, lo que implica que para cada coeficiente a_i de $f(x)$ y b_i de $g(x)$ se cumple:

$$\sigma(a_i) = \sigma(b_i).$$

Dado que es un monomorfismo, implica que es inyectivo, es decir, $\sigma(a_i) = \sigma(b_i)$, si y sólo si, $a_i = b_i$. Por lo tanto $f(x) = g(x)$.

□

Corolario 4.1

Sea F un campo y $\sigma : F \rightarrow \mathbb{C}$ un monomorfismo. Si $p(x)$ es un polinomio irreducible en $F[x]$, entonces $\sigma p(x)$ es un polinomio irreducible en $\sigma(F)[x]$.

Demostración. Supongamos que $\sigma p(x)$ es un polinomio reducible en $\sigma(F)[x]$. Por lo tanto, existen $g_0(x)h_0(x) \in \sigma F[x]$ tales que $\sigma p(x) = g_0(x)h_0(x)$ con $\deg(g_0) < \deg(\sigma p)$ y $\deg(h_0) < \deg(\sigma p)$, por el literal b) del lema anterior $\deg(\sigma p) = \deg(p)$. Luego, por el literal c) y b), $\sigma g(x) = g_0(x)$ y $\sigma h(x) = h_0(x)$. Además $\deg(\sigma g(x)) = \deg(g_0(x))$ y $\deg(\sigma h(x)) = \deg(h_0(x))$.

Así,

$$\sigma p(x) = \sigma g(x)\sigma h(x)$$

luego por el ítem a)

$$\sigma p(x) = \sigma(g(x)h(x)).$$

Finalmente, por el ítem d)

$$p(x) = g(x)h(x).$$

Ya que $\deg(g) < \deg(p)$ y $\deg(h) < \deg(p)$, obtenemos una contradicción, esto debido a que $p(x)$ es irreducible en $F[x]$. □

Lema 4.2

Sea F un campo, $f(x) \in F[x]$ y $\alpha \in \mathbb{C}$ algebraico sobre F . Si $\sigma : F(\alpha) \rightarrow \mathbb{C}$ es un monomorfismo, entonces $(\sigma f)(\sigma \alpha) = \sigma(f(\alpha))$. En particular, si α es una raíz de $f(x)$, entonces $\sigma(\alpha)$ es una raíz de $\sigma f(x)$.

Demostración. Si $f(x) = a_0 + a_1x + \cdots + a_nx^n \in F[x]$, entonces

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

Luego,

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

Si α es una raíz de $f(x)$, entonces $\sigma(\alpha)$ es una raíz de $\sigma f(x)$. Esta implicación se sigue de la igualdad demostrada, ya que si $f(\alpha) = 0$, entonces

$$\sigma(f(\alpha)) = \sigma(0) = 0,$$

entonces $\sigma(\alpha)$ es una raíz de $\sigma f(x)$.

□

Definición 4.3

Sea F un campo, $\sigma : F \rightarrow \mathbb{C}$ un monomorfismo y E una extensión de F . Un monomorfismo $\tau : E \rightarrow \mathbb{C}$, se dice que es una extensión de σ si $\tau(x) = \sigma(x)$ para todo $x \in F$.

Ejemplo 4.4. La función $\sigma : \mathbb{Q} \rightarrow \mathbb{C}$ definida por $\sigma(x) = x$ para todo $x \in \mathbb{Q}$, es un monomorfismo.

Para demostrar que σ es inyectiva, debemos verificar que si $\sigma(a) = \sigma(b)$ para $a, b \in \mathbb{Q}$, entonces $a = b$.

Supongamos que $\sigma(a) = \sigma(b)$, esto implica que $a = b$ ya que $\sigma(x) = x$, por lo tanto,

$$\sigma(a) = a$$

$$\sigma(b) = b.$$

Ahora, $\tau : \mathbb{Q}(\sqrt{5}) \rightarrow \mathbb{C}$ por $\tau(a + b\sqrt{5}) = a - b(\sqrt{5})$ para $a, b \in \mathbb{Q}$ es un monomorfismo.

Supongamos que $\sigma(x) = \sigma(y)$, entonces $x = y$ para $x, y \in \mathbb{Q}(\sqrt{5})$, donde $x = a + b\sqrt{5}$ e $y = c + d\sqrt{5}$, lo que implica que $a - b\sqrt{5} = c - d\sqrt{5}$, de donde tenemos que $a = c$ y $b = d$ por lo tanto $x = y$ teniendo así que σ es inyectiva.

Observemos que $\tau(a) = a$ para todo $a \in \mathbb{Q}$. Luego, $\tau(x) = \sigma(x)$ para todo $x \in \mathbb{Q}$. Por lo tanto, $\tau : \mathbb{Q}(\sqrt{5}) \rightarrow \mathbb{C}$ es una extensión de σ .

Teorema 4.2

Sea F un campo y $\sigma : F \rightarrow \mathbb{C}$ un monomorfismo. Sea $\alpha \in \mathbb{C}$ algebraico sobre F , $p(x) \in F[x]$ el polinomio irreducible de α sobre F y $\beta \in \mathbb{C}$ una raíz de $\sigma p(x) \in \mathbb{C}[x]$. Entonces:

- a) Existe una extensión $\tau : F(\alpha) \rightarrow \mathbb{C}$ de σ tal que $\tau(\alpha) = \beta$.
- b) Para toda extensión $\tau : F(\alpha) \rightarrow \mathbb{C}$ de σ se tiene que $\tau(\alpha)$ es una raíz de $\sigma p(x)$.

Demostración. a) Recordemos primero que $F(\alpha) = \{f(\alpha) / f(x) \in F[x]\}$ consideramos $\tau : F(\alpha) \rightarrow \mathbb{C}$, es decir,

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

Debemos verificar que $\tau : F(\alpha) \rightarrow \mathbb{C}$ este bien definida. Esto es necesario, ya que podríamos tener dos polinomios distintos $f(x), g(x) \in F[x]$ tales que $f(\alpha) = g(\alpha)$ con $\sigma f(\beta) \neq \sigma g(\beta)$. Demostraremos que dicha situación no sucede.

Sean $f(x), g(x) \in F[x]$ tales que $f(\alpha) = g(\alpha)$. El polinomio $f(x) - g(x)$ se anula en α . Dado que α es algebraico sobre F existe el polinomio irreducible $p(x) \in F[x]$ tal que $p(\alpha) = 0$. Como α es una raíz de $p(x)$, entonces $p(x)$ divide a $f(x) - g(x)$, así, $f(x) - g(x) \in \langle p(x) \rangle$ y luego, $f(x) - g(x) = p(x)q(x)$ con $q(x) \in F[x]$. De esta manera

$$\begin{aligned} \sigma(f(x) - g(x)) &= \sigma(p(x)q(x)) \\ \sigma f(x) - \sigma g(x) &= \sigma p(x)\sigma q(x). \end{aligned}$$

Por lo tanto, $\sigma f(\beta) - \sigma g(\beta) = \sigma p(\beta)\sigma q(\beta) = 0$, lo que implica que $\tau : F(\alpha) \rightarrow \mathbb{C}$ esta bien definida.

A partir del Lema 4.1 (a), $\tau : F(\alpha) \rightarrow \mathbb{C}$ es un homomorfismo, luego

$$\begin{aligned}\tau(p(\alpha)) &= (\tau p)(\tau(\alpha)) \\ &= \tau(c_0) + \tau(c_1)\tau(\alpha) + \dots + \tau(c_n)\tau(\alpha^n) \\ &= \sigma(c_0) + \sigma(c_1)\sigma(\alpha) + \dots + \sigma(c_n)\tau(\alpha^n)\end{aligned}$$

esto aplicando el Lema 4.2. También sabemos que

$$\tau(p(\alpha)) = \sigma(c_0) + \sigma(c_1)\beta + \dots + \sigma(c_n)\beta^n$$

obteniendo así que $\tau(\alpha) = \beta$.

Lo que nos queda probar que $\tau : F(\alpha) \rightarrow \mathbb{C}$ es inyectiva.

Sea $\tau(f(\alpha)) = \tau(g(\alpha))$, donde $f(x), g(x) \in F[x]$. Debemos demostrar que $f(\alpha) = g(\alpha)$. Por el algoritmo de Euclides $f(x) - g(x) = p(x)q(x) + r(x)$ donde $r(x) = 0$ ó $\deg(r) < \deg(p)$. Por lo tanto,

$$\sigma f(x) - \sigma g(x) = \sigma p(x)\sigma q(x) + \sigma r(x),$$

de donde obtenemos

$$\begin{aligned}\sigma f(\beta) - \sigma g(\beta) &= \sigma p(\beta)\sigma q(\beta) + \sigma r(\beta) \\ &= \sigma r(\beta).\end{aligned}$$

Pero $\tau(f(\alpha)) = \tau(g(\alpha))$, es decir, $\sigma f(\beta) = \sigma g(\beta)$. De esta forma $\sigma r(\beta) = 0$. Por el Corolario 4.1, $\sigma p(x)$ es un polinomio irreducible y mónico en $\sigma(F)[x]$. Entonces, $\sigma p(x)$ es el polinomio irreducible de β sobre $\sigma(F)$. Dado que $\sigma r(x) \in \sigma(F)[x]$, β es una raíz de $\sigma r(x)$ y $\deg(\sigma r) < \deg(p) = \deg(\sigma p)$, entonces necesariamente $\sigma r(x) = 0$. El Lema 4.1 (d) implica que $r(x) = 0$. Finalmente $f(x) - g(x) = p(x)q(x)$ y así $f(\alpha) - g(\alpha) = p(\alpha)q(\alpha) = 0$.

- b) Haciendo uso del Lema 4.2 la parte (b), si α es una raíz de $p(x) = c_0 + c_1x + \dots + c_nx^n \in F[x]$, entonces $\tau(\alpha)$ es una raíz de $\tau(p(\alpha))$, donde

$$\begin{aligned}\tau(p(\alpha)) &= \tau(c_0 + c_1\alpha + \dots + c_n\alpha^n) \\ &= \tau(c_0) + \tau(c_1)\tau(\alpha) + \dots + \tau(c_n)\tau(\alpha^n) \\ &= \sigma(c_0) + \sigma(c_1)\tau(\alpha) + \dots + \sigma(c_n)\tau(\alpha^n) \\ &= (\sigma p)(\tau(\alpha)).\end{aligned}$$

Entonces $\tau(\alpha)$ es una raíz de $\sigma p(x)$.

□

Ejemplo 4.5. Encontraremos todos los monomorfismos de $\mathbb{Q}(\sqrt{5})$ en \mathbb{C} .

En el caso de que $\phi : \mathbb{Q}(\sqrt{5}) \rightarrow \mathbb{C}$ sea un monomorfismo, entonces la restricción de ϕ a \mathbb{Q} también lo es. Interesa saber cómo son los monomorfismos $\sigma : \mathbb{Q} \rightarrow \mathbb{C}$. A partir del Corolario 1.1 decimos que existe una única función $\sigma : \mathbb{Q} \rightarrow \mathbb{C}$ definida por $\phi(x) = x$ para todo $x \in \mathbb{Q}$. En consecuencia, queremos encontrar todas las extensiones $\phi : \mathbb{Q}(\sqrt{5}) \rightarrow \mathbb{C}$ de σ , para esto haremos uso del Teorema 4.2.

El polinomio irreducible de $\sqrt{5}$ sobre \mathbb{Q} es $p(x) = x^2 - 5$ y luego $\mathbb{Q}(\sqrt{5}) = \{a + b\sqrt{5} / a, b \in \mathbb{Q}\}$. Según el Teorema 4.2, deseamos encontrar una raíz $\beta \in \mathbb{C}$ del polinomio $\sigma p(x) = x^2 - \sigma(5) = x^2 - 5$. Así, $\beta = \sqrt{5}$ o $\beta = -\sqrt{5}$. Por lo tanto, existen extensiones $\sigma_1 : \mathbb{Q}(\sqrt{5}) \rightarrow \mathbb{C}$ y $\sigma_2 : \mathbb{Q}(\sqrt{5}) \rightarrow \mathbb{C}$ de σ tales que $\sigma_1(\sqrt{5}) = \sqrt{5}$ y $\sigma_2(\sqrt{5}) = -\sqrt{5}$. Además, $\sigma_1(x) = \sigma_2(x) = \sigma(x) = x$ para todo $x \in \mathbb{Q}$. De esta manera, para todo $a, b \in \mathbb{Q}$.

$$\sigma_1(a + b\sqrt{5}) = \sigma_1(a) + \sigma_1(b)\sigma_1(\sqrt{5}) = a + b\sqrt{5}$$

y

$$\sigma_2(a + b\sqrt{5}) = \sigma_2(a) + \sigma_2(b)\sigma_2(\sqrt{5}) = a + b(-\sqrt{5}) = a - b\sqrt{5}.$$

Corolario 4.2

Sea F un campo $\sigma : F \rightarrow \mathbb{C}$ un monomorfismo, $\alpha \in \mathbb{C}$ algebraico sobre F y $p(x)$ el polinomio irreducible de α sobre F de grado n . Entonces, el número posible de extensiones $\tau : F(\alpha) \rightarrow \mathbb{C}$ de σ es igual a $[F(\alpha) : F] = n$.

Demostración. Si $p(x) \in F[x]$ es no nulo, entonces $\deg(p(x)) = \deg(\sigma(p(x))) = n$ esto por el Lema 4.1. Luego, si $p(x)$ es un polinomio irreducible en $F[x]$, entonces $\sigma p(x)$ es un polinomio irreducible en $\sigma(F)[x]$. Sea F un subcampo de \mathbb{C} y $p(x) \in F[x]$ irreducible sobre F , sabemos que $\deg(\sigma(p(x))) = n$, entonces $\sigma p(x)$ tiene n raíces distintas en \mathbb{C} . Finalmente aplicando el Teorema 4.2, se obtiene que $\tau : F(\alpha) \rightarrow \mathbb{C}$ de σ es igual a $[F(\alpha) : F] = n$. □

Corolario 4.3

Sea F un campo, $\sigma : F \rightarrow \mathbb{C}$ un monomorfismo y $\alpha, \beta \in \mathbb{C}$ algebraicos sobre F . Entonces, el número de extensiones $\tau : F(\alpha, \beta) \rightarrow \mathbb{C}$ de σ es igual a $[F(\alpha, \beta) : F]$.

Demostración. Sea $[F(\alpha) : F] = n$. Por el Corolario 4.2, el número de posible extensiones de $f(\alpha)$ en \mathbb{C} de σ es igual a $[F(\alpha) : F] = n$. Sean $\sigma_1, \dots, \sigma_n$ tales extensiones, para cada $j \in \{1, \dots, n\}$, $\sigma_j : F(\alpha) \rightarrow \mathbb{C}$ es un monomorfismo. El número posible de extensiones de $F(\alpha, \beta) = F(\alpha)(\beta)$ en \mathbb{C} de σ_j es $[F(\alpha)(\beta) : F(\alpha)]$. Luego existen $n[F(\alpha)(\beta) : F(\alpha)]$ extensiones $\tau : F(\alpha, \beta) \rightarrow \mathbb{C}$ de σ . Por el Corolario 3.1, obtenemos que

$$\begin{aligned} n[F(\alpha)(\beta) : F(\alpha)] &= [F(\alpha) : F][F(\alpha)(\beta) : F(\alpha)] \\ &= [F(\alpha, \beta) : F]. \end{aligned}$$

□

El corolario que sigue es una generalización del corolario anterior, el cual se demuestra por inducción.

Corolario 4.4

Sea F un campo, $\sigma : F \rightarrow \mathbb{C}$ un monomorfismo de campos y $\alpha_1, \dots, \alpha_k \in \mathbb{C}$ algebraicas sobre F . Entonces, el número de extensiones

$$\tau : F(\alpha_1, \dots, \alpha_k) \rightarrow \mathbb{C}$$

de σ es igual a $[F(\alpha_1, \dots, \alpha_k) : F]$.

Demostración. Al ser la demostración por inducción construimos la base inductiva e hipótesis inductiva para así llegar a nuestro paso inductivo.

Consideramos que el corolario es válido para $k = 1$. Entonces tenemos $\alpha_1 \in \mathbb{C}$ algebraico sobre F . Por el corolario anterior, el número de extensiones $\tau : F(\alpha_1) \rightarrow \mathbb{C}$ de σ es igual a $[F(\alpha_1) : F]$.

Supongamos que el corolario es válido para $k = m$, es decir, para $\alpha_1, \dots, \alpha_m \in \mathbb{C}$ algebraicos sobre F , el número de extensiones $\tau : F(\alpha_1, \dots, \alpha_m) \rightarrow \mathbb{C}$ de σ es igual a $[F(\alpha_1, \dots, \alpha_m) : F]$.

Ahora tomemos el campo $F(\alpha_1, \dots, \alpha_{m+1})$. Por la hipótesis de inducción, el número de extensiones de σ a $F(\alpha_1, \dots, \alpha_m)$ es igual a $[F(\alpha_1, \dots, \alpha_m) : F]$. Ahora, aplicamos el corolario previo al campo $F(\alpha_1, \dots, \alpha_m)$ con los elementos α_{m+1} y α_{m+1} (repetidos) para obtener que el número de extensiones de σ a $F(\alpha_1, \dots, \alpha_{m+1})$ es igual a $[F(\alpha_1, \dots, \alpha_m, \alpha_{m+1}) : F(\alpha_1, \dots, \alpha_m)] \cdot [F(\alpha_1, \dots, \alpha_m) : F]$.

Notemos que $[F(\alpha_1, \dots, \alpha_m, \alpha_{m+1}) : F(\alpha_1, \dots, \alpha_m)]$ es simplemente el grado de la extensión de α_{m+1} sobre $F(\alpha_1, \dots, \alpha_m)$, y denotamos este grado como n . Entonces, el número total de extensiones de σ a $F(\alpha_1, \dots, \alpha_{m+1})$ es $n \cdot [F(\alpha_1, \dots, \alpha_m) : F]$.

Por lo tanto, hemos demostrado que el corolario es válido para $k = m + 1$ y, por lo tanto, por inducción, es válido para cualquier k .

□

Ejemplo 4.6. Encontraremos todos los monomorfismos de $\mathbb{Q}(\sqrt{5}, i)$

Sabemos que $\mathbb{Q}(\sqrt{5}, i) = \mathbb{Q}(\sqrt{5})(i)$. Además,

$$\begin{array}{c} \mathbb{Q}(\sqrt{5}, i) \\ | \\ \mathbb{Q}(\sqrt{5}) \\ | \\ \mathbb{Q} \end{array}$$

Probaremos a continuación que $\{1, \sqrt{5}\}$ es una base de $\mathbb{Q}(\sqrt{5})$ como espacio vectorial sobre \mathbb{Q} y $\{1, i\}$ es una base de $\mathbb{Q}(\sqrt{5})(i)$ como espacio vectorial sobre $\mathbb{Q}(\sqrt{5})$.

Para que $\{1, \sqrt{5}\}$ sea una base, debemos probar verificar que $\{1, \sqrt{5}\}$ sea linealmente independiente, para esto mostraremos que la única forma en la que podemos obtener el vector nulo 0 como combinación lineal de los elementos de la

base es tomando los coeficientes c_1, c_2

$$c_1 1 + c_2 \sqrt{5} = 0.$$

Supongamos que c_1 y c_2 son los coeficientes que permite que la ecuación cumpla. Entonces

$$\begin{aligned} c_2 \sqrt{5} &= -c_1 \\ \sqrt{5} &= -\frac{c_1}{c_2}, \end{aligned}$$

lo que es una contradicción ya que $\sqrt{5}$ es un número irracional y no puede expresarse como una fracción $\frac{a}{b}$ con a y b enteros y $b \neq 0$. Por lo tanto, la única forma en que la ecuación se cumpla es si $c_1 = c_2 = 0$.

Ahora tomamos $x \in \mathbb{Q}(\sqrt{5})$ tal que $x = a + b\sqrt{5}$ con $a, b \in \mathbb{Q}$.

Dado que 1 y $\sqrt{5}$ son elementos de $\mathbb{Q}(\sqrt{5})$, podemos expresar x como:

$$x = a \cdot 1 + b \cdot \sqrt{5}.$$

Luego $\{1, i\}$ es una base de $\mathbb{Q}(\sqrt{5})(i)$ como espacio vectorial sobre $\mathbb{Q}(\sqrt{5})$.

De manera análoga consideramos c_1, c_2 y la ecuación

$$c_1 \cdot 1 + c_2 i = 0,$$

donde $c_1, c_2 \in \mathbb{Q}$,

$$\begin{aligned} c_1 + c_2 i &= 0 \\ c_2 i &= -c_1 \\ i &= -\frac{c_1}{c_2}. \end{aligned}$$

Pero sabemos que i es un número imaginario y no puede expresarse como una fracción $\frac{a}{b}$ con a y b enteros y $b \neq 0$. Por lo tanto, la única manera en que la ecuación se cumpla es si $c_1 = c_2 = 0$.

Finalmente, tomamos $y \in \mathbb{Q}(\sqrt{5})$ tal que $y = a + bi$ con $a, b \in \mathbb{Q}$. Dado que 1 e i son elementos de $\mathbb{Q}(\sqrt{5}, i)$ podemos expresar como $y = a \cdot 1 + bi$ lo que es una combinación lineal de los elementos de la base $\{1, i\}$.

Por lo tanto $\{1, i\}$ es generadora de $\mathbb{Q}(\sqrt{5})(i)$.

El conjunto $\{1, \sqrt{5}, i, \sqrt{i}\}$ es una base de $\mathbb{Q}(\sqrt{5}, i)$, como espacio vectorial sobre \mathbb{Q} y en consecuencia

$$\mathbb{Q}(\sqrt{5}, i) = \{a + b\sqrt{5} + ci + d\sqrt{5}i \mid a, b, c, d \in \mathbb{Q}\}$$

Cualquier monomorfismo de $\mathbb{Q}(\sqrt{5}, i)$ en \mathbb{C} es una extensión de la función $\sigma : \mathbb{Q} \rightarrow \mathbb{C}$ tal que $\sigma(x) = x$ para todo $x \in \mathbb{Q}$.

Sabemos que $\sigma_1 : \mathbb{Q}(\sqrt{5}) \rightarrow \mathbb{C}$ y $\sigma_2 : \mathbb{Q}(\sqrt{5}) \rightarrow \mathbb{C}$ definidas de la siguiente manera $\sigma_1(a + b\sqrt{5}) = a + b\sqrt{5}$ y $\sigma_2(a + b\sqrt{5}) = a - b\sqrt{5}$ para todo $a, b \in \mathbb{Q}$, son las únicas extensiones de σ . Por lo tanto, cualquier monomorfismo de $\mathbb{Q}(\sqrt{5}, i)$ en \mathbb{C} debe ser una extensión de σ_1 ó σ_2 .

Encontraremos las extensiones $\tau : \mathbb{Q}(\sqrt{5})(i) \rightarrow \mathbb{C}$ de σ_1 . El polinomio irreducible de i sobre $\mathbb{Q}(\sqrt{5})$ es $p(x) = x^2 + 1$. Las raíces de $\sigma_1 p(x) = x^2 + \sigma_1(1) = x^2 + 1$ son $i, -i$. De esta manera, existen dos extensiones de σ_1 . Estas son: $\tau_1 : \mathbb{Q}(\sqrt{5})(i) \rightarrow \mathbb{C}$ tal que $\tau_1(i) = i$ y $\tau_2 : \mathbb{Q}(\sqrt{5})(i) \rightarrow \mathbb{C}$ tal que $\tau_2(i) = -i$. Además, $\tau_1(a + b\sqrt{5}) = \sigma_1(a + b\sqrt{5}) = a + b\sqrt{5}$ para todo $a, b \in \mathbb{Q}$ y $\tau_2(a + b\sqrt{5}) = \sigma_1(a + b\sqrt{5}) = a + b\sqrt{5}$ para todo $a, b \in \mathbb{Q}$.

A continuación encontraremos las extensiones $\tau : \mathbb{Q}(\sqrt{5})(i) \rightarrow \mathbb{C}$ de σ_2 . El polinomio irreducible de i sobre $\mathbb{Q}(\sqrt{5})$ es $q(x) = x^2 + 1$ por lo que sus raíces de $\sigma_2 q(x) = x^2 + \sigma_2(1) = x^2 + 1$ son $i, -i$. De esta manera, existen dos extensiones de σ_2 . Estas son: $\tau_3 : \mathbb{Q}(\sqrt{5})(i) \rightarrow \mathbb{C}$ tal que $\tau_3(i) = i$ y $\tau_4 : \mathbb{Q}(\sqrt{5})(i) \rightarrow \mathbb{C}$ tal que $\tau_4(i) = -i$. Además, $\tau_3(a + b\sqrt{5}) = \sigma_2(a + b\sqrt{5}) = a - b\sqrt{5}$ para todo $a, b \in \mathbb{Q}$ y $\tau_4(a + b\sqrt{5}) = \sigma_2(a + b\sqrt{5}) = a - b\sqrt{5}$ para todo $a, b \in \mathbb{Q}$.

Por lo tanto, obtenemos que $\tau_1(\sqrt{5}) = \sqrt{5}$, $\tau_1(i) = i$, $\tau_2(\sqrt{5}) = \sqrt{5}$, $\tau_2(i) = -i$, $\tau_3(\sqrt{5}) = -\sqrt{5}$, $\tau_3(i) = i$ y $\tau_4(\sqrt{5}) = -\sqrt{5}$, $\tau_4(i) = -i$, lo que implica la existencia de 4 monomorfismos de $\mathbb{Q}(\sqrt{5}, i)$ en \mathbb{C} :

$$\tau_1(a + b\sqrt{5} + ci + d\sqrt{5}i) = a + b\sqrt{5} + ci + d\sqrt{5}i \text{ para todo } a, b, c, d \in \mathbb{Q},$$

$$\tau_2(a + b\sqrt{5} + ci + d\sqrt{5}i) = a + b\sqrt{5} - ci - d\sqrt{5}i \text{ para todo } a, b, c, d \in \mathbb{Q},$$

$$\tau_3(a + b\sqrt{5} + ci + d\sqrt{5}i) = a - b\sqrt{5} + ci - d\sqrt{5}i \text{ para todo } a, b, c, d \in \mathbb{Q},$$

$$\tau_4(a + b\sqrt{5} + ci + d\sqrt{5}i) = a - b\sqrt{5} - ci + d\sqrt{5}i \text{ para todo } a, b, c, d \in \mathbb{Q},$$

Teorema 4.3 Teorema del elemento primitivo

Sea E una extensión finita de un campo F . Entonces existe un elemento $\gamma \in E$ tal que $E = F(\gamma)$.

Demostración. Para la demostración de este teorema, probaremos que, si $\alpha, \beta \in \mathbb{C}$ son algebraicos sobre F , entonces existe $\gamma \in F(\alpha, \beta)$, tal que $f(\alpha, \beta) = F(\gamma)$.

Sea $\alpha, \beta \in \mathbb{C}$ algebraicos sobre F , $[F(\alpha, \beta) : F] = n$ y $\sigma : F \rightarrow \mathbb{C}$ definida por $\sigma(x) = x$ para todo $x \in F$. Por el Corolario 4.3, existen $\sigma_1, \dots, \sigma_n$ extensiones de $F(\alpha, \beta)$ en \mathbb{C} de σ todas distintas. Luego, cada $\sigma_i : F(\alpha, \beta) \rightarrow \mathbb{C}$ es un monomorfismo tal que $\sigma_i(x) = \sigma(x) = x$ para todo $x \in F$.

Probaremos que podemos encontrar un elemento $a \in F$ tal que $\sigma_i(\alpha + a\beta)$ son distintos para todo $i \in \{1, \dots, n\}$. Observemos que el polinomio $\sigma_j(\alpha) - \sigma_i(\alpha) + (\sigma_j(\beta) - \sigma_i(\beta))x$ es no nulo, cuando $i \neq j$, lo que es una contradicción. Consideremos el polinomio no nulo

$$h(x) = \prod_{i \neq j} (\sigma_j(\alpha) - \sigma_i(\alpha) + (\sigma_j(\beta) - \sigma_i(\beta))x).$$

Dicho polinomio posee un número finito de raíces en \mathbb{C} , a partir de encontrar un elemento $a \in F$ tal que

$$h(a) = \prod_{i \neq j} (\sigma_j(\alpha) - \sigma_i(\alpha) + (\sigma_j(\beta) - \sigma_i(\beta))a) \neq 0.$$

Así, para $i \neq j$, tenemos

$$\sigma_j(\alpha) - \sigma_i(\alpha) + (\sigma_j(\beta) - \sigma_i(\beta))a = \sigma_j(\alpha + a\beta) - \sigma_i(\alpha + a\beta) \neq 0$$

lo cual implica que $\sigma_i(\alpha + a\beta)$ son distintos para todo $i \in \{1, \dots, n\}$. Sea $\gamma = \alpha + a\beta$. Claramente $F(\gamma)$ es un subcampo de $F(\alpha, \beta)$. Demostraremos que $F(\gamma) = F(\alpha, \beta)$.

Las restricciones de cada $\sigma_i : F(\alpha, \beta) \rightarrow \mathbb{C}$ a $F(\gamma)$ siguen siendo monomorfismos, es decir, extensiones de σ . Dado que $\sigma_1(\gamma), \dots, \sigma_n(\gamma)$ son distintos, entonces $\sigma_1, \dots, \sigma_n$ de $F(\gamma)$ en \mathbb{C} son todos distintos. Por el Corolario 4.2, $[F(\gamma, \beta) : F] \geq n$.

Dado que el subespacio vectorial $F(\gamma)$ de $F(\alpha, \beta)$ sobre F , $[F(\alpha, \beta) : F] = n$ y $[F(\gamma) : F] \geq n$, entonces $F(\alpha, \beta) = F(\gamma)$.

Si E es una extensión finita de un campo F , por el Teorema 3.6, existen elementos $\delta_1, \dots, \delta_k$ en E tales que $E = F(\delta_1, \dots, \delta_k)$. Por lo previamente demostrado, existe $\gamma_1 \in F(\delta_1, \delta_2)$ tal que $F(\delta_1, \delta_2) = F(\gamma_1)$. Ahora,

$$\begin{aligned} E &= F(\delta_1, \dots, \delta_k) \\ &= F(\delta_1, \delta_2)(\delta_3, \dots, \delta_k) \\ &= F(\gamma_1)(\delta_3, \dots, \delta_k) \\ &= F(\gamma_1, \delta_3)(\delta_4, \dots, \delta_k). \end{aligned}$$

Continuando inductivamente con este proceso, demostramos lo deseado. \square

Ejemplo 4.7. Encontraremos $\gamma \in \mathbb{C}$ tal que $\mathbb{Q}(\sqrt{2}, \sqrt{5}) = \mathbb{Q}(\gamma)$

Para encontrar un elemento primitivo usando el Teorema 4.3, primero debemos probar que la extensión de campo $\mathbb{Q}(\sqrt{2}, \sqrt{5})$ sea finita. En este caso la extensión es finita, dado que $\sqrt{2}$ y $\sqrt{5}$ son algebraicos sobre \mathbb{Q} y, por lo tanto, $\mathbb{Q}(\sqrt{2}, \sqrt{5})$ es un campo de extensión finita de \mathbb{Q} .

El teorema del elemento primitivo establece que sea una extensión de campo finita, entonces existe un elemento primitivo que genera la extensión, es decir, existe un $\gamma \in \mathbb{C}$ tal que $\mathbb{Q}(\sqrt{2}, \sqrt{5}) = \mathbb{Q}(\gamma)$.

Para encontrar el elemento γ consideramos el polinomio irreducible que tenga como raíces a $\sqrt{2}$ y $\sqrt{5}$, dicho polinomio es

$$f(x) = (x^2 - 2)(x^2 - 5),$$

donde $f(x)$ es irreducible sobre \mathbb{Q} y tiene a $\sqrt{2}$ y $\sqrt{5}$ como raíces.

4.3 Extensión de Galois

Definición 4.4

Sea E una extensión finita de un campo F . Un monomorfismo $\tau : E \rightarrow \mathbb{C}$ se dice que fija F , si $\tau(x) = x$ para todo $x \in F$.

Lema 4.3

Sea K una extensión finita de un campo F y $\tau : K \rightarrow \mathbb{C}$ un monomorfismo que fija F . Si $\tau(K) \subset K$, entonces $\tau(K) = K$.

Demostración. Dado que $\tau : K \rightarrow \mathbb{C}$ fija F , entonces $\tau : K \rightarrow \mathbb{C}$ es una función lineal. Para demostrar que es una función lineal debemos verificar que τ verifique las siguientes propiedades:

- $f(x + y) = f(x) + f(y)$
- $f(ax) = af(x)$

para $x, y \in K$ y $a \in F$ se tiene que $\tau(x + y) = \tau(x) + \tau(y)$ y $\tau(ax) = a\tau(x)$ ya que fija F . Dado que $\tau : K \rightarrow \mathbb{C}$ es lineal inyectiva. Para probar esto supongamos que $\tau(\alpha) = \tau(\beta)$, llegando así que $\tau(\alpha) - \tau(\beta) = 0$, debido a la linealidad de τ implica que $\tau(\alpha - \beta) = 0$. Pero τ es un monomorfismo por lo que $\alpha - \beta = 0$, así $\alpha = \beta$. Así $\ker(\tau) = \{0\}$. Ahora $\dim(K) = \dim_F(\ker(\tau)) + \dim_F(\tau(K))$ llegando así que $\dim_F(\tau(K)) = \dim_F(K)$. Como $\tau(K)$ es un subespacio de K , obtenemos que $\tau(K) = K$. □

El lema expuesto también se lo conoce como **Extensión normal**, ya que K es una extensión normal de F si K es una extensión finita de F tal que F es el campo fijo de $G(K/F)$.

Ejemplo 4.8. En el ejemplo ?? encontramos todos los monomorfismos

$$\tau : \mathbb{Q}(\sqrt{5}, i) \rightarrow \mathbb{C}.$$

Capítulo 4. Galois

Estos monomorfismos fijan \mathbb{Q} y además, $\tau(\mathbb{Q}(\sqrt{5}, i) \subset \mathbb{Q}(\sqrt{5}, i)$. Por el Lema 4.3 $\tau_1, \tau_2, \tau_3, \tau_4$ son todos los automorfismos de $\mathbb{Q}(\sqrt{5}, i)$. En consecuencia, $G(\mathbb{Q}(\sqrt{5}, i)/\mathbb{Q}) = \{\tau_1, \tau_2, \tau_3, \tau_4\}$, que como sabemos es un grupo bajo la composición de funciones.

Dado que $\tau_1(\sqrt{5}) = \sqrt{5}, \tau_1(i) = i, \tau_2(\sqrt{5}) = \sqrt{5}, \tau_2(i) = -i, \tau_3(\sqrt{5}) = -\sqrt{5}, \tau_3(i) = i, \tau_4(\sqrt{5}) = -\sqrt{5}, \tau_4(i) = -i$, entonces

$$\tau_2\tau_3(\sqrt{5}) = \tau_2(\tau_3(\sqrt{5})) = \tau_2(-\sqrt{5}) = -\tau_2(\sqrt{5}) = -\sqrt{5}$$

y

$$\tau_2\tau_3(i) = \tau_2(\tau_3(i)) = \tau_2(i) = -i.$$

Por lo tanto $\tau_2\tau_3 = \tau_4$.

Este procedimiento resulta similar para los productos restantes, obteniendo así la siguiente tabla:

\circ	τ_1	τ_2	τ_3	τ_4
τ_1	τ_1	τ_2	τ_3	τ_4
τ_2	τ_2	τ_1	τ_4	τ_3
τ_3	τ_3	τ_4	τ_1	τ_2
τ_4	τ_4	τ_3	τ_2	τ_1

Teorema 4.4

Sea G el grupo de automorfismos de un campo K y H un subgrupo de G . Entonces, el conjunto $K^H = \{x \in K / \sigma(x) = x \text{ para todo } \sigma \in H\}$ es un campo llamado el campo fijo de H .

Demostración. Es suficiente probar que K^H es un subcampo de K , para esto hacemos uso del Lema 1.3.

Primero partimos demostrando que 0 y 1 están en K^H , esto es evidente dado que $\sigma \in H$ es un automorfismo $\sigma(0) = 0$ y $\sigma(1) = 1$.

Continuando con la demostración probaremos la cerradura bajo el producto y la resta.

Sean $x, y \in K^H$, $\sigma \in H$. Entonces $\sigma(x) = x$ y $\sigma(y) = y$. Ahora

$$\sigma(x - y) = \sigma(x) - \sigma(y) = x - y$$

y

$$\sigma(xy) = \sigma(x)\sigma(y) = xy.$$

Por lo tanto, $x - y \in K^H$ y $xy \in K^H$. Como $\sigma : (K^*, \cdot) \rightarrow (K^*, \cdot)$ es un homomorfismo de grupos, entonces $\sigma(x^{-1}) = \sigma(x)^{-1} = x^{-1}$ y por lo tanto, $x^{-1} \in K^H$. Finalmente hemos probado que K^H es un subcampo de K . \square

Ejemplo 4.9. Consideramos en grupo $G = \{\tau_1, \tau_2, \tau_3, \tau_4\}$ del ejemplo ?? y el subgrupo $H = \{\tau_1, \tau_4\}$ de G . Encontraremos el campo fijo de H .

Sabemos que τ_1 es la función identidad de $\mathbb{Q}(\sqrt{5}, i)$ y $\tau_4(a + b\sqrt{5} + ci + d\sqrt{5}i) = a - b\sqrt{5} - ci + d\sqrt{5}i$ para todo $a, b, c, d \in \mathbb{Q}$. Teniendo así,

$$\begin{aligned} (\mathbb{Q}(\sqrt{5}, i))^H &= \{x \in \mathbb{Q}(\sqrt{5}, i) / \tau_1(x) = x \text{ y } \tau_4(x) = x\} \\ &= \{a + b\sqrt{5} + ci + d\sqrt{5}i / \tau_4(a + b\sqrt{5} + ci + d\sqrt{5}i) = \\ &\quad a - b\sqrt{5} - ci + d\sqrt{5}i\} \end{aligned}$$

Si $\tau_4(a + b\sqrt{5} + ci + d\sqrt{5}i) = a - b\sqrt{5} - ci + d\sqrt{5}i$. Entonces,

$$a - b\sqrt{5} - ci + d\sqrt{5}i = a + b\sqrt{5} + ci + d\sqrt{5}i,$$

lo que nos lleva a decir que $2b\sqrt{5} + 2ci = 0$, de donde $b\sqrt{5} + ci = 0$. Así $b = c = 0$. Por lo tanto, el campo fijo de H es:

$$(\mathbb{Q}(\sqrt{5}, i))^H = \{a + d\sqrt{5}i / a, d \in \mathbb{Q}\} = \mathbb{Q}(\sqrt{5}i).$$

Definición 4.5

La extensión finita K de un campo F , se denomina **extensión de Galois**, si para todo monomorfismo $\sigma : K \rightarrow \mathbb{C}$ que fija F se tiene que $\sigma(K) = K$. Es

decir, para todo monomorfismo $\sigma : K \rightarrow \mathbb{C}$ se tiene que $\sigma \in G(K/F)$.

Ejemplo 4.10. La extensión $\mathbb{Q}(\sqrt{5}, i)$ de \mathbb{Q} es una extensión de Galois. De igual manera sucede con la extensión $\mathbb{Q}(\sqrt{2}, i)$ de \mathbb{Q} .

Teorema 4.5

Sea K una extensión finita de un campo F , es una extensión de Galois, si y sólo si, K es el campo de descomposición de algún polinomio $f(x) \in F[x]$.

Demostración. \Rightarrow) Sea K una extensión de Galois de F , dado que K es una extensión finita de F , existe $\alpha \in K$ tal que $K = F(\alpha)$ esto por el Teorema 4.3. Sea $p(x)$ el polinomio irreducible de α sobre F y $\deg(p) = n$. Sabemos que existen n distintos monomorfismos de K en \mathbb{C} que fijan F . Como K es una extensión de Galois, entonces los n homomorfismos por la definición 4.4 son automorfismos de K . Sea $\sigma_1, \dots, \sigma_n$ automorfismos de K , por el Teorema 4.2 $\sigma_1(\alpha) = \alpha_1, \dots, \sigma_n(\alpha) = \alpha_n$ son las n raíces de $p(x)$ y todas en K . Por lo tanto, $K = F(\alpha_1, \dots, \alpha_n)$.

\Leftarrow) K es un campo de descomposición de algún polinomio $f(x) \in F[x]$ (no necesariamente irreducible) con raíces $\alpha_1, \dots, \alpha_n \in \mathbb{C}$. Así $K = F(\alpha_1, \dots, \alpha_n)$. Sea $\sigma : K \rightarrow \mathbb{C}$ un monomorfismo que fija F y α_i una de las raíces de $f(x)$. Si consideramos a $q(x)$ el polinomio irreducible de α_i sobre F , entonces $q(x)$ es un divisor de $f(x)$. Luego, por el Teorema 4.2 $\sigma(\alpha_i)$ es una raíz de $q(x)$, por lo tanto α_i también es una raíz de $f(x)$. Así $\sigma(\alpha_i) \in K$, entonces σ es un automorfismo de K , demostrando así que K es una extensión de Galois. \square

Observación 4.1. Sea F un campo, $p(x) \in F[x]$ un polinomio irreducible en $F[x]$ y $\deg(p) = n$. Si $\alpha_1, \dots, \alpha_n \in \mathbb{C}$ son las raíces de $p(x)$, las cuales son distintas, $K = F(\alpha_1, \dots, \alpha_n)$ es el campo de descomposición de $p(x)$ y $\tau \in G(K/F)$, por lo tanto, $\tau(\alpha_1), \dots, \tau(\alpha_n)$ son las mismas n raíces distintas de $p(x)$. Así, τ permuta las raíces $\alpha_1, \dots, \alpha_n$ de $p(x)$. De esta manera, podemos mirar a τ como un elemento del grupo de permutaciones S_n de n elementos $\{1, \dots, n\}$. Concluimos que, $G(K/F)$

es isomorfo a un grupo de S_n . Luego a partir del Corolario 4.4 el número de elementos del grupo $G(K/F)$ es $[K : F]$.

Ejemplo 4.11. Sea K una extensión de Galois de un campo F . Si $p(x) \in F[x]$ es irreducible en $F[x]$ y $\alpha \in K$ es una raíz de $p(x)$, demostraremos que $p(x)$ tiene todas sus raíces en K .

Dado que $p(x)$ es irreducible en $F[x]$, el campo de descomposición K de $p(x)$ sobre F es una extensión de Galois.

Sabemos que α es una raíz de $p(x)$ en K , lo que implica que $p(\alpha) = 0$. Consideremos el conjunto de todas las raíces de $p(x)$ en \bar{F} , denotado por $\{\alpha, \alpha_2, \dots, \alpha_n\}$. Dado que $p(x)$ es irreducible, todas las raíces son distintas. Además, $K = F(\alpha)$ es el campo de descomposición de $p(x)$. Entonces, K contiene todas las raíces de $p(x)$.

Consideremos un automorfismo $\sigma \in G(K/F)$. Como σ es un automorfismo que fija F , se extiende a un automorfismo sobre \bar{F} . Debido a que α es una raíz de $p(x)$, tenemos $\sigma(\alpha)$ también es una raíz de $p(x)$.

Dado que σ es un automorfismo arbitrario en $G(K/F)$, cada raíz de $p(x)$ es llevada a otra raíz de $p(x)$ por algún automorfismo en $G(K/F)$. Esto implica que todas las raíces de $p(x)$ están en K .

Por lo tanto, hemos demostrado que si $p(x)$ es irreducible en $F[x]$ y α es una raíz de $p(x)$ en K , entonces todas las raíces de $p(x)$ están en K .

4.4 Teorema Fundamental de la Teoría de Galois

Teorema 4.6

Sea K una extensión de Galois de un campo F . Sea $G = G(K/F)$ el grupo de automorfismos de K sobre F . Entonces F es el campo fijo de G .

Demostración. La demostración se realiza mostrando que F es igual al campo fijo

de G , es decir, $F = K^G$, donde por el Teorema 4.4 se define de la siguiente manera:

$$K^G = \{x \in K \mid \sigma(x) = x \text{ para todo } \sigma \in G\}.$$

Supongamos, por contradicción, que $F \neq K^G$. Entonces, existe $\alpha \in K^G$ tal que $\alpha \notin F$. Como $\alpha \in K$ y K es algebraico sobre F , existe el polinomio irreducible $p(x) \in F[x]$ de α sobre F . Necesariamente, $\deg(p) > 1$, dado que $\alpha \notin F$, lo que implica $[F(\alpha) : F] = n > 1$. Por lo tanto, existe un monomorfismo $\sigma : F(\alpha) \rightarrow C$ tal que $\sigma(\alpha) \neq \alpha$ por el Teorema 4.2.

Sea $\tau : K \rightarrow C$ una extensión de $\sigma : F(\alpha) \rightarrow C$. Como K es una extensión de Galois de F , entonces $\tau(K) = K$, de donde $\tau \in G$. Ahora, $\tau(\alpha) = \sigma(\alpha) \neq \alpha$. En consecuencia, $\alpha \notin K^G$, lo que es una contradicción. Por lo tanto, $F = K^G$. \square

Definición 4.6

Si K es una extensión de Galois de un campo F , entonces el grupo de automorfismos de K que fijan F , se llama el grupo de Galois de K sobre F .

Nota. Si F es un campo y K es el campo de descomposición del polinomio $f(x) \in F[x]$, entonces diremos que $G(K/F)$ es el grupo de Galois de $f(x)$.

Teorema 4.7

Sea K una extensión de Galois de un campo F y E un campo tal que $F \leq E \leq K$. Entonces:

- a) K es una extensión de Galois de E .
- b) E es el campo fijo del subgrupo $G(K/E)$ de $G(K/F)$ y $[K : E] = \circ(G(K/E))$.
- c) La función $E \rightarrow G(K/E)$ de los campos intermedios entre F y K y el conjunto de subgrupos de $G(K/F)$ es inyectiva y sobreyectiva.
- d) Si E_0 es un campo tal que $F \leq E_0 \leq E \leq K$, entonces $G(K/E) \leq G(K/E_0)$.

e) E es una extensión normal de F , si y sólo si $G(K/E)$ es un subgrupo normal de $G(K/F)$. Luego $G(E/F)$ es isomorfo a $G(K/F)/G(K/E)$

Demostración. a) Sea $\tau : K \rightarrow \mathbb{C}$ una extensión de $\sigma : E \rightarrow \mathbb{C}$ definida por $\sigma(x) = x$ para todo $x \in E$. Dado que $\sigma : E \rightarrow \mathbb{C}$ es una extensión de $i : F \rightarrow \mathbb{C}$ definida por $i(x) = x$ para todo $x \in F$, y como $\tau : K \rightarrow \mathbb{C}$ es una extensión de $i : F \rightarrow \mathbb{C}$ y K es una extensión de Galois de F , entonces $\tau(K) = K$. Por lo tanto, K es una extensión de Galois de E .

b) Es una conclusión inmediata del ítem a) y del Teorema 4.4.

c) Demostraremos primero que la función es inyectiva.

Sean E, E' campos distintos tales que $F \leq E \leq K$ y $F \leq E' \leq K$. Sabemos que los campos fijos de $G(K/E)$ y $G(K/E')$ son E y E' , respectivamente. Como $E \neq E'$, entonces necesariamente $G(K/E) \neq G(K/E')$, y por lo tanto, la función es inyectiva.

Demostraremos que la función es sobreyectiva. Sea H un subgrupo de $G(K/F)$. Debemos demostrar que existe un campo E con $F \leq E \leq K$ tal que $H = G(K/E)$.

Dado que K es una extensión finita de F , existe $\alpha \in K$ tal que $K = F(\alpha)$ por el Teorema 4.3. Sea $H = \{\sigma_1, \dots, \sigma_r\}$ y $f(x) = (x - \sigma_1(\alpha)) \cdots (x - \sigma_r(\alpha))$. Claramente, $\deg(f) = r$. Para cualquier $\sigma \in H$, los elementos $\sigma\sigma_1, \dots, \sigma\sigma_r$ siguen estando en H y son todos distintos. Luego, $\{\sigma\sigma_1, \dots, \sigma\sigma_r\} = \{\sigma_1, \dots, \sigma_r\}$, lo cual implica que $\{\sigma\sigma_1(\alpha), \dots, \sigma\sigma_r(\alpha)\} = \{\sigma_1(\alpha), \dots, \sigma_r(\alpha)\}$. Por lo tanto, $\sigma f(x) = (x - \sigma\sigma_1(\alpha)) \cdots (x - \sigma\sigma_r(\alpha)) = f(x)$. El coeficiente de x^{r-1} del polinomio $\sigma f(x)$ es

$$(-\sigma\sigma_1(\alpha)) - \dots - \sigma\sigma_r(\alpha) = \sigma(-\sigma_1(\alpha) - \dots - \sigma_r(\alpha))$$

y el de $f(x)$ es

$$-\sigma_1(\alpha) - \dots - \sigma_r(\alpha).$$

Se debe tener que

$$\sigma(-\sigma_1(\alpha) - \dots - \sigma_1(\alpha_r)) = -\sigma_1(\alpha) - \dots - \sigma_1(\alpha_r).$$

Así, el coeficiente a_{r-1} de x^{r-1} del polinomio $f(x)$ es invariante por los elementos de H . Esto es, $\sigma_i(a_{r-1}) = a_{r-1}$ para todo $i \in \{1, \dots, r\}$. Por lo tanto, a_{r-1} es un elemento del campo fijo de H , el que denotamos por E . Puede verificarse que la misma situación ocurre con el resto de los coeficientes del polinomio $f(x)$. Es decir, los coeficientes de $f(x)$ son elementos en E . Así, $f(x)$ es un polinomio en $E[x]$ y que se anula en α , de donde $[K : E] \leq r$. Pero $\sigma_1, \dots, \sigma_r$ son r distintos automorfismos de K que fijan E , en consecuencia $[K : E] \geq r$. Por lo tanto, $[K : E] = r$ y $H = G(K/E)$.

d) Sea E_0 un campo tal que $F \leq E_0 \leq E \leq K$. Entonces, $G(K/E) \leq G(K/E_0)$.

Dado $\alpha \in K$ y $f(x)$ el polinomio irreducible de α sobre F . Como $F \leq E_0 \leq E \leq K$, entonces α es también algebraico sobre E_0 . Sea $g(x)$ el polinomio irreducible de α sobre E_0 . Dado que $f(x)$ es irreducible sobre F , también lo es sobre E_0 . Esto implica que $g(x)$ y $f(x)$ tienen las mismas raíces en K .

Consideremos $H = G(K/E)$ y $H_0 = G(K/E_0)$. Luego H y H_0 son subgrupos de $\text{Gal}(K/F)$, y E y E_0 son los campos fijos respectivos de H y H_0 . Dado que α es una raíz de $f(x)$ y $g(x)$ en K , α es fijo por todos los automorfismos en H y H_0 , lo que significa que $\alpha \in E$ y $\alpha \in E_0$.

Por lo tanto, $E_0 = E$ y, en consecuencia, $G(K/E) = G(K/E_0)$.

e) Sea K una extensión normal de F . Si σ está en $G(E/F)$ y τ está en $G(E/K)$, debemos demostrar que $\sigma^{-1}\tau\sigma \in G(E/K)$; es decir, debemos mostrar que $\sigma^{-1}\tau\sigma(\alpha) = \alpha$ para todo $\alpha \in K$. Supongamos que $f(x)$ es el polinomio irreducible de α sobre F . Entonces $\sigma(\alpha)$ también es una raíz de $f(x)$ que está en K , pues K es una extensión normal de F . Luego, $\tau(\sigma(\alpha)) = \sigma(\alpha)$ y $\sigma^{-1}\tau\sigma(\alpha) = \alpha$.

Recíprocamente, sea $G(E/K)$ un subgrupo normal de $G(E/F)$. Debemos demostrar que $F = KG(K/F)$. Sea $\tau \in G(E/K)$. Para todo $\sigma \in G(E/F)$ existe $\tau \in G(E/K)$ tal que $\tau\sigma = \sigma\tau$. De esta manera, para todo $\alpha \in K$

$\tau(\sigma(\alpha)) = \sigma(\tau(\alpha)) = \sigma(\alpha)$; luego, $\sigma(\alpha)$ es el campo fijo de $G(E/K)$. Sea σ la restricción de σ a K . Entonces σ es un automorfismo de K que fija F , pues $\sigma(\alpha) \in K$ para todo $\alpha \in K$; luego, $\sigma \in G(K/F)$.

A continuación, mostraremos que el campo fijo de $G(K/F)$ es F . Sea β un elemento en K que queda fijo por todos los automorfismos en $G(K/F)$. En particular, $\sigma(\beta) = \beta$ para todo $\sigma \in G(E/F)$. Por lo tanto, β pertenece al campo fijo F de $G(E/F)$.

Finalmente, debemos mostrar que si K es una extensión normal de F , entonces

$$G(K/F) \cong G(E/F)/G(E/K).$$

Sea $\sigma \in G(E/F)$, y sea σ_K el automorfismo de K obtenido restringiendo σ a K . Como K es una extensión normal, el argumento del párrafo precedente muestra que $\sigma_K \in G(K/F)$. Tenemos así una función $\phi : G(E/F) \rightarrow G(K/F)$ definida por $\sigma \mapsto \sigma_K$. Esta función es un homomorfismo de grupos pues

$$\phi(\sigma\tau) = (\sigma\tau)_K = \sigma_K\tau_K = \phi(\sigma)\phi(\tau).$$

El núcleo de ϕ es $G(E/K)$. Por (b),

$$\circ(G(E/F))/\circ(G(E/K)) = [K : F] = \circ(G(K/F)).$$

Luego, la imagen de ϕ es $G(K/F)$ y ϕ es sobreyectiva. Por el Primer Teorema de Isomorfía, tenemos

$$G(K/F) \cong G(E/F)/G(E/K).$$

□

Ejemplo 4.12. Consideremos el polinomio $f(x) = x^4 - 3 \in \mathbb{Q}[x]$. Por el criterio de Eisenstein, el polinomio $f(x)$ es irreducible en $\mathbb{Q}[x]$ y las raíces en \mathbb{C} de $f(x)$ son $\sqrt[4]{3}, -\sqrt[4]{3}, \sqrt[4]{3}i, -\sqrt[4]{3}i$. Si $\alpha = \sqrt[4]{3}$, entonces el campo de descomposición de $f(x)$ es

$$K = \mathbb{Q}(\alpha, -\alpha, \alpha i, -\alpha i) = \mathbb{Q}(\alpha, \alpha i) = \mathbb{Q}(\alpha)(\alpha i) = \mathbb{Q}(\alpha)(i) = \mathbb{Q}(\alpha, i)$$

Encontraremos los elementos del grupo de Galois $G(K/\mathbb{Q})$ y la correspondencia biyectiva entre los subcampos de K y los subgrupos de $G(K/\mathbb{Q})$. (Notemos que

cualquier subcampo de K contiene a \mathbb{Q} . Dado que $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$, entonces existen cuatro monomorfismos, $\sigma_1, \sigma_2, \sigma_3, \sigma_4$ de $\mathbb{Q}(\alpha)$ en \mathbb{C} tales que $\sigma_1(\alpha) = \alpha$, $\sigma_2(\alpha) = -\alpha$, $\sigma_3(\alpha) = \alpha i$ y $\sigma_4(\alpha) = -\alpha i$. Dado que $[\mathbb{Q}(\alpha)(i) : \mathbb{Q}(\alpha)] = 2$, entonces cada monomorfismo $\sigma_i : \mathbb{Q}(\alpha) \rightarrow \mathbb{C}$ da origen a dos automorfismos de $\mathbb{Q}(\alpha)(i)$. Si $\tau_1, \tau_2, \dots, \tau_8$ son los automorfismos de $\mathbb{Q}(\alpha)(i)$, entonces

$$\begin{aligned} \tau_1(\alpha) &= \alpha, & \tau_1(i) &= i, \\ \tau_2(\alpha) &= \alpha, & \tau_2(i) &= -i, \\ \tau_3(\alpha) &= -\alpha, & \tau_3(i) &= i, \\ \tau_4(\alpha) &= -\alpha, & \tau_4(i) &= -i, \\ \tau_5(\alpha) &= \alpha i, & \tau_5(i) &= i, \\ \tau_6(\alpha) &= \alpha i, & \tau_6(i) &= -i, \\ \tau_7(\alpha) &= -\alpha i, & \tau_7(i) &= i, \\ \tau_8(\alpha) &= -\alpha i, & \tau_8(i) &= -i. \end{aligned}$$

Por lo tanto, el grupo de Galois de $f(x)$ es

$$G(\mathbb{Q}(\alpha, i)/\mathbb{Q}) = \{\tau_1, \tau_2, \tau_3, \dots, \tau_8\}.$$

La tabla de multiplicación del grupo es

\circ	τ_1	τ_2	τ_3	τ_4	τ_5	τ_6	τ_7	τ_8
τ_1	τ_1	τ_2	τ_3	τ_4	τ_5	τ_6	τ_7	τ_8
τ_2	τ_2	τ_1	τ_4	τ_3	τ_8	τ_7	τ_6	τ_5
τ_3	τ_3	τ_4	τ_1	τ_2	τ_7	τ_8	τ_5	τ_6
τ_4	τ_4	τ_3	τ_2	τ_1	τ_6	τ_5	τ_8	τ_7
τ_5	τ_5	τ_6	τ_7	τ_8	τ_3	τ_4	τ_1	τ_2
τ_6	τ_6	τ_5	τ_8	τ_7	τ_2	τ_1	τ_4	τ_3
τ_7	τ_7	τ_8	τ_5	τ_6	τ_1	τ_2	τ_3	τ_4
τ_8	τ_8	τ_7	τ_6	τ_5	τ_4	τ_3	τ_2	τ_1

4.4. Teorema Fundamental de la Teoría de Galois

Los subgrupos cíclicos de $G(\mathbb{Q}(\alpha, i)/\mathbb{Q})$ son $\langle \tau_1 \rangle = \{\tau_1\}$, $\langle \tau_2 \rangle = \{\tau_1, \tau_2\}$, $\langle \tau_3 \rangle = \{\tau_1, \tau_3\}$, $\langle \tau_4 \rangle = \{\tau_1, \tau_4\}$, $\langle \tau_5 \rangle = \{\tau_1, \tau_5, \tau_3, \tau_7\}$, $\langle \tau_6 \rangle = \{\tau_1, \tau_6\}$, $\langle \tau_7 \rangle = \langle \tau_5 \rangle$, $\langle \tau_8 \rangle = \{\tau_1, \tau_8\}$.

Existen otros subgrupos de $G(\mathbb{Q}(\alpha, i)/\mathbb{Q})$ que no son cíclicos los cuales son

$$\{\tau_1, \tau_2, \tau_3, \tau_4\} \text{ y } \{\tau_1, \tau_3, \tau_6, \tau_8\}$$

. Encontraremos los campos fijos de cada subgrupo de $G(K/\mathbb{Q})$. Sabemos que

$$\{1, \alpha, \alpha^2, \alpha^3, i, \alpha i, \alpha^2 i, \alpha^3 i\}$$

es una base de K como espacio vectorial sobre \mathbb{Q} . Encontraremos $K^{\langle \tau_1, \tau_3 \rangle} = \{x \in K \mid \tau_3(x) = x\}$. Si

$$\begin{aligned} \tau_3(a_0 + a_1\alpha + a_2\alpha^2 + a_3\alpha^3 + a_4i + a_5\alpha i + a_6\alpha^2 i + a_7\alpha^3 i) \\ = a_0 + a_1\alpha + a_2\alpha^2 + a_3\alpha^3 + a_4i + a_5\alpha i + a_6\alpha^2 i + a_7\alpha^3 i, \end{aligned}$$

entonces

$$\begin{aligned} a_0 - a_1\alpha + a_2\alpha^2 - a_3\alpha^3 + a_4i - a_5\alpha i + a_6\alpha^2 i - a_7\alpha^3 i = a_0 + a_1\alpha + a_2\alpha^2 + a_3\alpha^3 \\ + a_4i + a_5\alpha i + a_6\alpha^2 i + a_7\alpha^3 i, \end{aligned}$$

de donde

$$\begin{aligned} K^{\langle \tau_1, \tau_3 \rangle} &= \{a_0 + a_2\alpha^2 + a_4i + a_6\alpha^2 i \mid a_0, a_2, a_4, a_6 \in \mathbb{Q}\} \\ &= \mathbb{Q}(\sqrt{3}, i) \\ &= \mathbb{Q}(\sqrt{9}, i). \end{aligned}$$

Encontraremos $K^{\langle \tau_1, \tau_3, \tau_6, \tau_8 \rangle} = \{x \in K \mid \tau_3(x) = x \wedge \tau_6(x) = x \wedge \tau_8(x) = x\}$.

Sabemos que

$$\tau_3(a_0 + a_2\alpha^2 + a_4i + a_6\alpha^2 i) = a_0 + a_2\alpha^2 + a_4i + a_6\alpha^2 i.$$

Ahora,

$$\tau_6(a_0 + a_2\alpha^2 + a_4i + a_6\alpha^2 i) = a_0 + a_2\alpha^2 + a_4i + a_6\alpha^2 i$$

implica que

$$a_0 - a_2\alpha^2 - a_4i + a_6\alpha^2 i = a_0 + a_2\alpha^2 + a_4i + a_6\alpha^2 i.$$

Luego,

$$\tau_6(a_0 + a_6\alpha^2i) = a_0 + a_6\alpha^2i.$$

Dado que $\tau_8(a_0 + a_6\alpha^2i) = a_0 + a_6\alpha^2i$, entonces

$$K^{\langle\tau_1, \tau_3, \tau_6, \tau_8\rangle} = \{a_0 + a_6\alpha^2i \mid a_0, a_6 \in \mathbb{Q}\} = \mathbb{Q}(\sqrt{9}i) = \mathbb{Q}(\sqrt{3}i).$$

En forma similar se encuentran los campos fijos restantes correspondientes a cada subgrupo de $G(K/\mathbb{Q})$. Se obtienen

$$K^{\langle\tau_1, \tau_2\rangle} = \mathbb{Q}(\sqrt[4]{3})$$

$$K^{\langle\tau_1, \tau_4\rangle} = \mathbb{Q}(\sqrt[4]{3}i)$$

$$K^{\langle\tau_1, \tau_6\rangle} = \mathbb{Q}(\sqrt[4]{3} + \sqrt[4]{3}i)$$

$$K^{\langle\tau_1, \tau_8\rangle} = \mathbb{Q}(\sqrt[4]{3} - \sqrt[4]{3}i)$$

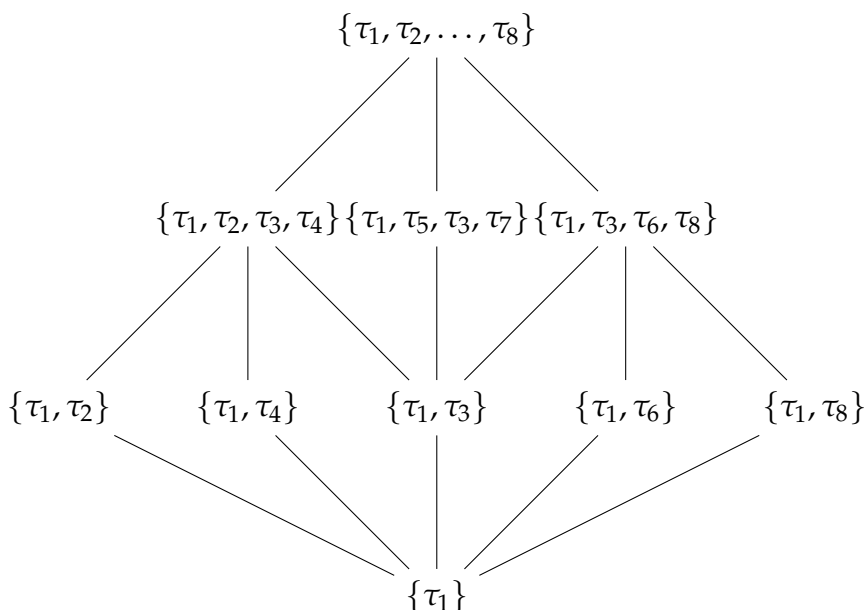
$$K^{\langle\tau_1, \tau_2, \tau_3, \tau_4\rangle} = \mathbb{Q}(\sqrt{3})$$

$$K^{\langle\tau_1, \tau_5, \tau_3, \tau_7\rangle} = \mathbb{Q}(i).$$

De esta forma, la correspondencia biyectiva es:

$$\begin{aligned} \mathbb{Q} &\longrightarrow G(\mathbb{Q}(\alpha, i)/\mathbb{Q}) \\ \mathbb{Q}(\sqrt{3}, i) &\longrightarrow \{\tau_1, \tau_3\} \\ \mathbb{Q}(\sqrt[4]{3}) &\longrightarrow \{\tau_1, \tau_2\} \\ \mathbb{Q}(\sqrt[4]{3}i) &\longrightarrow \{\tau_1, \tau_4\} \\ \mathbb{Q}(\sqrt[4]{3} + \sqrt[4]{3}i) &\longrightarrow \{\tau_1, \tau_6\} \\ \mathbb{Q}(\sqrt[4]{3} - \sqrt[4]{3}i) &\longrightarrow \{\tau_1, \tau_8\} \\ \mathbb{Q}(\sqrt{3}) &\longrightarrow \{\tau_1, \tau_2, \tau_3, \tau_4\} \\ \mathbb{Q}(i) &\longrightarrow \{\tau_1, \tau_5, \tau_3, \tau_7\} \\ \mathbb{Q}(\sqrt{3}i) &\longrightarrow \{\tau_1, \tau_3, \tau_6, \tau_8\}. \end{aligned}$$

La correspondencia biyectiva se representa por el siguiente diagrama



4.5 El grupo de Galois de un polinomio de Grado 3

Estudiaremos a continuación el grupo de Galois de un polinomio de grado 3 sobre un campo F . Consideramos el polinomio $f(x) = x^3 + ax^2 + bx + c \in F[x]$, dicho polinomio es equivalente a,

$$f(x) = \left(x + \frac{1}{3}a\right)^3 + \left(b - \frac{1}{3}a^2\right) \left(x + \frac{1}{3}a\right) + c - \frac{1}{3}ab + \frac{2}{27}a^3.$$

Para verificar dicha equivalencia manipulamos el polinomio $f(x) = x^3 + ax^2 + bx + c$, primero añadiendo y restando términos para completar el cubo perfecto:

$$f(x) = x^3 + ax^2 + bx + c = x^3 + ax^2 + \frac{a^2}{3}x^2 - \frac{a^2}{3}x^2 + bx + c,$$

agrupando términos convenientemente tenemos lo siguiente:

$$\begin{aligned} &= \left(x^3 + \frac{a^2}{3}x^2\right) + \left(ax^2 - \frac{a^2}{3}x^2 + bx\right) + c \\ &= \left(x^3 + \frac{a^2}{3}x^2\right) + \left(\left(x - \frac{a}{3}\right)^2\right) + c - \frac{a^2}{9} \\ &= \left(x + \frac{a}{3}\right)^3 + \left(b - \frac{a^2}{3}\right) \left(x + \frac{a}{3}\right) + c - \frac{a^2}{9} \\ &= \left(x + \frac{a}{3}\right)^3 + \left(b - \frac{a^2}{3}\right) \left(x + \frac{a}{3}\right) + c - \frac{1}{3}ab + \frac{2}{27}a^3. \end{aligned}$$

Así verificamos que el polinomio $f(x) = x^3 + ax^2 + bx + c$ es equivalente al polinomio $f(x) = \left(x + \frac{1}{3}a\right)^3 + \left(b - \frac{1}{3}a^2\right)\left(x + \frac{1}{3}a\right) + c - \frac{1}{3}ab + \frac{2}{27}a^3$.

Luego, sea $y = x + \frac{1}{3}a$ y consideremos el polinomio

$$g(y) = y^3 + \left(b - \frac{1}{3}a^2\right)y + c - \frac{1}{3}ab + \frac{2}{27}a^3.$$

Ahora, si $\beta \in \mathbb{C}$ es una raíz de $f(x)$, entonces $\beta + \frac{1}{3}a$ es una raíz de $g(y)$. En efecto,

$$\begin{aligned} g\left(\beta + \frac{1}{3}a\right) &= \left(\beta + \frac{1}{3}a\right)^3 + \left(b - \frac{1}{3}a^2\right)\left(\beta + \frac{1}{3}a\right) + c - \frac{1}{3}ab + \frac{2}{27}a^3 \\ &= c + b\beta + \beta^3 + a\beta^2 = 0. \end{aligned}$$

Además, si $\gamma \in \mathbb{C}$ es una raíz de $g(y)$, entonces $\gamma - \frac{1}{3}a$ es una raíz de $f(x)$. Por lo tanto, obtenemos el siguiente resultado:

Lema 4.4

Sea F un campo. Entonces, los polinomios $f(x) = x^3 + ax^2 + bx + c \in F[x]$ y $g(x) = x^3 + \left(b - \frac{1}{3}a^2\right)x + c - \frac{1}{3}ab + \frac{2}{27}a^3 \in F[x]$ tienen el mismo campo de descomposición.

Luego, para saber cuál es el grupo de Galois que le corresponde a un polinomio de grado 3 sobre un campo F , basta estudiar polinomios de la forma $f(x) = x^3 + bx + c \in F[x]$.

Sea $p(x) = x^3 + bx + c \in F[x]$ irreducible en $F[x]$ y $\alpha, \beta, \gamma \in \mathbb{C}$ las raíces de $p(x)$. De la relación existente entre las raíces de $p(x)$ y sus coeficientes, obtenemos $\alpha + \beta + \gamma = 0$, $\alpha\beta + \alpha\gamma + \beta\gamma = b$ y $\alpha\beta\gamma = -c$.

Sea $\delta = (\alpha - \beta)(\alpha - \gamma)(\beta - \gamma)$. Sea $\delta = (\alpha - \beta)(\alpha - \gamma)(\beta - \gamma)$. A continuación desarrollaremos el resultado de δ^2 .

δ :

$$\delta = (\alpha - \beta)(\alpha - \gamma)(\beta - \gamma)$$

4.5. El grupo de Galois de un polinomio de Grado 3

desarrollando, δ^2 :

$$\begin{aligned}\delta^2 &= (\alpha - \beta)^2(\alpha - \gamma)^2(\beta - \gamma)^2 \\ &= (\alpha^2 - 2\alpha\beta + \beta^2)(\alpha^2 - 2\alpha\gamma + \gamma^2)(\beta^2 - 2\beta\gamma + \gamma^2) \\ &= (\alpha^2\beta^2 - 2\alpha\beta^3 + \beta^4)(\alpha^2\gamma^2 - 2\alpha\gamma^3 + \gamma^4)(\beta^2\gamma^2 - 2\beta\gamma^3 + \gamma^4) \\ &= \alpha^2\beta^2\gamma^2 \cdot (\alpha^2 - 2\beta^2 + \beta^4)(\alpha^2 - 2\gamma^2 + \gamma^4)(\beta^2 - 2\gamma^2 + \gamma^4).\end{aligned}$$

Luego relacionando con los coeficientes del polinomio $p(x)$:

$$\alpha + \beta + \gamma = 0$$

$$\alpha\beta + \alpha\gamma + \beta\gamma = b$$

$$\alpha\beta\gamma = -c$$

hacemos uso de las relaciones para simplificar, llegando así que

$$\delta^2 = -4b^3 - 27c^2.$$

Luego, $\delta^2 \in F$. Reemplazando $\gamma = -\alpha - \beta$ en $\delta = (\alpha - \beta)(\alpha - \gamma)(\beta - \gamma)$ y en $\alpha\beta + \alpha\gamma + \beta\gamma = b$, respectivamente, obtenemos que

$$\delta = (\alpha - \beta)(5\alpha\beta + 2\alpha^2 + 2\beta^2)$$

y

$$\alpha\beta + \alpha^2 + \beta^2 = -b.$$

De estas últimas dos relaciones, $\delta = (\alpha - \beta)(5\alpha\beta + 2(-b - \alpha\beta)) = 2b\beta - 2b\alpha - 3\alpha\beta^2 + 3\alpha^2\beta$.

Dado que $\alpha\beta\gamma = \alpha\beta(-\alpha - \beta) = -c$, entonces $\alpha\beta^2 = c - \alpha^2\beta$. Por lo tanto,

$$\delta = 2b\beta - 2b\alpha - 3(c - \alpha^2\beta) + 3\alpha^2\beta = 2b\beta - 2b\alpha - 3c + 6\alpha^2\beta.$$

Así, $\beta(6\alpha^2 + 2b) = \delta + 2b\alpha + 3c$.

Notemos que $6\alpha^2 + 2b \neq 0$, de lo contrario $p(x)$ no sería el polinomio irreducible de α sobre F . Concluimos que $\beta = \frac{\delta + 2b\alpha + 3c}{6\alpha^2 + 2b}$, de donde $\beta \in F(\delta, \alpha)$.

A partir del estudio previo realizado obtenemos como resultado el siguiente teorema:

Teorema 4.8

Sea F un campo y $p(x) = x^3 + bx + c \in F[x]$ irreducible en $F[x]$. Entonces $K = F(\delta_0, \alpha)$ es el campo de descomposición de $p(x)$, donde $\delta_0 \in \mathbb{C}$ es una raíz del polinomio $q(x) = x^2 + 4b^3 + 27c^2$ y $\alpha \in \mathbb{C}$ es una raíz de $p(x)$.

Demostración. Sean $\alpha, \beta, \gamma \in \mathbb{C}$ las raíces de $p(x)$, entonces el campo de descomposición de $p(x)$ es $K = F(\alpha, \beta, \gamma)$. Por lo demostrado anteriormente $\beta \in F(\delta, \alpha)$, donde $\delta = (\alpha - \beta)(\alpha - \gamma)(\beta - \gamma)$. Dado que $\alpha + \beta + \gamma = 0$, entonces $\gamma \in F(\delta, \alpha)$. Claramente $K = F(\alpha, \beta, \gamma) = F(\delta, \alpha)$. Como δ es una raíz de $q(x)$, entonces $\delta_0 = \delta$ o $\delta_0 = -\delta$. Concluimos que $K = F(\delta_0, \alpha)$. \square

Corolario 4.5

Sea F un campo, $p(x) = x^3 + bx + c \in F[x]$ irreducible en $F[x]$ y K el campo de descomposición de $p(x)$.

- a) Si $-4b^3 - 27c^2$ es un cuadrado en F , entonces $G(K/F)$ es un grupo de orden 3, es decir, isomorfo a $(\mathbb{Z}_3, +)$.
- b) Si $-4b^3 - 27c^2$ no es un cuadrado en F , entonces $G(K/F)$ es un grupo isomorfo a S_3 .

Demostración. a) Si $-4b^3 - 27c^2$ es un cuadrado en F , entonces existe $\delta_0 \in F$ una raíz de $q(x) = x^2 + 4b^3 + 27c^2$. Si $\alpha \in \mathbb{C}$ es una raíz de $p(x)$, entonces por el Teorema 4.8, $K = F(\delta_0, \alpha) = F(\alpha)$. Dado que $[F(\alpha) : F] = 3$, obtenemos que $G(K/F)$ es un grupo de orden 3.

- b) Si $-4b^3 - 27c^2$ no es un cuadrado en F , entonces el polinomio $q(x) = x^2 + 4b^3 + 27c^2$ no tiene raíces en F y por lo tanto, es irreducible en $F[x]$. Como $\delta = (\alpha - \beta)(\alpha - \gamma)(\beta - \gamma)$ es una raíz de $q(x)$, entonces $q(x)$ es el polinomio irreducible de δ sobre F . Si $\alpha \in \mathbb{C}$ es una raíz de $p(x)$, por el Teorema 4.8, $K = F(\delta, \alpha)$. Dado que $[F(\delta) : F] = 2$ y $[F(\alpha) : F] = 3$ son divisores de $[K : F]$, entonces 6 es un divisor de $[K : F]$. Luego tenemos que, $[K : F] = 6$. Por lo tanto, $G(K/F)$ es un grupo isomorfo a S_3 .

□

Ejemplo 4.13. Encontraremos el grupo de Galois del polinomio

$$p(x) = x^3 - 5x + 1 \in \mathbb{Q}[x]$$

. Dado que al considera $p = 5$, haciendo uso del criterio de Eisenstein deducimos que $p(x)$ es irreducible en $\mathbb{Q}[x]$, luego por el corolario previo

$$\begin{aligned} -4b^3 - 27c^2 &= -4(-5)^3 - 27(7)^2 \\ &= 500 - 1323 \\ &= -823. \end{aligned}$$

Ahora, $-4b^3 - 27c^2 = -823$ no es un cuadrado en \mathbb{Q} . Por lo tanto, el grupo de Galois es isomorfo a S_3

Ejemplo 4.14. Encontraremos el grupo de Galois del polinomio $p(x) = x^3 - x - 1 \in \mathbb{Q}(\sqrt{23}i)[x]$. Determinaremos si $p(x)$ es irreducible o reducible en $\mathbb{Q}(\sqrt{23}i)[x]$.

Supongamos que $p(x)$ tiene una raíz en el campo $\mathbb{Q}(\sqrt{23}i) = \{a + b\sqrt{23}i \mid a, b \in \mathbb{Q}\}$. Entonces, existen $a, b \in \mathbb{Q}$ tales que $a + b\sqrt{23}i$ es una raíz de $p(x)$. Luego,

$$a^3 - a - 69ab^2 - 1 + b(3a^2 - 1 - 23b^2)\sqrt{23}i = 0,$$

de donde $a^3 - a - 69ab^2 - 1 = 0$ y $b(3a^2 - 1 - 23b^2) = 0$. Así, $b = 0$ o $3a^2 - 1 - 23b^2 = 0$.

Si $b = 0$, entonces $p(x)$ tiene una raíz en \mathbb{Q} , lo cual es una contradicción. Si $3a^2 - 1 - 23b^2 = 0$, entonces de $a^3 - a - 69ab^2 - 1 = 0$ obtenemos que $8a^3 - 2a + 1 = 0$, lo cual implica que el polinomio $8x^3 - 2x + 1$ tiene una raíz en \mathbb{Q} . Es fácil verificar que dicho polinomio no tiene raíces en \mathbb{Q} . Hemos demostrado que $p(x)$ es irreducible en $\mathbb{Q}(\sqrt{23}i)[x]$.

Ahora,

$$-4b^3 - 27c^2 = -4(-1)^3 - 27(-1)^2 = -23$$

es un cuadrado en $\mathbb{Q}(\sqrt{23}i)$. Por lo tanto, el grupo de Galois de $p(x)$ es un grupo de orden 3.

4.6 El Grupo de Galois del Polinomio $x^n - 1$

En esta demostración, exploraremos propiedades de la estructura del grupo de Galois del polinomio $f(x) = x^n - 1$ sobre \mathbb{Q} y demostraremos su naturaleza abeliana. En el caso particular en que $n = p$ es un número primo, mostraremos que el grupo es cíclico.

Definición 4.7

Un número complejo ω se dice que es una raíz primitiva n -ésima de la unidad, si $\omega^n = 1$, pero $\omega^m \neq 1$ para cualquier entero positivo $m < n$.

Observación 4.2. Si ω es una raíz primitiva n -ésima de la unidad, entonces $\omega, \omega^2, \dots, \omega^{n-1}, \omega^n = 1$ son todos distintos. Esta afirmación se fundamenta en que si existen $p, q \in \mathbb{Z}$ tales que $\omega^p = \omega^q$ con $1 \leq p < q \leq n$, entonces $\omega^{q-p} = 1$ con $1 \leq q - p < n$, lo cual lleva a una contradicción. En consecuencia, $x^n - 1 = (x - 1)(x - \omega) \cdots (x - \omega^{n-1})$.

Observación 4.3. Sabemos que $\omega = \cos\left(\frac{2\pi}{n}\right) + i \operatorname{sen}\left(\frac{2\pi}{n}\right)$ es una raíz n -ésima primitiva de la unidad.

Demostraremos primero que el conjunto $C_n = \{\alpha \in \mathbb{C} \mid \alpha^n = 1\}$ es un grupo con el producto usual de \mathbb{C} . Para esto debemos verificar que sea cerrado bajo el producto, existencia del elemento neutro, la asociatividad y la existencia de inversos.

Cerradura: Sea $\alpha, \beta \in C_n$, entonces $\alpha \cdot \beta \in C_n$ ya que

$$(\alpha \cdot \beta)^n = \alpha^n \cdot \beta^n = 1 \cdot 1 = 1.$$

Asociatividad: Dado que el conjunto de \mathbb{C} es asociativa, entonces C_n también es asociativa.

Sea $\alpha, \beta, \gamma \in \mathbb{C}_n$, entonces $(\alpha \cdot (\beta \cdot \gamma)) = ((\alpha \cdot \beta) \cdot \gamma)$

$$\begin{aligned} (\alpha^n \cdot (\beta^n \cdot \gamma^n)) &= (\alpha^n \cdot (\beta \cdot \gamma)^n) \\ &= (\alpha \cdot \beta \cdot \gamma)^n \\ &= ((\alpha \cdot \beta)^n \cdot \gamma^n) \\ &= ((\alpha^n \cdot \beta^n) \cdot \gamma^n). \end{aligned}$$

Elemento Neutro: El número complejo 1 es el elemento neutro en \mathbb{C} , y $1^n = 1$. Por lo tanto, 1 es el elemento neutro en \mathbb{C}_n

Inverso: Para cada $\alpha \in \mathbb{C}_n$, existe un $\alpha^{-1} \in \mathbb{C}$ tal que $\alpha \cdot \alpha^{-1} = \alpha^{-1} \cdot \alpha = 1$. Dado que $\alpha^n = 1$ implica que $\alpha^{-n} = 1$ y por lo tanto, α^{-1} es el inverso de α .

Además, \mathbb{C}_n es un grupo cíclico dado que $\omega = \cos\left(\frac{2\pi}{n}\right) + i \sin\left(\frac{2\pi}{n}\right)$ es un generador de \mathbb{C}_n . De la teoría de grupos, sabemos que si m es un entero primo relativo con n , entonces ω^m también es un generador del grupo \mathbb{C}_n . Además, \mathbb{C}_n tiene $\phi(n)$ generadores, siendo $\phi: \mathbb{Z}^+ \rightarrow \mathbb{Z}^+$ la función definida por $\phi(n) = s$, donde s es el número de enteros positivos menores o iguales a n y primos relativos con n . Dicha función es conocida como la función ϕ de Euler. Concluimos que existen $\phi(n)$ raíces primitivas n -ésimas de la unidad.

Lema 4.5

Si ω es una raíz primitiva n -ésima de la unidad, entonces se tiene que $Q(1, \omega, \dots, \omega^{n-1}) = Q(\omega)$ es el campo de descomposición del polinomio $f(x) = x^n - 1$ sobre \mathbb{Q} . Por lo tanto, $Q(\omega)$ es una extensión de Galois de \mathbb{Q} .

Demostración. A partir de la observación anterior se verifica dicho lema. □

Definición 4.8

El polinomio $\phi_n(x) = (x - \omega_1)(x - \omega_2) \dots (x - \omega_{\phi(n)})$, donde $\omega_1, \omega_2, \dots, \omega_{\phi(n)}$ son las raíces primitivas n -ésimas de la unidad, se llama el n -ésimo **polinomio ciclotómico**.

Teorema 4.9

El n -ésimo polinomio ciclotómico $\phi_n(x)$ es un elemento en $\mathbb{Q}[x]$ e irreducible sobre \mathbb{Q} .

Demostración. El lector puede revisar la demostración en [3] de la bibliografía. \square

Corolario 4.6

El grupo de Galois del polinomio $f(x) = x^n - 1$ sobre \mathbb{Q} tiene $\phi(n)$ elementos.

Demostración. Si ω es una raíz primitiva n -ésima de la unidad, del Lema 4.5, $K = \mathbb{Q}(\omega)$ es una extensión de Galois de \mathbb{Q} . Por el Teorema 4.9, $\phi_n(x)$ es el polinomio irreducible de ω sobre \mathbb{Q} . Por lo tanto, el grupo de Galois $G(K/\mathbb{Q})$ tiene $\deg(\phi_n) = \phi(n)$ elementos. \square

Ejemplo 4.15. Encontraremos el grupo de Galois del polinomio $f(x) = x^8 - 1$ sobre \mathbb{Q} . Sabemos que, $\omega = \cos\left(\frac{\pi}{4}\right) + i \sin\left(\frac{\pi}{4}\right) = \frac{1}{2}\sqrt{2} + \frac{1}{2}\sqrt{2}i$ es un generador del grupo $\mathbb{C}_8 = \{\alpha \in \mathbb{C} \mid \alpha^8 = 1\}$. El campo de descomposición de $f(x)$ es $\mathbb{Q}(\omega)$ y el polinomio irreducible $\phi_8(x)$ asociado a la raíz primitiva octava de la unidad ω sobre \mathbb{Q} es:

$$\begin{aligned} \phi_8(x) &= (x - \omega)(x - \omega^3)(x - \omega^5)(x - \omega^7) \\ &= \left(x + \frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2}i\right)\left(x - \frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2}i\right)\left(x - \frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i\right)\left(x + \frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i\right) \\ &= \left(x^2 - \frac{1}{2}\right)^2\left(x^2 + \frac{1}{2}\right)^2 \\ &= \left(x^4 - x^2 + \frac{1}{4}\right)\left(x^4 + x^2 + \frac{1}{4}\right) \\ &= x^8 - x^6 + \frac{1}{2}x^4 - \frac{1}{4}. \end{aligned}$$

Por lo tanto, $\phi_8(x) = x^8 - x^6 + \frac{1}{2}x^4 - \frac{1}{4}$ es el polinomio irreducible de ω sobre \mathbb{Q} . Para el polinomio $f(x) = x^8 - 1$ sobre \mathbb{Q} , consideramos las raíces primitivas octavas de la unidad, denotadas como ω_k , donde k es un entero tal que $1 \leq k \leq 7$. Cada una de estas raíces está asociada a un automorfismo τ_k en el grupo de Galois $G(\mathbb{Q}(\omega)/\mathbb{Q})$, definido como $\tau_k(\omega) = \omega^k$.

Para explorar la acción de algunos de estos automorfismos, observemos específicamente $\tau_2^2(\omega)$ y $\tau_3^2(\omega)$. Calculamos:

$$\tau_2^2(\omega) = \tau_2(\tau_2(\omega)) = \tau_2(\omega^2) = (\tau_2(\omega))^2 = (\omega^2)^2 = \omega^4,$$

$$\tau_3^2(\omega) = \tau_3(\tau_2(\omega)) = \tau_3(\omega^2) = (\tau_3(\omega))^2 = (\omega^3)^2 = \omega^6.$$

Siguiendo un razonamiento similar, se obtienen los resultados para $\tau_4^2(\omega)$, $\tau_5^2(\omega)$, $\tau_6^2(\omega)$, y $\tau_7^2(\omega)$:

$$\tau_4^2(\omega) = \omega^8 = 1,$$

$$\tau_5^2(\omega) = \omega^2,$$

$$\tau_6^2(\omega) = \omega^4,$$

$$\tau_7^2(\omega) = \omega^6.$$

Notamos que $\tau_7^2(\omega)$ es equivalente a $\tau_2(\omega)$, ya que $\omega^8 = 1$ implica $\omega^9 = \omega$. De manera similar, se obtienen los productos para otros τ_k .

\circ	τ_1	τ_2	τ_3	τ_4	τ_5	τ_6	τ_7
τ_1	τ_1	τ_2	τ_3	τ_4	τ_5	τ_6	τ_7
τ_2	τ_2	τ_4	τ_6	1	τ_2	τ_4	τ_6
τ_3	τ_3	τ_6	τ_1	τ_4	τ_7	τ_2	τ_5
τ_4	τ_4	1	τ_4	1	τ_4	1	τ_4
τ_5	τ_5	τ_2	τ_7	τ_4	τ_1	τ_6	τ_3
τ_6	τ_6	τ_4	τ_2	1	τ_6	τ_4	τ_2
τ_7	τ_7	τ_6	τ_5	τ_4	τ_3	τ_2	τ_1

Teorema 4.10

El grupo de Galois del polinomio $f(x) = x^n - 1$ sobre \mathbb{Q} es isomorfo a U_n .

Luego, el grupo de Galois es Abeliano.

Demostración. Sea ω una raíz primitiva de la unidad. Entonces, $K = \mathbb{Q}(\omega)$ es el campo de descomposición de $f(x)$ y $[K : \mathbb{Q}] = \varphi(n)$. Si σ es un elemento en el grupo de Galois $G(K/\mathbb{Q})$, entonces $\sigma(\omega)$ es una raíz del n -ésimo polinomio

ciclotómico $\phi_n(x)$ y, por lo tanto, existe un entero positivo k tal que $\sigma(\omega) = \omega^k$ con $(k, n) = 1$.

Observemos que, si $k \equiv s \pmod{n}$, entonces existe $q \in \mathbb{Z}$ tal que $k = s + nq$. Luego,

$$\sigma(\omega) = \omega^k = \omega^{s+nq} = \omega^s(\omega^n)^q = \omega^s.$$

Definamos una función $\Psi : G(K/\mathbb{Q}) \rightarrow U_n$ por $\Psi(\sigma) = \bar{k}$. Sean σ, τ elementos en $G(K/\mathbb{Q})$. Existen enteros k, r tales que $\sigma(\omega) = \omega^k$ y $\tau(\omega) = \omega^r$ con $(k, n) = 1$ y $(r, n) = 1$.

Demostraremos que Ψ es un homomorfismo de grupos. Dado que $\sigma\tau(\omega) = \sigma(\tau(\omega)) = \sigma(\omega^r) = \sigma(\omega)^r = (\omega^k)^r = \omega^{kr}$, entonces

$$\Psi(\sigma\tau) = \overline{k \cdot r} = \bar{k} \cdot \bar{r} = \Psi(\sigma)\Psi(\tau).$$

Demostraremos a continuación que Ψ es inyectiva. Si $\Psi(\sigma) = \bar{1}$, entonces $\sigma(\omega) = \omega$. Un elemento cualquiera β de $K = \mathbb{Q}(\omega)$ es de la forma $\beta = \sum_{i=0}^{\varphi(n)-1} a_i \omega^i$, donde $a_0, a_1, \dots, a_{\varphi(n)-1}$ son elementos en \mathbb{Q} . Ahora,

$$\sigma(\beta) = \sum_{i=0}^{\varphi(n)-1} \sigma(a_i \omega^i) = \sum_{i=0}^{\varphi(n)-1} a_i \sigma(\omega^i) = \sum_{i=0}^{\varphi(n)-1} a_i \omega^i = \beta,$$

lo cual demuestra que $\sigma = \text{id}_K$ (donde id_K es la función identidad de K) y por lo tanto, Ψ es inyectiva.

Como $G(K/\mathbb{Q})$ y U_n son grupos con $\varphi(n)$ elementos, entonces Ψ es sobreyectiva. □

Corolario 4.7

Si p es un número primo, entonces el grupo de Galois del polinomio $f(x) = x^p - 1$ es cíclico con $p - 1$ elementos.

Demostración. Por el teorema anterior, el grupo de Galois del polinomio $f(x) = x^p - 1$ sobre \mathbb{Q} es isomorfo a U_p . Pero $U_p = \mathbb{Z}_p - \{0\}$ y dado que \mathbb{Z}_p es un campo finito con p elementos, entonces $\mathbb{Z}_p - 0$ es un grupo cíclico con el producto de \mathbb{Z}_p con $p - 1$ elementos. □

4.7 Solubilidad por Radicales

Teorema 4.11

Sea F un campo y $f(x) = x^3 + ax^2 + bx + c \in F[x]$. Entonces $f(x)$ es soluble por radicales sobre F .

Demostración. En la sección 4.5, se estudia que los polinomios $f(x) = x^3 + ax^2 + bx + c$ y $g(x) = x^3 + \left(b - \frac{1}{3}a^2\right)x + c - \frac{1}{3}ab + \frac{2}{27}a^3$ están relacionados por la siguiente propiedad: Si $\beta \in \mathbb{C}$ es una raíz de $f(x)$, entonces $\beta + \frac{1}{3}a$ es una raíz de $g(x)$, y si $\gamma \in \mathbb{C}$ es una raíz de $g(x)$, entonces $\gamma - \frac{1}{3}a$ es una raíz de $f(x)$. Por lo tanto, los campos de descomposición de $f(x)$ y $g(x)$ son iguales. De esta forma, para encontrar las raíces de $f(x)$, basta con encontrar las raíces del polinomio

$$g(x) = x^3 + px + q, \quad (4.1)$$

donde $p = b - \frac{1}{3}a^2$ y $q = c - \frac{1}{3}ab + \frac{2}{27}a^3$. Si suponemos que $p = 0$, entonces las soluciones de $x^3 + q = 0$ serán las raíces cúbicas de $-q$. Ahora, si suponemos que $q = 0$, entonces las soluciones de $x^3 + px = x(x^2 + p) = 0$ serán 0 y las raíces cuadradas de $-p$. Podemos suponer que $pq \neq 0$. Consideremos la ecuación cuadrática

$$x^2 + qx - \frac{1}{27}p^3 = 0, \quad (4.2)$$

cuyas soluciones son no nulas. Como

$$\frac{1}{2} \left(-q \pm \sqrt{q^2 + \frac{4}{27}p^3} \right) = -\frac{1}{2}q \pm \sqrt{\frac{1}{4}q^2 + \frac{1}{27}p^3}.$$

Por lo tanto, las soluciones de esta ecuación son: $-\frac{1}{2}q + \delta$ y $-\frac{1}{2}q - \delta$, donde $\delta \in \mathbb{C}$ y $\delta^2 = \frac{1}{4}q^2 + \frac{1}{27}p^3$.

Sea $u \in \mathbb{C}$ tal que $u^3 = -\frac{1}{2}q + \delta$. Si $v = -\frac{p}{3u}$, entonces $v^3 = -\frac{1}{2}q - \delta$. En efecto,

$$\begin{aligned} v^3 &= -\frac{p^3}{27u^3} = -\frac{p^3}{27\left(-\frac{1}{2}q + \delta\right)} = \frac{p^3\left(\frac{1}{2}q - \delta\right)}{27\left(\frac{1}{4}q^2 - \delta^2\right)} \\ &= -\frac{p^3}{27\left(-\frac{1}{2}q - \delta\right)} = \frac{p^3\left(-\frac{1}{2}q - \delta\right)}{p^3} = -\frac{1}{2}q - \delta. \end{aligned}$$

Ahora, sabemos que

$$u^3 + v^3 = -q \quad \text{y} \quad 3uv + p = 0. \quad (4.3)$$

Utilizando estas relaciones, obtenemos que

$$(u + v)^3 + p(u + v) + q = u^3 + v^3 + (3uv + p)(u + v) + q = 0,$$

lo que demuestra que $u + v$ es una raíz de (1). Esta solución se puede escribir como

$$\sqrt[3]{-\frac{1}{2}q + \sqrt{\frac{1}{4}q^2 + \frac{1}{27}p^3}} + \sqrt[3]{-\frac{1}{2}q - \sqrt{\frac{1}{4}q^2 + \frac{1}{27}p^3}}.$$

Si $\omega \neq 1$ es una raíz cúbica primitiva de la unidad, es decir, si $\omega = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$ o $\omega = -\frac{1}{2} - \frac{\sqrt{3}}{2}i$, entonces se puede verificar que $u\omega + v\omega^2$ y $u\omega^2 + v\omega$ también son raíces de $g(x)$. \square

Ejemplo 4.16. Utilizando el método dado en la demostración del Teorema 4.11, encontraremos todas las raíces en \mathbb{C} del polinomio $f(x) = x^3 + 3ix - 1 - i$. Claramente, $p = 3i$ y $q = -1 - i$. La ecuación (4.2) es $x^2 - (1 + i)x + i = 0$. Una solución de esta ecuación es $\delta = i$. Una raíz cúbica de i es $u = \frac{1}{2}\sqrt{3} + \frac{1}{2}i$. Ahora, $v = -\frac{1}{3}iu = -\frac{1}{2} - \frac{1}{2}\sqrt{3}i$. Las soluciones de $f(x)$ son:

$$\begin{aligned} u + v &= \frac{1}{2}\sqrt{3} - \frac{1}{2} + \left(\frac{1}{2} - \frac{1}{2}\sqrt{3}\right)i, \\ u\omega + v\omega^2 &= u\left(-\frac{1}{2} + \frac{1}{2}\sqrt{3}i\right) + v\left(-\frac{1}{2} + \frac{1}{2}\sqrt{3}i\right)^2 \\ &= -\frac{1}{2}\sqrt{3} - \frac{1}{2} + \left(\frac{1}{2} + \frac{1}{2}\sqrt{3}\right)i, \\ u\omega^2 + v\omega &= u\left(-\frac{1}{2} + \frac{1}{2}\sqrt{3}i\right)^2 + v\left(-\frac{1}{2} + \frac{1}{2}\sqrt{3}i\right) \\ &= 1 - i. \end{aligned}$$

Teorema 4.12

Sea F un campo y $f(x) = x^4 + ax^3 + bx^2 + cx + d \in F[x]$. Entonces $f(x)$ es soluble por radicales.

Demostración. Sustituyendo x por $y - \frac{1}{4}a$ en $f(x)$, obtenemos

$$f\left(y - \frac{1}{4}a\right) = y^4 + py^2 + qy + r,$$

donde $p = b - \frac{3}{8}a^2$, $q = c - \frac{1}{2}ab + \frac{1}{8}a^3$ y $r = d - \frac{1}{4}ac - \frac{3}{256}a^4 + \frac{1}{16}a^2b$. A continuación, buscaremos $\beta, \gamma, \delta \in \mathbb{C}$ tales que

$$y^4 + py^2 + qy + r = (y^2 + \beta y + \gamma)(y^2 - \beta y + \delta).$$

Dado que

$$(y^2 + \beta y + \gamma)(y^2 - \beta y + \delta) = y^4 + (\gamma + \delta - \beta^2)y^2 + (\beta\delta - \beta\gamma)y + \gamma\delta,$$

entonces

$$\gamma + \delta - \beta^2 = p, \beta\delta - \beta\gamma = q \text{ y } \gamma\delta = r. \quad (4.4)$$

Utilizando estas relaciones, obtenemos que

$$\begin{aligned} \beta^6 + 2p\beta^4 + (p^2 - 4r)\beta^2 - q^2 &= \beta^6 + 2(\gamma + \delta - \beta^2)\beta^4 \\ &\quad + ((\gamma + \delta - \beta^2)^2 - 4\gamma\delta)\beta^2 - (\beta\delta - \beta\gamma)^2 = 0. \end{aligned}$$

Por lo tanto, β^2 es una raíz de la ecuación $z^3 + 2pz^2 + (p^2 - 4r)z - q^2 = 0$, que podemos calcular para obtener β . A partir de las relaciones (4.4), obtenemos γ y δ . Luego, calculamos las soluciones de las ecuaciones $y^2 + \beta y + \gamma = 0$ e $y^2 - \beta y + \delta = 0$. Finalmente, al sustituir estas soluciones en $x = y - \frac{1}{4}a$, obtenemos las soluciones de $f(x)$. \square

4.7.1 Grupos Solubles

Nota. • Sea G un grupo y H un subgrupo de G , entonces, se dice que H es un **subgrupo normal** de G si y sólo si

$$(\text{Para todo elemento } g \in G) (Hg = gH)$$

• Sea H un subgrupo normal de G y sea la operación (\times) definida en G/H de la siguiente manera $aH \times bH := abH$. Entonces, $(G/H; \times)$ es un grupo y se lo llama **Grupo cociente** o **grupo factor**.

Definición 4.9

Un grupo G es soluble si existe una cadena finita de subgrupos

$$G = N_0 \supset N_1 \supset \dots \supset N_k = \{e\}$$

tal que

1. N_i sea subgrupo normal de N_{i-1} .
2. N_{i-1}/N_i es abeliano.

Corolario 4.8

Todo grupo abeliano es soluble.

Demostración. Para demostrar que todo grupo abeliano es soluble, podemos utilizar la definición de grupo soluble y la propiedad de los grupos abelianos.

Un grupo G se dice soluble si existe una serie de subgrupos:

$$G = N_0 \supset N_1 \supset N_2 \supset \dots \supset N_k = \{e\}$$

donde cada subgrupo N_i es normal en N_{i-1} y el grupo cociente N_{i-1}/N_i es abeliano.

Ahora, consideremos un grupo abeliano G . Dado que G es abeliano, todos los subgrupos de G son normales. Por lo tanto, podemos construir una serie de subgrupos:

$$G = N_0 \supset N_1 \subset N_2 \supset \dots \supset N_k = \{e\}$$

donde cada subgrupo N_i es normal en N_{i-1} .

Veamos ahora si los grupos cociente N_{i-1}/N_i son abelianos. Tomemos dos elementos g_1N_i y g_2N_i en el grupo cociente N_{i-1}/N_i . La operación en el grupo cociente se define como $(g_1N_i)(g_2N_i) = (N_1N_2)N_i$.

Dado que G es abeliano, la operación de multiplicación en G es conmutativa.

Por lo tanto, para cualquier par de elementos g_1, g_2 en G , se tiene que $g_1g_2 = g_2g_1$. Esto implica que $(g_1g_2)N_i = (g_2g_1)N_i = (g_2N_i)(g_1N_i)$.

Por lo tanto, el grupo cociente N_{i+1}/N_i es abeliano para cualquier i .

En conclusión, hemos construido una serie de subgrupos donde cada subgrupo es normal en el siguiente y los grupos cociente son abelianos. Por lo tanto, todo grupo abeliano es soluble. \square

Ejemplo 4.17. Probaremos a continuación que el grupo simétrico de grado 3 es soluble.

Para demostrar que el grupo simétrico de grado 3, S_3 , es soluble, consideremos el subgrupo $N_1 = e, (1, 2, 3), (1, 3, 2)$.

N_1 es un subgrupo normal de S_3 ya que es cerrado bajo la operación de multiplicación y toma de inversos.

Ahora, consideremos los grupos cociente S_3/N_1 y N_1/e .

El grupo cociente S_3/N_1 tiene un orden de 2, ya que N_1 tiene 3 elementos y la identidad e se incluye en N_1 . Como cualquier grupo de orden 2 es abeliano, S_3/N_1 es abeliano.

El grupo cociente N_1/e tiene un orden de 3, ya que N_1 tiene 3 elementos y se excluye la identidad $\{e\}$. Como cualquier grupo de orden 3 es abeliano, N_1/e es abeliano.

Por lo tanto, se ha demostrado que el grupo simétrico de grado 3, S_3 , es soluble.

Nota. Dado el grupo G y los elementos a y b de G , entonces el conmutador de a y b es el elemento $a^{-1}b^{-1}ab$. El subgrupo conmutador, G' , de G es el subgrupo de G generador por todos los conmutadores de G .

El grupo G' es un subgrupo normal de G , además el grupo G/G' es abeliano, pues dados dos elementos, aG' bG' con $a, b \in G$, entonces

$$(aG')(bG') = abG' = ba(b^{-1}a^{-1}ab)G' = baG' = (bG')(aG').$$

Si consideramos un grupo conmutador de G' sería $G^{(2)} = (G')'$. Este es el

subgrupo de G generador por todos los elementos $(a')^{-1}(b')^{-1}a'b'$ donde $a', b' \in G'$. Continuando de esta forma definimos los subgrupos conmutadores más altos $G^{(m)} = (G^{(m-1)})'$.

Lema 4.6

El grupo G es soluble si y sólo si $G^{(k)} = \{e\}$ para algún entero k .

Demostración. Si G es un grupo soluble, existe una cadena

$$G = N_0 \supset N_1 \supset N_2 \supset \dots \supset N_k = \{e\}$$

donde cada N_i es normal en N_{i-1} , y donde N_{i-1}/N_i es abeliano. Pero entonces, el subgrupo conmutador N'_{i-1} de N_{i-1} debe estar contenido en N_i , es decir, $N'_{i-1} \subseteq N_i$, entonces para cada i se deduce lo siguiente,

$$N_i \supset N'_{i-1}.$$

Creando así, una cadena descendente de subgrupos conmutadores, pues, $N_1 \supset N'_0 = G'$, $N_2 \supset N'_1 \supset (G')' = G^{(2)}$, \dots , $N_i \supset G^{(i)}$, $\{e\} = N_k \supset G^{(k)}$. De donde resulta que $G^{(k)} = \{e\}$.

Recíprocamente, si $G^{(k)} = \{e\}$, sea $N_0 = G$, $N_1 = G'$, $N_2 = G''$, \dots , $N_k = G^{(k)} = \{e\}$. Tenemos $G = N_0 \supset N_1 \supset \dots \supset N_k = \{e\}$ con cada N_i normal en N_{i-1} . Finalmente,

$$\frac{N_{i-1}}{N_i} = \frac{G^{(i-1)}}{G^{(i)}} = \frac{G^{(i-1)}}{(G^{(i-1)})'}$$

luego es abeliano. Así pues, según la definición de grupo soluble obtenemos que G es un grupo soluble. □

Corolario 4.9

Si G es un grupo soluble y $\phi : G \rightarrow \bar{G}$ un homomorfismo, donde \bar{G} es una imagen homomórfica de G bajo ϕ , entonces \bar{G} es soluble.

Demostración. Dado que \bar{G} es una imagen homomórfica de G , es decir, $\bar{G} = \phi(G)$. G es un grupo soluble, entonces existe una cadena finita de subgrupos

$$G = N_0 \supset N_1 \supset N_2 \supset \dots \supset N_k = \{e\}$$

donde N_i es normal tal que $G = N_0$, $N_k = \{e\}$ y cada grupo cociente N_{i-1}/N_i es abeliano.

Para cada subgrupo N_i en G el homomorfismo ϕ induce un subgrupo $\phi(N_i)$ en \bar{G}

$$\bar{G} = \phi(N_0) \supset \phi(N_1) \supset \phi(N_2) \supset \dots \supset \phi(N_k) = \{e\}.$$

Como $G^{(k)} = \{e\}$ para alguna k , $(\bar{G}^{(k)}) = \{e\}$ para la misma k , esto por homomorfismo de grupos. De donde, de acuerdo con el lema previo, \bar{G} es soluble. \square

El siguiente lema es esencial en la prueba de que la familia de grupos S_n , con $n \geq 5$, no es soluble, para esto recordemos que **el orden de un ciclo** con k movimientos es igual a k . En general el orden de una permutación σ es el mínimo común múltiplo de las longitudes de los ciclos que componen a σ .

Lema 4.7

Sea $G = S_n$ donde $n \geq 5$, entonces $G^{(k)}$ para cada $k = 1, 2, \dots$, contiene todo ciclo de orden 3 de S_n , aquí S_n es simétrico de grado n .

Demostración. Observemos primero que para un grupo arbitrario G , si N es un subgrupo normal de G entonces N' también es un subgrupo normal de G .

Afirmamos que si N es un subgrupo normal de $G = S_n$ donde $n \geq 5$, que contiene todo ciclo de orden 3 en S_n , entonces N' debe también contener todo ciclo de orden 3. Supongamos los elementos $a = (1, 2, 3)$, $b = (1, 4, 5)$ de N ; entonces $a^{-1} = (3, 2, 1)$ y $b^{-1} = (5, 4, 1)$, por lo tanto

$$a^{-1}b^{-1}ab = (3, 2, 1)(5, 4, 1)(1, 2, 3)(1, 4, 5) = (1, 4, 2),$$

como conmutador de elementos de N debe estar en N' . Dado que N' es un subgrupo normal de G para cualquier $\pi(1) = i_1$, $\pi(4) = i_2$ y $\pi(2) = i_3$, donde i_1, i_2 e i_3 son cualesquiera tres enteros distintos en el rango de 1 a n , entonces $\pi^{-1}(1, 4, 2)\pi = (i_1, i_2, i_3)$ está en N' . Luego N contiene todos los ciclos de orden 3. Haciendo $N = G$, que es ciertamente normal en G y contiene todos los ciclos de orden tres, tenemos que G' contiene todos los ciclos de orden 3; como G' es

normal en G , G'' contiene todos los ciclos de orden 3; como G'' es normal en G , G''' contiene todos los ciclos de orden 3. Continuando de esta forma llegamos a la conclusión de que $G^{(k)}$ contiene todos los ciclos de orden 3 para cualquier k . \square

Teorema 4.13

S_n no es soluble para $n \geq 5$.

Demostración. Si $G = S_n$ según el lema previo $G^{(k)}$ contiene todos los ciclos de orden 3 de S_n para todo k . Por tanto, $G^{(k)} \neq \{e\}$ para toda k , de donde G no puede ser soluble esto por el lema 4.6. \square

4.7.2 Ecuación general de grado n

Definición 4.10

Si $n \geq 1$ y F es un campo y $K = F(a_0, \dots, a_{n-1})$ es un campo de fracciones algebraicas en las indeterminadas a_0, \dots, a_{n-1} , llamaremos polinomio general de grado n sobre K el polinomio

$$f(x) = x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0 \in F[x]$$

y $f(x) = 0$ ecuación de grado n .

Definición 4.11

Diremos que un polinomio en varias variables es simétrico si queda invariante bajo cualquier permutación de sus variables.

Definición 4.12

Llamaremos polinomios simétricos elementales de $F[x_1, \dots, x_n]$ a los polinomios

$$s_0(x_1, \dots, x_n) = 1 \text{ y } s_k(x_1, \dots, x_n) = \sum_{1 \leq i_1 < \dots < i_k \leq n} x_{i_1} x_{i_2} \dots x_{i_k} \text{ para } k = 1, \dots, n$$

Ejemplo 4.18. Para $n = 2$:

$$s_0(x_1, x_2) = 1$$

$$s_1(x_1, x_2) = x_1 + x_2$$

$$s_2(x_1, x_2) = x_1x_2$$

para $n = 3$

$$s_0(x_1, x_2, x_3) = 1$$

$$s_1(x_1, x_2, x_3) = x_1 + x_2 + x_3$$

$$s_2(x_1, x_2, x_3) = x_1x_2 + x_1x_3 + x_2x_3$$

$$s_3(x_1, x_2, x_3) = x_1x_2x_3$$

para $n = 4$:

$$s_0(x_1, x_2, x_3, x_4) = 1$$

$$s_1(x_1, x_2, x_3, x_4) = x_1 + x_2 + x_3 + x_4$$

$$s_2(x_1, x_2, x_3, x_4) = x_1x_2 + x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 + x_3x_4$$

$$s_3(x_1, x_2, x_3, x_4) = x_1x_2x_3 + x_1x_2x_4 + x_1x_3x_4 + x_2x_3x_4$$

$$s_4(x_1, x_2, x_3, x_4) = x_1x_2x_3x_4$$

Nota. Para los polinomios simétricos elementales $K[x_1, \dots, x_n]$ y $K[x_1, \dots, x_{n+1}]$

- $s_{n+1}(x_1, \dots, x_{n+1}) = x_{n+1}s_n(x_1, \dots, x_n)$
- $s_k(x_1, \dots, x_{n+1}) = s_k(x_1, \dots, x_n) + x_{n+1}s_{k-1}(x_1, \dots, x_n)$

Teorema 4.14

Sea K un campo y s_0, s_1, \dots, s_n los polinomios simétricos elementales en $K[x_1, \dots, x_n]$ entonces

$$(x - x_1) \dots (x - x_n) = \sum_{k=0}^n (-1)^{n-k} s_{n-k}(x_1, \dots, x_n) x^k$$

Demostración. Su demostración la puede encontrar en la siguiente referencia [?]

□

Nota (Fórmulas de Vieta). Sean $\alpha_1, \dots, \alpha_n$ y c_1, \dots, c_n números complejos tales que

$$(x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n) = x^n + c_1x^{n-1} + c_2x^{n-2} + \dots + c_n.$$

Entonces $c_k = (-1)^k \sigma_k(\alpha_1, \dots, \alpha_n)$ para $k = 1, \dots, n$. Donde σ_k son las sumas elementales simétricas

Teorema 4.15

Sea F un campo y $n \geq 1$. Entonces, el campo de las fracciones algebraicas simétricas de $F(x_1, \dots, x_n)$ es $F(s_1, \dots, s_n)$. Además, la extensión $F(x_1, \dots, x_n)/F(s_1, \dots, s_n)$ es finita de Galois, y su grupo de Galois es S_n .

Demostración. Sea $p(x) = (x - x_1) \cdots (x - x_n)$ entonces $p(x) = \sum_{k=0}^n (-1)^{n-k} s_{n-k}(x_1, \dots, x_n) x^k$, luego $p(x) \in F(s_1, \dots, s_n)[x]$ y dado que los elementos x_1, \dots, x_n son algebraicos sobre $F(s_1, \dots, s_n)$ y cada una de las raíces son simples (multiplicidad 1) de $p(x)$ por lo tanto, son separables por lo que $F(x_1, \dots, x_n)/F(s_1, \dots, s_n)$ es finita de Galois por lo que $\circ(G(F(x_1, \dots, x_n)/F(s_1, \dots, s_n))) \leq n!$.

Por otro lado si $\sigma \in S_n$ tenemos que la siguiente aplicación $\bar{\sigma} : F(x_1, \dots, x_n) \rightarrow F(x_1, \dots, x_n)$ definida por $\bar{\sigma}(p(x_1, \dots, x_n)) = p(x_{\sigma(1)}, \dots, x_{\sigma(n)})$ es un homomorfismo de campos. Consideramos a continuación $r : S_n \rightarrow \text{Automorfismos de } F(x_1, \dots, x_n)$ definido como $r(\sigma) = \bar{\sigma}$. Notar que r es un homomorfismo inyectivo y dado que S_n deja fijos los elementos de $F(s_1, \dots, s_n)$ tenemos un monomorfismo de S_n en $F(x_1, \dots, x_n)/F(s_1, \dots, s_n)$ por lo que $n! = \circ(S_n) \geq \circ(G(F(x_1, \dots, x_n)/F(s_1, \dots, s_n)))$, pero dado que

$$\circ(G(F(x_1, \dots, x_n)/F(s_1, \dots, s_n))) \geq n!$$

tenemos que $S_n = \circ(G(F(x_1, \dots, x_n)/F(s_1, \dots, s_n)))$, por lo tanto

$$S_n \cong G(F(x_1, \dots, x_n)/F(s_1, \dots, s_n))$$

□

Teorema 4.16

Sea F un campo característica cero. Entonces el grupo de Galois de polinomio general de grado n sobre F es isomorfo a S_n .

Demostración. Sean a_0, \dots, a_{n-1} los coeficientes de $f_n(x)$ y sean $\alpha_1, \dots, \alpha_n$ las raíces de $f_n(x)$ en una extensión de $F(a_0, \dots, a_{n-1})$ luego tenemos que el campo de descomposición de $f_n(x)$ sobre $F(a_0, \dots, a_{n-1})$ es $F(a_0, \dots, a_{n-1}, \alpha_1, \dots, \alpha_n)$ y así tenemos que $f_n(x) = (x - \alpha_1) \dots (x - \alpha_n)$ por lo que $a_k = (-1)^{n-k} s_{n-k}(\alpha_1, \dots, \alpha_n)$ para $k = 0, \dots, n - 1$. Consideremos el siguiente homomorfismo de anillos $\phi : F[a_0, \dots, a_{n-1}] \rightarrow F[(-1)^n s_n, \dots, -s_1]$ definido de la siguiente manera $\phi(h(a_0, \dots, a_{n-1})) = h((-1)^n s_n, \dots, -s_1)$. Ahora veamos que este homomorfismo es inyectivo si

$$\begin{aligned} \phi(h(a_0, \dots, a_{n-1})) &= \phi(g(a_0, \dots, a_{n-1})) \\ h((-1)^n s_n, \dots, -s_1) &= g((-1)^n s_n, \dots, -s_1), \end{aligned}$$

expandimos las funciones y usamos las raíces de $p(x)$. Por lo tanto

$$\begin{aligned} h((-1)^n s_n(\alpha_1, \dots, \alpha_n), \dots, -s_1(\alpha_1, \dots, \alpha_n)) &= g((-1)^n s_n(\alpha_1, \dots, \alpha_n), \dots, -s_1(\alpha_1, \dots, \alpha_n)) \\ h(a_0, \dots, a_{n-1}) &= g(a_0, \dots, a_{n-1}) \end{aligned}$$

para que sea sobreyectiva debemos probar que para cada elemento $b \in B$ existe a tal que $\phi(a) = b$, donde $\phi : A \rightarrow B$.

Dado un polinomio h en $F[(-1)^n s_n, \dots, -s_1]$ que podemos expresar

$$h = h((-1)^n s_n, \dots, -s_1)$$

existe un elemento $g \in F[a_0, \dots, a_{n-1}]$, tenemos

$$h = h((-1)^n s_n, \dots, -s_1)$$

expandimos las funciones a las raíces algebraicas $\alpha_1, \dots, \alpha_n$, entonces

$$\begin{aligned} h((-1)^n s_n(\alpha_1, \dots, \alpha_n), \dots, -s_1(\alpha_1, \dots, \alpha_n)) \\ = h(a_0, \dots, a_{n-1}), \in F[a_0, \dots, a_{n-1}] \end{aligned}$$

por lo que hemos demostrado es sobreyectiva. Así, ϕ es un isomorfismo de anillos, lo que se puede extender a un isomorfismo ϕ' de $F(a_0, \dots, a_{n-1})$

en $F((-1)^n s_n, \dots, -s_1)$ y este a otro isomorfismo ϕ'' de $F(a_0, \dots, a_{n-1})[x]$ en $F((-1)^n s_n, \dots, -s_1)[x]$, así

$$\phi''(f_n(x)) = x^n - s_1 x^{n-1} + \dots + (-1)^n s_n = (x - x_1) \dots (x - x_n).$$

Por último como $F(a_0, \dots, a_{n-1}, \alpha_1, \dots, \alpha_n)$ es el campo de descomposición de $f_n(x)$ sobre $F(a_0, \dots, a_{n-1})$ y $F(x_1, \dots, x_n)$ es el campo de descomposición de la imagen isomorfa de $f_n(x)$ sobre $F(s_1, \dots, s_n)$ tenemos que

$$F(a_0, \dots, a_{n-1}, \alpha_1, \dots, \alpha_n) / F(a_0, \dots, a_{n-1}) \cong F(x_1, \dots, x_n) / F(s_1, \dots, s_n)$$

y así también sus respectivos grupos de Galois, por el teorema previo sabemos que

$$G(F(x_1, \dots, x_n) / F(s_1, \dots, s_n)) \cong S_n$$

entonces, el grupo de galois de f_n es S_n , es decir,

$$G(F(a_0, \dots, a_{n-1}, \alpha_1, \dots, \alpha_n) / F(a_0, \dots, a_{n-1})) \cong S_n.$$

□

4.7.3 Extensiones radicales

Definición 4.13

Una extensión K de un campo F se dice que es una extensión radical de F , si existe una cadena de subcampos

$$F = F_0 \subset F_1 \subset \dots \subset F_r = E$$

tal que $i = 1, 2, \dots, r$, tenemos $F_i = F_{i-1}(\alpha_i)$ y $\alpha_i^{n_i} \in F_{i-1}$.

Ejemplo 4.19. Queremos demostrar que $Q(\sqrt{1 + \sqrt{2}})$ es una extensión radical de Q . Comencemos observando que $(\sqrt{1 + \sqrt{2}})^2 = 1 + \sqrt{2} \in Q(\sqrt{1 + \sqrt{2}})$, lo cual significa que $\sqrt{2}$ está en $Q(\sqrt{1 + \sqrt{2}})$. Por lo tanto, $Q(\sqrt{1 + \sqrt{2}}) = Q(\sqrt{2}, \sqrt{1 + \sqrt{2}})$.

Ahora, para demostrar que $Q(\sqrt{2}, \sqrt{1 + \sqrt{2}})$ es una extensión radical de Q , necesitamos mostrar que ambos $\sqrt{2}$ y $(\sqrt{1 + \sqrt{2}})^2$ están en $Q(\sqrt{2}, \sqrt{1 + \sqrt{2}})$.

1. $\sqrt{2} \in Q(\sqrt{2}, \sqrt{1+\sqrt{2}})$: Esto es evidente ya que estamos incluyendo $\sqrt{2}$ en la extensión.

2. $(\sqrt{1+\sqrt{2}})^2 \in Q(\sqrt{2}, \sqrt{1+\sqrt{2}})$:

$$(\sqrt{1+\sqrt{2}})^2 = 1 + \sqrt{2}$$

Ya que $1 + \sqrt{2}$ ya está en $Q(\sqrt{2}, \sqrt{1+\sqrt{2}})$, esto demuestra que $(\sqrt{1+\sqrt{2}})^2$ también está en la extensión.

Al incluir tanto $\sqrt{2}$ como $(\sqrt{1+\sqrt{2}})^2$ en $Q(\sqrt{2}, \sqrt{1+\sqrt{2}})$, podemos concluir que $Q(\sqrt{1+\sqrt{2}})$ es una extensión radical de Q .

Definición 4.14

Si $f(x) \in F[x]$, entonces es soluble por radicales si existe una extensión radical L de F tal que f se descompone sobre L .

Lema 4.8

Supongamos que el campo F tenga todas las raíces n -ésimas de la unidad y supongamos que $a \neq 0$ está en F . Sea $x^n - a \in F[x]$ y sea K su campo de descomposición sobre F . Entonces

1. $K = F(u)$ donde u es cualquier raíz de $x^n - a$.
2. El grupo de galois de $x^n - a$ sobre F es abeliano.

Demostración. Dado que F contiene todas las raíces n -ésimas de la unidad, es decir, contiene a $\omega = e^{\frac{2\pi i}{n}}$; notese que $\omega^n = 1$ pero $\omega^m \neq 1$ para $0 < m < n$. Si $u \in K$ es cualquier raíz de $x^n - a$, entonces $u, u\omega^2, \dots, u\omega^{n-1}$ son todas las raíces de $x^n - a$. Que sean raíces es evidente, ahora probaremos que dichas raíces sean distintas, para esto tenemos que $\omega^p u = \omega^q u$ con $0 \leq p < q < n$, entonces debido a que $u \neq 0$ y $(\omega^p - \omega^q)u = 0$, debemos tener que $\omega^p = \omega^q$ lo que es imposible ya que $\omega^{q-p} = 1$ con $1 \leq p < q < n$ esto por la observación 4.6. Luego dado que $\omega \in F$, todos los $u, u\omega^2, \dots, u\omega^{n-1}$ esten en $F(u)$, así $F(u)$ descompone a $x^n - a$. Además $F(u)$ es el campo más pequeño que contiene a F y a u y al contener a ω también

debe contener a $u\omega^i$. Por lo tanto, el campo $F(u)$ es el campo de descomposición de $x^n - a$ y así $K = F(u)$.

Si τ, σ son dos elementos cualquiera de $x^n - a$, es decir, si τ, σ son automorfismos de $K = F(u)$ que dejan todos los elementos de F fijos, entonces como tanto $\sigma(u)$ y $\tau(u)$ son raíces de $x^n - a$, $\sigma(u) = \omega^i u$ y $\tau(u) = \omega^j u$. Si F contiene a las raíces de unidad, entonces

$$\begin{aligned}\tau\sigma(u) &= \tau(\omega^i u) = \omega^i \tau(u) = \omega^i \omega^j u = \omega^{i+j} u \\ \sigma\tau(u) &= \sigma(\omega^j u) = \omega^j \sigma(u) = \omega^j \omega^i u = \omega^{j+i} u.\end{aligned}$$

Por lo tanto, $\sigma\tau$ y $\tau\sigma$ coinciden sobre u y sobre F , de donde, en todo $K = F(u)$. Así $\sigma\tau = \tau\sigma$ entonces el grupo de Galois es abeliano, es decir, $G(K/F)$ es abeliano, en particular es soluble esto por el Corolario 4.8. \square

Teorema 4.17

Si $p(x) \in F[x]$ es soluble por radicales sobre F , entonces el grupo de Galois sobre F de $p(x)$ es un grupo soluble.

Demostración. Consideramos K como el campo de descomposición de $p(x)$ sobre F , el grupo de Galois de $p(x)$ sobre F es $G(K/F)$.

Dado que $p(x)$ es soluble por radicales, entonces existe una extensión radical, es decir,

$$F \subset F_1 = F(\alpha_1) \subset F_2 = F_1(\alpha_2) \subset \dots \subset F_k = F_{k-1}(\alpha_k),$$

donde $\alpha_1^{r_1} \in F(\alpha_1)$, $\alpha_k^{r_k} \in F_{k-1}$ y donde $K \subset F_k$. Sin pérdida de generalidad podemos suponer que F_k es una extensión normal de F , esto dado que F_k es una extensión finita de F tal que F es el campo fijo de $G(K/F)$.

Como extensión normal de F , F_k es también una extensión normal de cualquier campo intermedio, de donde F_k es una extensión normal de cada una de las F_i .

Luego por el lema previo todo F_i es una extensión normal de F_{i-1} y debido a que F_k es una extensión normal de F_{i-1} de acuerdo con el Teorema Fundamental de la Teoría de Galois $G(F_k/F_i)$ es un subgrupo normal en $G(F_k/F_{i-1})$.

Continuando con la demostración consideramos la cadena

$$G(F_k/F) \subset G(F_k/F_1) \subset \dots \subset G(F_k/F_{k-1}) \subset \{e\};$$

entonces cada grupo es un subgrupo normal en el que le precede.

Como F_i es una extensión normal de F_{i-1} de acuerdo con el Teorema Fundamental de la Teoría de Galois 4.7, el grupo de Galois de F_i es isomorfo a

$$G(F_k/F_{i-1})/G(F_k/F_i),$$

pero según el lema previo $G(F_i/F_{i-1})$ es un grupo abeliano. Así, todos los grupos cocientes $G(F_k/F_{i-1})/G(F_k/F_i)$ de la cadena es abeliano. Por lo tanto, el grupo $G(F_k/F)$ es soluble.

Finalmente, dado que $K \subset F_k$ es una extensión normal de F (por ser un campo de descomposición) según el Teorema Fundamental de la Teoría de Galois $G(F_k/K)$ es un subgrupo normal de $G(F_k/F)$ y $G(K/F)$ es isomorfo a

$$G(F_k/F)/G(F_k/K).$$

Así pues, $G(K/F)$ es una imagen homomórfica de $G(F_k/F)$ que es un grupo soluble. Por lo tanto el grupo de Galois $G(K/F)$ de $p(x)$ sobre F es soluble.

El recíproco de este teorema se puede encontrar en la referencia proporcionada [?]. □

Recordemos que un polinomio general de grado n sobre F se entiende como $p(x) = x^n + a_1x^{n-1} + \dots + a_n$ y cerrado con el teorema clásico de Abel.

Teorema 4.18

El polinomio general de grado $n \geq 5$ no es soluble por radicales.

Demostración. En el Teorema ?? demostramos que el Grupo de Galois de un polinomio general de grado n es isomorfo a S_n .

Luego por el Teorema ?? S_n no es un grupo soluble para $n \geq 5$ y finalmente por el Teorema ?? $p(x)$ no es soluble por radicales. □

Conclusiones

- A partir del análisis de la teoría de Galois, mediante la revisión de material bibliográfico especializado, se logró generar una monografía sobre la insolubilidad de ecuaciones algebraicas de grado mayor o igual a cinco por medio de radicales.
- La examinación de los documentos especializados sobre la teoría de Galois, permitió la comprensión de dicha teoría.
- El estudio de la Teoría de Galois aplicada a la insolubilidad de ecuaciones algebraicas de grado mayor o igual a cinco por medio de radicales, ofrece a los estudiantes explorar y comprender un tema específico que no se ve en los cursos regulares de pregrado.
- La monografía, resultado de este trabajo servirá como fuente de conocimiento valioso para los estudiantes, sobre lo que es la teoría de Galois aplicada a la insolubilidad de ecuaciones algebraicas de grado mayor o igual a cinco por medio de radicales.

Bibliografía

- [1] **AXLER, S; GEHRING, F; RIBET, K.** *Abstract Algebra*. 3ª ed. [en línea]. New York-USA: Editorial Board, 2002. [Consulta: 18 de Octubre 2023]. Disponible en:
<https://math24.files.wordpress.com/2013/02/algebra-serge-lang.pdf>
- [2] **JUDSON, T; BEEZER, R.** *Algebra Abstracta*. [en línea]. Texas-USA: Stephen F. Austin State University. [Consulta: 15 de Noviembre 2023]. Disponible en:
https://www.academia.edu/40352218/Algebra_Abtracta_Teor%C3%ADa_y_Aplicaciones
- [3] **GALLIAN, J.** *Contemporary Abstract Algebra* [en línea]. 9ª ed. Minnesota-USA: Cengage Learning, 2017. [Consulta: 17 de abril 2023]. Disponible en:
<https://books.google.com.ec/books?id=JMUaCgAAQBAJ&printsec=frontcover&dq=Contemporana#v=onepage&q&f=false>
- [4] **LABRA, A; SUAZO, A.** *Elementos de la teoría de cuerpos* [en línea]. Chile: Jc Sáez Editor, 2011. [Consulta: 15 de marzo 2023]. Disponible en:
<https://cmmedu.uchile.cl/repositorio/Instructional%20design%20of%20materiales%20or%20pedagogical%20models%29./Herramientas%20para%20la%20formaci%C3%B3n%20de%20profesores%20de%20matem%C3%A1tica/12%20-%20Elementos%20de%20Teor%C3%ADa%20de%20Cuerpos.pdf>
- [5] **LANG, S.** *Graduate texts in Mathematics*. 3ª ed. USA: Editorial Board (North America), 2002. [Consulta: 06 de enero del 2024]. Disponible en:
<https://math24.files.wordpress.com/2013/02/algebra-serge-lang.pdf>
- [6] **ROTMAN, J.** *GALOIS THEORY* 2ª ed. [en línea]. California-USA: Editorial

Bibliografía

- Board (North America), 1998. [Consulta: 10 de abril 2023]. Disponible en:
http://www.ismailnacicangul.com/dosyalar/rotman-galois_theory.pdf
- [7] **STEWART, I.** *GALOIS THEORY*. 3ª ed. [en línea]. Reino Unido: Chapman & Hall/CRCR mathematics, 1945. [Consulta: 10 de abril 2023]. Disponible en:
https://math.illinoisstate.edu/schebol/teaching/407-14-files/Stewart-galois_theory.pdf
- [8] **RIQUELME, E** *Teoría de Galois y ecuaciones algebraicas*. [en línea]. Chile: Univerdiad del BÍO BÍO. [Consulta: 05 de Febrero 2024]. Disponible en:
http://repobib.ubiobio.cl/jspui/bitstream/123456789/1996/3/Riquelme_Faundez_Edgaro.pdf