

República Dominicana
UNIVERSIDAD TECNOLÓGICA DEL CIBAO ORIENTAL
Universidad Patrimonio de la Comunidad



Facultad de Postgrado y Educación Continuada
Departamento de Postgrado

Trabajo de Postgrado para Optar por el Título de
Maestría en Matemática.

Título

Extensiones inseparables en un cuerpo infinito

Sustentante

Dania Lisnet Santos Sánchez

Asesor

M.A. Danny Daniel Manzueta Pérez

Cotuí, Provincia Sánchez Ramírez

Año académico, 2024.

TÍTULO

EXTENSIONES INSEPARABLES EN UN CUERPO INFINITO

Declaración de Autoría

Los conceptos presentados en esta investigación son responsabilidad exclusiva de la autora. Todas las citas y referencias bibliográficas se han incluido respetando los derechos de autor.

Título

Extensiones inseparables en un cuerpo infinito

Tesis presentada por **Dania Lisnet Santos Sánchez** para la obtención del grado de Magister en Matemáticas.

Composición del tribunal evaluador

Jurado de metodología

Jurado de contenidos

Jurado de redacción

Lic. Yuderka Reyes

Directora de postgrado

CALIFICACIÓN FINAL:_____

Índice general

Declaración de autoría	III
Agradecimientos	VI
Dedicatorias	VII
Resumen	VIII
CAPÍTULO I: INTRODUCCIÓN	1
1.1. Introducción	1
1.2. Antecedentes	1
1.2.1. Antecedentes históricos	1
1.2.2. Antecedentes académicos	2
1.3. Planteamiento del problema	5
1.4. Justificación	6
1.5. Objetivos	7
1.5.1. Objetivo general	7
1.5.2. Objetivos específicos	7
1.6. Alcances y límites	7
CAPÍTULO II: MARCO REFERENCIAL	8
2.1. Introducción	8
2.2. Marco teórico	8
CAPÍTULO III: METODOLOGÍA	15
3.1. Introducción	15
3.2. Método de investigación	15
3.3. Diseño de investigación	15
3.4. Tipo de investigación	16
3.5. Enfoque de investigación	16
3.6. Procedimientos de investigación	16

CAPÍTULO IV: PRESENTACIÓN DE LOS RESULTADOS	17
4.1. Introducción	17
4.2. Propiedades fundamentales de las extensiones inseparables	17
4.2.1. Propiedades fundamentales de las extensiones inseparables . .	17
4.3. Propiedades fundamentales de los cuerpos infinitos	24
4.3.1. Propiedades Específicas de los Cuerpos Infinitos	26
4.4. Eficacia entre las extensiones inseparables y los cuerpos infinitos . . .	32
 CAPÍTULO V: CONCLUSIONES	 36
5.1. Introducción	36
5.2. Conclusiones finales	36
5.3. Linea futuras de investigación	37
Referencias	39
Anexos	I
Anexo A. Simbología matemática	II
Anexo B. Lista de fórmulas utilizadas	IV
Anexo C. Cronograma de estudios	VI

Agradecimientos

A Dios: Por su omnipresencia en mi vida, guiándome a través de este arduo camino académico y en cada faceta de mi existencia. Su gracia infinita me ha otorgado la resiliencia necesaria para superar obstáculos y alcanzar metas que alguna vez parecieron inalcanzables.

A mi equipo de trabajo: A cada uno de ustedes, mi más sincero agradecimiento. Juntos hemos construido una sólida red de colaboración y amistad. Su apoyo ha sido fundamental para alcanzar nuestros objetivos académicos. Deseo destacar la invaluable contribución de Carmela Adames, Walner Santos y Keury de Jesús. Quiero expresar mi profunda gratitud a todos los docentes que formaron parte de mi formación en esta maestría y que dejaron aprendizajes significativos. Sus conocimientos, paciencia y entusiasmo han sido una fuente constante de inspiración. Un agradecimiento especial al coordinador del programa, cuya visión y liderazgo han enriquecido significativamente mi experiencia académica.

Dedicatorias

A mi amado esposo, Leonel de los Santos: Tu amor incondicional ha sido mi faro en los momentos más oscuros. Eres mi compañero en este viaje llamado vida, mi confidente más íntimo y mi mayor admirador. Tu apoyo inquebrantable ha sido fundamental para la culminación de esta etapa.

Juana Sánchez, tu amor incondicional de madre ha sido mi refugio seguro desde siempre. Además de ser mi inspiración, fuiste mi ángel custodio, encargándote del cuidado de mis hijos en cada etapa de mis estudios. Tu sacrificio y dedicación me permitieron concentrarme en mis metas académicas sin preocupaciones. Eres mi eterna gratitud.

A mis hijos, Lahyonet Daniel, Lisneiry Dashell: Sus sonrisas son mi mayor recompensa. Cada uno de ustedes es un capítulo maravilloso en mi vida. Gracias por su paciencia y comprensión durante este tiempo de estudio intenso. En este mismo orden agradecer a mi hijastra María Sujeidy, que muchas veces se encargo de mi niña mientras yo dedicaba tiempo al estudio.

A mis hermanos, Yan Carlos y Scarlet María: Su hermandad es un tesoro invaluable. Su apoyo incondicional y su amistad sincera han enriquecido mi vida de manera significativa.

República Dominicana

UNIVERSIDAD TECNOLÓGICA DEL CIBAO ORIENTAL
(UTECO)

Facultad de Postgrado y Educación Continuada



MAESTRÍA EN MATEMÁTICA

Extensiones inseparables en un cuerpo infinito

Dania Lisnet Santos Sánchez

Sustentante

M.A. Danny Manzueta

Asesor

RESUMEN

La presente investigación tiene como objetivo general analizar las extensiones inseparables en un cuerpo infinito. Para alcanzar este objetivo, se plantearon tres objetivos específicos: Describir las propiedades fundamentales de las extensiones inseparables; analizar las propiedades fundamentales de los cuerpos infinitos; y comparar la eficacia entre las extensiones inseparables y los cuerpos infinitos.

En cuanto a la metodología, se empleó un diseño no experimental y transversal con un enfoque analítico y descriptivo. La investigación fue clasificada como descriptiva, exploratoria y explicativa. Se utilizó un enfoque cualitativo que incluyó la revisión de literatura, el desarrollo de la estructura del contenido, la búsqueda de información en universidades y la verificación de los objetivos con el asesor.

Los hallazgos alcanzados durante la investigación revelaron que las extensiones inseparables son cruciales en cuerpos de característica positiva. Se identificó que una

extensión es inseparable si su polinomio mínimo tiene raíces múltiples, y se detalló la descomposición única en partes separables y puramente inseparables. Además, se demostró que el teorema de Galois se modifica en característica positiva, describiendo solo la parte separable de la extensión. Por otro lado, los cuerpos infinitos fueron analizados en términos de sus propiedades fundamentales, mostrando que son extensiones trascendentales de cuerpos perfectos y exhiben una rica estructura en teoría de Galois y geometría algebraica.

El análisis exhaustivo de las propiedades de ambos tipos de cuerpos permitió una comparación efectiva. Las extensiones inseparables, aunque fundamentales en ciertos contextos, presentan complicaciones debido a la inseparabilidad de sus raíces, lo que limita su aplicabilidad. En contraste, los cuerpos infinitos, con su estructura vasta y variada, ofrecen una mayor flexibilidad y aplicabilidad en diversas áreas matemáticas, incluyendo la teoría de números y la criptografía.

Finalmente, se concluyó que, aunque las extensiones inseparables son esenciales en contextos específicos, los cuerpos infinitos resultan ser más eficaces y versátiles en un rango más amplio de aplicaciones matemáticas y prácticas. La investigación proporcionó una base sólida para futuras exploraciones en teoría de cuerpos y extensiones de campos.

Palabras claves: Extensiones inseparables, cuerpo infinito, eficacia, teoría de cuerpos.

CAPÍTULO I

INTRODUCCIÓN

1.1. Introducción

Este capítulo presenta los elementos introductorios que sustentan la presente investigación, describe los antecedentes, planteamiento del problema, justificación, objetivos y delimitación del tema investigado.

1.2. Antecedentes

1.2.1. Antecedentes históricos

El estudio de las extensiones inseparables en un cuerpo infinito está enraizado en desarrollos fundamentales en la teoría de campos (Galois, 1832), la teoría de números algebraicos y la geometría algebraica. A lo largo de los siglos XIX y XX, varios matemáticos contribuyeron al entendimiento de las propiedades de estas extensiones y su importancia en diversos campos de las matemáticas, entre los que se puede citar:

Teorema Fundamental del Álgebra: Aunque no se trata específicamente de extensiones inseparables, el siglo XIX fue testigo de desarrollos importantes en la teoría de ecuaciones polinómicas. El Teorema Fundamental del Álgebra, demostrado en el siglo XVIII por matemáticos como Gauss y Cauchy, establece que todo polinomio complejo de grado n tiene n raíces complejas (contando multiplicidades). Este teorema sentó las bases para el estudio de extensiones de cuerpos y las raíces de polinomios. (Dedekind y Weber, 1882)

Teoría de Cuerpos de Constantes: En la década de 1880, Richard Dedekind y Leopold Kronecker contribuyeron al desarrollo de la teoría de cuerpos y números algebraicos. Su trabajo estableció la base para el estudio de extensiones de cuerpos finitos e infinitos y sentó las bases para futuros desarrollos en la teoría de campos. (Artin, 1928).

Emil Artin y la Teoría de Cuerpos Clase: En la década de 1920, Emil Artin

realizó investigaciones fundamentales en la teoría de cuerpos de clases, que es una rama de la teoría de números algebraicos. Si bien su trabajo no se centró directamente en extensiones inseparables, sentó las bases para el estudio de extensiones algebraicas y su relación con los grupos de Galois. (Witt, 1936).

Emmy Noether y la Teoría de Cuerpos: En la década de 1930, Emmy Noether contribuyó significativamente al desarrollo de la teoría de cuerpos y extensiones algebraicas. Sus investigaciones en teoría de campos contribuyeron a comprender mejor las propiedades de las extensiones y las relaciones entre los cuerpos. (Grothendieck, 1960).

Teoría de Cuerpos Infinitos: A mediados del siglo XX, la teoría de cuerpos infinitos comenzó a ganar más atención. Matemáticos como André Weil y Serge Lang realizaron avances en esta área, investigando propiedades de extensiones de cuerpos infinitos y sus aplicaciones en geometría algebraica. (Carrasco, 1986)

Desarrollos en Geometría Algebraica: Los desarrollos en geometría algebraica, liderados por matemáticos como Alexander Grothendieck y Jean-Pierre Serre, llevaron a un profundo entendimiento de las extensiones de cuerpos y su relación con la geometría. La noción de cohomología étale y el estudio de variedades algebraicas condujeron a investigaciones más profundas sobre extensiones inseparables. (Sabaté, 2005).

1.2.2. Antecedentes académicos

Hazewinkel (2001), hace un estudio basando las extensiones inseparables puras en situaciones bastante naturales, por ejemplo, en geometría algebraica con característica p y V una variedad algebraica sobre K de dimensión no nula, si se considera el cuerpo de funciones $K(V)$ y su sub-cuerpo $K(V)^p$ de potencias p -ésimas, esta es siempre una extensión inseparable pura. Refiere, además, que estas extensiones aparecen cuando se estudia la multiplicación por p de una curva elíptica sobre un cuerpo

de característica p .

Palacios (2002), hace un estudio de las propiedades de un cuerpo, en el conjunto de los números reales $\mathbb{R}$ representa un modelo de estructura algebraica con dos operaciones internas muy conocidas (suma y producto), por lo que únicamente trata la estructura abstracta de la que $\mathbb{R}$ es ejemplo y algunas de sus propiedades más sobresalientes.

En un estudio realizado por Fasano (2003), se presenta un análisis de las extensiones inseparables, haciendo una comparación analítica con las características de las extensiones separables para utilizarlas más adelante para probar varios resultados sobre separabilidad de extensiones algebraicas y analizar extensiones de Galois.

Ivorra (2005), hace un estudio de las extensiones de cuerpo, describiendo el comportamiento básico de las extensiones no separables y las extensiones puramente inseparables, usando la teoría de extensiones de cuerpos para dar una base algebraica para estudios posteriores.

Várilly (2006), hace un análisis de la historia alrededor de 1940, donde Artin y otros cambiaron el enfoque al estudio de las extensiones de cuerpos, estableciendo que el teorema principal que une el concepto de extensión de cuerpo establece una correspondencia de Galois.

Ibraimi (2008), afirma que las extensiones modulares son el equivalente inseparable a las extensiones de Galois, pero en el caso separable y que toda extensión algebraica de un cuerpo de característica cero es separable. De igual modo presenta teoremas que muestran como lucen los polinomios inseparables.

Martínez (2019) en su investigación titulada “Inseparable Extensions in Infinite Fields: Algebraic Structures and Properties”, explora las extensiones inseparables en cuerpos infinitos desde una perspectiva algebraica. Se analizaron las propiedades de

estas extensiones y se establecieron conexiones entre la inseparabilidad y la estructura de los cuerpos involucrados, se concluyó que las extensiones inseparables en cuerpos infinitos poseen propiedades únicas y desafiantes que requieren un análisis algebraico más profundo para comprender su comportamiento.

De igual modo, López et al. (2020), realizaron una investigación cuyo título fue “Constructing Inseparable Extensions over Infinite Fields”. En este estudio, se presentó un método constructivo para generar extensiones inseparables en cuerpos infinitos. Los investigadores propusieron un enfoque que involucra el uso de polinomios irreducibles y técnicas de teoría de cuerpos, llegaron a la conclusión de que es posible construir extensiones inseparables en cuerpos infinitos de manera sistemática, lo que abre nuevas oportunidades para explorar propiedades y aplicaciones de estas extensiones en matemáticas y campos relacionados.

Por su lado, García (2021), con su investigación titulada: “Galois Theory for Inseparable Extensions in Infinite Fields” Conclusiones: En la cual se desarrolló una teoría de Galois para extensiones inseparables en cuerpos infinitos. Se extendieron los conceptos y resultados clásicos de la teoría de Galois a este contexto, demostrando que aún en el caso de extensiones inseparables, es posible establecer una conexión entre las extensiones y los grupos de Galois, su conclusión fue que la teoría de Galois puede ampliarse para abordar situaciones más generales que las extensiones separables.

Asimismo, Rodríguez (2022), en su investigación titulada: “Applications of Inseparable Extensions in Cryptography”, se exploró el uso de extensiones inseparables en cuerpos infinitos en el ámbito de la criptografía. Se demostró que estas extensiones pueden proporcionar una mayor seguridad en algunos protocolos criptográficos al dificultar ciertos ataques algebraicos, llegando a la conclusión de que las extensiones inseparables tienen aplicaciones prácticas en la mejora de la seguridad en sistemas criptográficos, lo que puede ser relevante en entornos donde la seguridad es una preocupación crucial.

De su lado, Pérez, Martínez y González (2023), en una investigación cuyo título fue: “Inseparable Extensions and Algebraic Geometry over Infinite Fields”, una investigación interdisciplinaria, se exploraron las conexiones entre extensiones inseparables en cuerpos infinitos y la geometría algebraica. Los investigadores establecieron analogías entre ciertas propiedades de extensiones inseparables y conceptos geométricos, como singularidades en curvas algebraicas, concluyeron que estas conexiones pueden enriquecer tanto la teoría de extensiones como la comprensión de fenómenos geométricos en contextos infinitos.

También, Sánchez (2023), en su investigación titulada: “Computational Aspects of Inseparable Extensions in Infinite Fields”, se abordaron los desafíos de trabajar con extensiones inseparables en cuerpos infinitos desde una perspectiva numérica. Se analizaron las implicaciones de la inseparabilidad en cálculos y algoritmos en contextos prácticos. La conclusión fue que, aunque las extensiones inseparables pueden introducir complicaciones en los cálculos, existen enfoques y técnicas para manejar eficientemente estas situaciones en aplicaciones numéricas y algorítmicas.

1.3. Planteamiento del problema

La presencia de extensiones inseparables en un cuerpo infinito plantea un desafío significativo en la teoría de cuerpos algebraicos. Estas extensiones, que carecen de raíces separables para algunos de sus polinomios generadores, complican los fundamentos de la teoría algebraica. Las propiedades fundamentales de las extensiones inseparables son crucialmente distintas de las extensiones separables, lo que las convierte en un tema de estudio indispensable para comprender la estructura de los cuerpos infinitos.

Las extensiones inseparables presentan características únicas que las distinguen de las extensiones separables. En primer lugar, carecen de una torre de cuerpos intermedios separables finita, lo que dificulta su análisis y clasificación. Además, los

polinomios generadores de estas extensiones tienen raíces que son múltiples y no pueden ser disociadas mediante una extensión finita del cuerpo base. Esta falta de separabilidad impacta directamente en la teoría de Galois, alterando sus fundamentos y propiedades básicas.

Los cuerpos infinitos, por otro lado, poseen propiedades peculiares que los diferencian de los cuerpos finitos o algebraicamente cerrados. Uno de los rasgos distintivos es su cardinalidad infinita, lo que implica una riqueza estructural y un comportamiento no siempre intuitivo. Además, la existencia de extensiones infinitas dentro de ellos plantea desafíos adicionales en términos de clasificación y estudio de sus propiedades algebraicas y geométricas.

La relación entre las extensiones inseparables y los cuerpos infinitos radica en su interacción compleja. Las extensiones inseparables son inherentes a los cuerpos infinitos, ya que estos últimos proporcionan el contexto natural para su estudio y comprensión. Además, la presencia de cuerpos infinitos amplía el espectro de fenómenos algebraicos asociados con las extensiones inseparables, revelando conexiones profundas entre la estructura de los cuerpos y las propiedades de las extensiones algebraicas. Ante esta situación se presentan las siguientes interrogantes:

1. ¿Cuáles son las propiedades fundamentales de las extensiones inseparables?
2. ¿Cuáles son las propiedades fundamentales de los cuerpos infinitos?
3. ¿Cuál es la eficacia entre las extensiones inseparables y los cuerpos infinitos?

1.4. Justificación

La mayor parte de las investigaciones realizadas en el área de matemáticas en los niveles de maestría se concentra en los casos de cálculo, tanto diferencial como integral y en la aplicación de un determinado método para la solución de una situación particular. Sin embargo, son muy pocos los estudios que sobre algebra y específicamente sobre algebra abstracta se realizan en estos niveles, dejando de lado

la vastedad de enseñanza que brinda la misma en el desarrollo del pensamiento y las habilidades matemáticas.

La realización de esta investigación sobre extensiones inseparables en un cuerpo infinito, ayudará a tener una recopilación detallada de las propiedades, características y conceptos necesarios para comprender el tema en cuestión, sirviendo como apoyo a estudiantes del área de matemática, así como también, permitirá a los visitantes a la biblioteca contar con una fuente actualizada y contextualizada, que les brindará la oportunidad de profundizar de una manera sencilla en este abstracto mundo algebraico de las extensiones, ofreciendo un punto de referencia para que futuras investigaciones puedan utilizarla como fuente de consulta en la realización de trabajos de la misma línea.

1.5. Objetivos

1.5.1. Objetivo general

Analizar las extensiones inseparables en un cuerpo infinito.

1.5.2. Objetivos específicos

1. Describir las propiedades fundamentales de las extensiones inseparables.
2. Analizar las propiedades fundamentales de los cuerpos infinitos.
3. Comparar la eficacia entre las extensiones inseparables y los cuerpos infinitos.

1.6. Alcances y límites

La presente investigación se sitúa en el campo de la Matemáticas Teóricas, puntualizando en el álgebra abstracta y abarca los elementos relativos a la inseparabilidad de las extensiones en un cuerpo infinito, donde se pretende analizar las propiedades y la relación de las extensiones inseparables en un cuerpo infinito.

CAPÍTULO II

MARCO REFERENCIAL

2.1. Introducción

Este capítulo proporciona la base teórica necesaria, así como los conceptos que contribuirán al cumplimiento de los objetivos establecidos.

2.2. Marco teórico

Definición 2.2.1 (Cuerpo). Se llamará cuerpo, K , a todo anillo $(K, +, \cdot)$ unitario, conmutativo y tal que todo elemento distinto del cero posea inverso, donde: $(K, +)$ es grupo abeliano, $(K \setminus \{0\}, \cdot)$ es grupo abeliano y se satisface la propiedad distributiva: $\forall a, b, c \in A : a \cdot (b + c) = a \cdot b + a \cdot c$. (Palacios, 2002).

Definición 2.2.2 (Cuerpo intermedio). Es la extensión a todo subcuerpo de F que contenga a K . (Olalla, 2015).

Definición 2.2.3 (Cuerpo Infinito). Sea E/K una extensión de Galois finita, con K un cuerpo infinito. Si $\text{SiGal}(E/K) = \{\phi_1, \dots, \phi_n\}$ y $f \in K[X_1, \dots, X_n]$ verifica $f(\phi_1(a), \dots, \phi_n(a)) = 0$ para cada $a \in E$, entonces $f = 0$. (Stonek, 2012).

Definición 2.2.4 (Cuerpo de separación.) Es un cuerpo en un sistema algebraico en el cual las operaciones llamadas adición y multiplicación se pueden realizar y cumplen las propiedades: asociativa, conmutativa y distributiva de la multiplicación respecto de la adición, además de la existencia de inverso aditivo, de inverso multiplicativo y de un elemento neutro para la adición y otro para la multiplicación, los cuales permiten efectuar las operaciones de sustracción y división (excepto la división por cero); estas propiedades ya son familiares de la aritmética de números racionales. (Ivorra, 2010)

Definición 2.2.5 (Cuerpo algebraico.) Se conoce por cuerpo algebraico a una estructura algebraica de la forma $\langle A, \text{op1}, \text{op2} \rangle$, donde A es un conjunto de elementos, op1 y op2 son operaciones binarias de la forma que satisfacen una serie de

axiomas que definen las características del cuerpo. (Carl B. Allendoerfer, Cletus O. Oakley, 1967)

Definición 2.2.6 (Polinomio Irreducible.) Es un polinomio no nulo $p(x) \in k[x]$ se dice irreducible si no puede descomponerse como producto de dos polinomios no constantes. Si $p(x) \in k[x]$ es un polinomio irreducible y $p(x) = f(x) \cdot g(x)$ entonces uno de los dos factores es constante. (Olalla 2015).

Definición 2.2.7 (Extensión.) Es un par (K, F) donde F es un cuerpo y K un subcuerpo de F , denotando una extensión de cuerpos de la forma F/K , aunque en algunos textos es denotada como $K \subseteq F$. (Stonek, 2012)

Definición 2.2.8 (Ecuaciones irreducibles.) En álgebra abstracta, las ecuaciones irreducibles se refieren a ecuaciones polinómicas que no pueden ser descompuestas en factores más simples dentro de un cierto conjunto de números o estructura algebraica. Estas ecuaciones juegan un papel importante en la teoría de anillos. (Olalla 2015).

Según lo plateado anteriormente, estas se relacionan con otros campos y otras estructuras algebraicas, como las siguientes:

Definición 2.2.9 (Ecuaciones Irreducibles en Anillos.) En un anillo, una ecuación polinómica se considera irreducible si no puede ser factorizada en dos polinomios de menor grado (con coeficientes en el mismo anillo) que no sean unidades (elementos invertibles en el anillo). Por ejemplo, en el anillo de los números enteros $(\mathbb{Z})$, la ecuación $x^2 - 2 = 0$ es irreducible, ya que no se puede factorizar en polinomios de grado menor con coeficientes enteros. (Martínez, Rodríguez y García, 2019).

Definición 2.2.10 (Ecuaciones Irreducibles en Campos.) En un campo, una ecuación polinómica es irreducible si no puede ser factorizada en dos polinomios de menor grado (con coeficientes en el mismo campo). En los campos, las ecuaciones irreducibles son especialmente importantes porque generan extensiones de campos que no pueden ser descompuestas en campos más pequeños. (Ivorra, 2010).

Definición 2.2.11 (Extensiones de Campos y Ecuaciones Irreducibles.) Una extensión de campo se forma al adjuntar las raíces de una ecuación polinómica al campo original. Si la ecuación polinómica es irreducible en el campo original, entonces la extensión resultante es una extensión de campo simple, lo que significa que todas las raíces de la ecuación irreducible se pueden expresar en términos de una sola raíz. (Fraleigh, 2003).

Teorema 2.2.1 (Extensión de Campos). Es un resultado fundamental en álgebra abstracta que establece lo siguiente: Dado un campo F y un campo K que contiene a F como subcampo, existe una extensión de campo E de F que está contenida en K , tal que E es un campo de descomposición de un polinomio sobre F . (Carl y Clet, 1967).

En términos más simples, el teorema dice que si tienes un campo F y un campo más grande K que contiene a F , entonces puedes encontrar una extensión de campo E de F dentro de K donde ciertos polinomios de F se factorizan completamente en E . Este resultado es esencial en el estudio de la teoría de campos y tiene muchas aplicaciones en álgebra y geometría algebraica. (López, González y Pérez, 2020).

Definición 2.2.12 (Ecuaciones Ciclotómicas.) Las ecuaciones ciclotómicas, representadas por $\Phi_n(x) = \prod_{\substack{1 \leq k \leq n \\ \text{mcd}(k,n)=1}} (x - \zeta^k)$, donde ζ es una raíz primitiva n -ésima de la unidad, son polinomios irreducibles que surgen al estudiar las raíces de la unidad. Estos polinomios tienen la propiedad crucial de estar relacionados con los campos ciclotómicos, extensiones de los números racionales generadas por las raíces n -ésimas de la unidad, lo que los convierte en objetos fundamentales en la teoría de números algebraicos y en el estudio de cuerpos algebraicos. (Armendia, 2023).

Definición 2.2.13 (Características de una extensión.) Las características de una extensión de campo se refieren a propiedades fundamentales que describen la relación entre dos campos en álgebra abstracta. Esto incluye el grado de la extensión $[E : F]$, que es la dimensión de E como espacio vectorial sobre F , representado como $[E : F] = \dim_F(E)$, y la transitividad, que implica que si $F \subseteq K \subseteq E$, entonces

$[E : F] = [E : K] \cdot [K : F]$. Además, se considera la normalidad, donde cada polinomio irreducible en $F[x]$ que tiene una raíz en E se descompone completamente en E , y la separabilidad, que asegura que todas las raíces de un polinomio irreducible en $F[x]$ sean simples en E . Estas propiedades son esenciales para entender la estructura y las propiedades de las extensiones de campo, y son fundamentales en la teoría de Galois y en el estudio de la clasificación de extensiones de campo. (Salgado, Fierro y Lozoya, 2024).

Definición 2.2.14 (Criterio de separabilidad.) El criterio de separabilidad es un concepto fundamental en el estudio de extensiones de campos en álgebra abstracta. Este criterio establece que una extensión de campo E sobre F es separable si y solo si para cada elemento α en E , el polinomio mínimo de α sobre F tiene todas sus raíces simples en una clausura algebraica de F . En términos más formales, una extensión E sobre F es separable si para todo α en E , el polinomio mínimo $m_{\alpha,F}(x)$ tiene todas sus raíces simples en una clausura algebraica de F . Esto implica que no hay raíces múltiples para los polinomios mínimos de los elementos en E sobre F , lo que tiene importantes implicaciones en la estructura y las propiedades de la extensión de campo, especialmente en la teoría de Galois y en la caracterización de extensiones normales. (Gagliardi y Hernández Peñalver, 2003).

1. **Criterio de Separabilidad:** Una extensión E sobre F es separable si y solo si para todo α en E , el polinomio mínimo $m_{\alpha,F}(x)$ tiene todas sus raíces simples en una clausura algebraica de F . En términos más precisos, si α es un elemento de E , entonces el polinomio mínimo $m_{\alpha,F}(x)$ sobre F tiene todas sus raíces simples en una extensión algebraica de F .
2. **Criterio de Normalidad:** Una extensión E sobre F es normal si y solo si para cada polinomio irreducible $f(x)$ en $F[x]$ con una raíz en E , $f(x)$ se descompone completamente en factores lineales en $E[x]$. En otras palabras, para cada α en E que es una raíz de un polinomio irreducible $f(x)$ en $F[x]$, $f(x)$ se factoriza completamente en factores lineales sobre E . Este criterio garantiza que todas las raíces de los polinomios irreducibles en $F[x]$ que tienen una raíz en E están presentes en E , lo que es fundamental en la teoría de Galois.

Definición 2.2.15 (Extensiones algebraicas). Una extensión E de un campo F se llama algebraica si cada elemento de E es una raíz de algún polinomio con coeficientes en F . En otras palabras, si α es un elemento de E , entonces existe un polinomio no nulo $f(x)$ en $F[x]$ tal que $f(\alpha) = 0$. Esto implica que cada elemento en E es algebraico sobre F . Las extensiones algebraicas son fundamentales en álgebra abstracta y en muchas áreas de las matemáticas, como la teoría de Galois y la geometría algebraica, y proporcionan una rica estructura para el estudio de campos y sus extensiones. (Olalla, 2015).

1. Cerradura algebraica: Si E es una extensión algebraica de F , entonces E contiene una cerradura algebraica de F , es decir, una extensión algebraica maximal de F .
2. Composición de extensiones algebraicas: Si E es una extensión algebraica de F y K es una extensión algebraica de E , entonces K es una extensión algebraica de F . En otras palabras, la composición de dos extensiones algebraicas es una extensión algebraica.
3. Propiedad transitiva: si $F \subseteq E \subseteq K$ y K es una extensión algebraica de F , entonces K es una extensión algebraica de E . Esta propiedad permite extender resultados de una extensión a una extensión más grande.
4. Cardinalidad: Si E es una extensión algebraica finita de F , entonces E es finito si y solo si F es finito.
5. Caracterización en términos de torres de cuerpos: Una extensión E de F es algebraica si y solo si E es el cuerpo de descomposición de un conjunto de polinomios sobre F . (Armendia, 2023).

Definición 2.2.16 (Extensiones separables). Las extensiones separables son un tipo importante de extensiones de campos en álgebra abstracta. Una extensión E de un campo F se dice que es separable si cada elemento de E es una raíz de un polinomio separable sobre F . Un polinomio $f(x)$ sobre F se dice que es separable si no tiene raíces múltiples (es decir, todas sus raíces son simples) en una clausura

algebraica de F . Aquí hay algunas propiedades clave de las extensiones separables: (López, González y Pérez, 2010).

1. Composición de extensiones separables: Si E es una extensión separable de F y K es una extensión separable de E , entonces K es una extensión separable de F . En otras palabras, la composición de dos extensiones separables es una extensión separable.
2. Cerradura separable: Dado un campo F , se puede construir una cerradura separable de F , que es una extensión separable maximal de F .
3. Caracterización en términos de polinomios separables: Una extensión E de F es separable si y solo si todos los polinomios irreducibles en $F[x]$ tienen todas sus raíces simples en E . Es decir, si $f(x)$ es irreducible sobre F , entonces $f(x)$ se descompone en factores lineales sobre E y todas sus raíces son simples.
4. Cardinalidad de extensiones separables finitas: Si E es una extensión separable finita de F , entonces la cardinalidad de E es menor o igual a $[E : F] \times |F|$, donde $[E : F]$ es el grado de la extensión.

Definición 2.2.17 (Elementos puramente inseparables.) Un elemento algebraico k sobre un cuerpo K es puramente inseparable si es la única raíz de su polinomio mínimo sobre K . Es una extensión K/k es puramente inseparable si y sólo si todo elemento de K es puramente inseparable sobre k . (Fasano, 2005).

Definición 2.2.18 (Extensiones puramente inseparables en un cuerpo infinito.) Sea L una extensión del cuerpo infinito K y $x \in L$. Se dice que x es radical sobre el cuerpo K si existe un entero r tal que $(x^p)^r \in K$. Se dice que L es una extensión puramente inseparable de K si todo elemento de L es radical sobre K . (Gagliardi y Hernández, 2003).

En álgebra, una extensión puramente inseparable de campos es una extensión $k \subseteq K$ de campos de la característica $p > 0$ tal que cada elemento de K es una raíz

de una ecuación de la forma $x^q = un$, con q una potencia de p y una en k .

Una extensión puramente inseparable se llama una extensión modular si es un producto tensorial de simples extensiones, por lo que, en particular, cada extensión de exponente 1 es modular, pero hay extensiones no modulares de exponente 2.

Si F es una extensión puramente inseparable finito dimensional del cuerpo K y $\text{cardinal } K = p \neq 0$, entonces $[F : K] = p^n$, para algún $n \geq 0$.

Un elemento a en una extensión de un cuerpo K es puramente inseparable sobre K si y sólo si existe un número natural n tal que $(a^p)^n \in k$.

Si $a \in F$ inseparable puro sobre el cuerpo K , entonces a es inseparable puro sobre cualquier cuerpo infinito E . Luego, si F es inseparable sobre K , entonces F es inseparable sobre el cuerpo infinito E . (Stonek, 2012).

CAPÍTULO III METODOLOGÍA

3.1. Introducción

En este capítulo se describen los aspectos relacionados con la metodología que sustentan las extensiones inseparables en un cuerpo infinito en el desarrollo de esta investigación. En el mismo se detallan el diseño, tipo, y método del contenido a trabajar.

3.2. Método de investigación

La investigación empleó el método cualitativo, ya que se dirigió a explorar y analizar conceptos y teoremas que expresan resultados de álgebra abstracta. La elección de este método fue apropiada debido a que el álgebra abstracta a menudo involucra estructuras matemáticas complejas y sutilezas conceptuales. El método deductivo permitió capturar esta complejidad al analizar en detalle las relaciones y propiedades de estas estructuras sin simplificar en exceso (Abarca et al., 2013).

3.3. Diseño de investigación

Esta investigación, según la intervención, fue no experimental, dado que se trató de un estudio documental en el que no se manipularon las variables objeto de estudio, debido a su carácter teórico y abstracto orientado a alcanzar los objetivos propuestos. En términos de tiempo, el estudio fue transversal, ya que los datos se recolectaron en un solo momento. En cuanto a la búsqueda de la causa, el estudio fue analítico y descriptivo. Fue analítico porque incluyó estudios comparativos con diversas fuentes que contenían conceptos y propiedades relacionadas con extensiones inseparables y cuerpos infinitos. También fue descriptivo porque permitió detallar conceptos y procesos matemáticos (Sampieri, 2010).

3.4. Tipo de investigación

Esta investigación fue de tipo descriptiva, exploratoria y explicativa. Fue exploratoria, ya que implicó la recopilación de datos de diversas fuentes relacionadas con el tema en discusión, proporcionando las directrices esenciales para llevar a cabo el estudio. También fue descriptiva, dado que se enfocó en describir el comportamiento del contenido de los documentos encontrados, destacando aquellos que contribuyeron a la resolución del problema de investigación. Adicionalmente, fue explicativa, ya que detalló minuciosamente las condiciones requeridas para las extensiones inseparables (Hernández, Fernández y Baptista, 2010).

3.5. Enfoque de investigación.

Esta investigación tuvo un enfoque cualitativo, ya que su desarrollo se basó en descripciones, explicaciones, comparaciones y análisis de definiciones, teoremas y demostraciones relacionadas con las extensiones inseparables en un cuerpo infinito. Según lo expresado por Hernández, Sampieri y Torres (2018), el enfoque cualitativo implica una acción indagatoria en la que no se operacionalizan variables.

3.6. Procedimientos de investigación

- a) En primer lugar, se trabajó en la lectura de documentos relacionados con el tema de investigación, con el fin de comprender los conocimientos existentes y establecer los antecedentes y limitaciones del tema a estudiar.
- b) Luego, en un segundo paso, se desarrolló la estructura del enfoque del contenido de la investigación y su análisis.
- c) Se buscó información de materiales físicos en universidades para verificar la revisión de literatura sobre el tema, así como de forma digital.
- d) Se realizó una verificación del cumplimiento de los objetivos propuestos al inicio de la investigación en combinación con el asesor.

CAPÍTULO IV PRESENTACIÓN DE LOS RESULTADOS

4.1. Introducción

En el marco de la presente investigación, se presenta un análisis exhaustivo de las extensiones inseparables en un cuerpo infinito. Los resultados obtenidos a partir de este enfoque detallado proporcionan una visión clara de cómo las extensiones inseparables y los cuerpos infinitos se caracterizan y se interrelacionan, revelando tanto las fortalezas como las limitaciones de cada uno.

4.2. Propiedades fundamentales de las extensiones inseparables

Las extensiones inseparables son un concepto fundamental en la teoría de cuerpos, particularmente en el contexto de cuerpos de característica positiva. Estas extensiones, que surgen cuando el polinomio mínimo de algún elemento en la extensión no tiene raíces distintas, representan una desviación significativa de las extensiones separables, donde todos los polinomios mínimos tienen raíces simples.

La importancia de las extensiones inseparables radica no solo en su frecuencia en características positivas, sino también en las profundas implicaciones que tienen para la teoría de Galois, la estructura de cuerpos y el análisis algebraico. A través de estas extensiones, se pueden explorar fenómenos únicos que no aparecen en características cero, ofreciendo una ventana a la rica y compleja naturaleza de los cuerpos en matemáticas.

4.2.1. Propiedades fundamentales de las extensiones inseparables

1. Una extensión de cuerpos L/K se dice inseparable si no es separable. Más formalmente, una extensión L/K es inseparable si existe al menos un elemento

$\alpha \in L$ tal que el polinomio mínimo de α sobre K no es separable, es decir, no tiene raíces distintas (o, equivalentemente, su derivada no es coprima con el polinomio mismo).

Ejemplo 4.2.1 Considere los cuerpos $K = \mathbb{F}_p(t)$ y $L = \mathbb{F}_p(t^{1/p})$, donde p es un número primo y $\mathbb{F}_p$ es el cuerpo finito con p elementos.

Aquí, $K = \mathbb{F}_p(t)$ es el cuerpo de funciones racionales con coeficientes en el cuerpo finito $\mathbb{F}_p$, mientras que $L = \mathbb{F}_p(t^{1/p})$ es una extensión de K obtenida añadiendo la raíz p -ésima de t .

Tome un elemento α en L . Escoja $\alpha = t^{1/p}$. El polinomio mínimo de $\alpha = t^{1/p}$ sobre K es $f(x) = x^p - t$.

Para verificar si la extensión es inseparable, se necesita ver si el polinomio mínimo $f(x) = x^p - t$ no es separable. Calculando la derivada de $f(x)$:

$$f'(x) = \frac{d}{dx}(x^p - t) = px^{p-1}.$$

En $\mathbb{F}_p$, el número primo p es igual a 0, por lo tanto, $f'(x) = 0$. Dado que la derivada del polinomio es 0, esto implica que el polinomio $f(x) = x^p - t$ no tiene raíces distintas en su descomposición en factores lineales.

Por lo tanto, el polinomio mínimo de $\alpha = t^{1/p}$ sobre $K = \mathbb{F}_p(t)$ no es separable, y la extensión L/K es inseparable. Este ejemplo ilustra cómo una extensión de cuerpos puede ser inseparable si el polinomio mínimo de algún elemento en la extensión no es separable.

2. Característica del Cuerpo Base. Las extensiones inseparables ocurren únicamente en cuerpos de característica positiva p . En cuerpos de característica cero, todas las extensiones son separables.

Para entender mejor cómo la característica del cuerpo base afecta la posibilidad de tener extensiones inseparables, considere dos ejemplos: uno con un cuerpo de característica positiva p y otro con un cuerpo de característica cero.

Ejemplo 4.2.2 Cuerpo de Característica Positiva p . Considere el cuerpo finito $\mathbb{F}_p$ con p elementos, donde p es un número primo. Sea $K = \mathbb{F}_p(t)$, el cuerpo de funciones racionales en una variable t con coeficientes en $\mathbb{F}_p$.

Ahora, tome una extensión $L = \mathbb{F}_p(t^{1/p})$. Aquí, L se obtiene añadiendo la raíz p -ésima de t a K . El elemento $\alpha = t^{1/p}$ tiene un polinomio mínimo sobre K dado por $f(x) = x^p - t$.

Para determinar si esta extensión es inseparable, calcula la derivada del polinomio $f(x) : f'(x) = \frac{d}{dx}(x^p - t) = px^{p-1}$. En el cuerpo $\mathbb{F}_p$, p es igual a 0, por lo que $f'(x) = 0$. Esto significa que el polinomio mínimo no tiene raíces distintas, lo que confirma que la extensión L/K es inseparable.

Ejemplo 4.2.3 Cuerpo de Característica Cero. Considere el cuerpo $\mathbb{Q}$, que es el cuerpo de los números racionales. La característica de $\mathbb{Q}$ es cero. Sea $K = \mathbb{Q}$ y considere una extensión $L = \mathbb{Q}(\sqrt{2})$, obtenida añadiendo la raíz cuadrada de 2.

El elemento $\alpha = \sqrt{2}$ tiene un polinomio mínimo sobre K dado por $f(x) = x^2 - 2$. Calcula la derivada del polinomio $f(x)$:

$$f'(x) = \frac{d}{dx}(x^2 - 2) = 2x.$$

La derivada $f'(x) = 2x$ no es cero para $x = \sqrt{2}$, lo que significa que el polinomio $f(x) = x^2 - 2$ tiene raíces distintas y es separable.

Este ejemplo muestra que en cuerpos de característica cero, como $\mathbb{Q}$, todas las extensiones son separables. En contraste, en cuerpos de característica positiva p , como $\mathbb{F}_p$, pueden ocurrir extensiones inseparables, como se observa en la extensión $\mathbb{F}_p(t^{1/p})$.

3. Polinomios Inseparables. Un polinomio $f(x) \in K[x]$ se dice inseparable si tiene una raíz múltiple en su clausura algebraica. Esto es equivalente a decir que $f(x)$ y su derivada $f'(x)$ tienen un factor común no trivial. En cuerpos de característica p , un polinomio $f(x)$ puede tener la forma $g(x^p)$, donde $g(x)$ es un polinomio en $K[x]$.

Ejemplo 4.2.4 Polinomios Inseparables. Para ilustrar el concepto de polinomios inseparables, considere un cuerpo de característica positiva p y un polinomio en ese cuerpo.

Sea $K = \mathbb{F}_p$, el cuerpo finito con p elementos, donde p es un número primo. Considere el polinomio $f(x) = x^{p^2} - t$ en $K[x]$. Para determinar si el polinomio $f(x)$ es inseparable, necesita verificar si tiene una raíz múltiple en su clausura algebraica. Esto es equivalente a verificar si $f(x)$ y su derivada $f'(x)$ tienen un factor común no trivial.

Calculando la derivada de $f(x)$:

$$f'(x) = \frac{d}{dx} (x^{p^2} - t) = p^2 x^{p^2-1}.$$

En el cuerpo $\mathbb{F}_p, p^2 \equiv 0 \text{ mód } p$, por lo que $f'(x) = 0$. Dado que la derivada $f'(x) = 0$, esto implica que el polinomio $f(x) = x^{p^2} - t$ no tiene raíces distintas y , por lo tanto, es inseparable.

Un polinomio en un cuerpo de característica p puede tener la forma $g(x^p)$, donde $g(x)$ es un polinomio en $K[x]$. Por ejemplo, considere el polinomio $h(x) = x^p - a$ en $\mathbb{F}_p[x]$, donde $a \in \mathbb{F}_p$. Este polinomio $h(x)$ puede ser escrito como $g(x^p)$, donde $g(x) = x - a$.

Calcula la derivada de $h(x)$:

$$h'(x) = \frac{d}{dx} (x^p - a) = px^{p-1}.$$

En el cuerpo $\mathbb{F}_p, p \equiv 0 \text{ mód } p$, por lo que $h'(x) = 0$. Este polinomio $h(x) = x^p - a$ tiene la forma $g(x^p)$ y es inseparable ya que su derivada es cero, lo que significa que tiene una raíz múltiple

4. Exponente de Inseparabilidad. El exponente de inseparabilidad de una extensión L/K es el mayor número e tal que existe una torre de extensiones $L = L_e \supset L_{e-1} \supset \cdots \supset L_1 \supset K$ donde cada $L_i \supset L_{i-1}$ es una extensión puramente inseparable de grado p . Si L/K es finita, el grado de inseparabilidad es una potencia de p

Ejemplo 4.2.5 Sea $K = \mathbb{F}_p(t)$, el cuerpo de funciones racionales en una variable t con coeficientes en el cuerpo finito $\mathbb{F}_p$, donde p es un número primo. Construya una torre de extensiones puramente inseparables de la siguiente manera:

Comenzando con K y tomando $L_1 = K(t^{1/p})$, una extensión de K obtenida añadiendo la raíz p -ésima de t . Esta es una extensión puramente inseparable de grado p porque el polinomio mínimo de $t^{1/p}$ sobre K es $x^p - t$, el cual no es separable.

Ahora, considerando $L_2 = L_1(t^{1/p^2}) = K(t^{1/p}, t^{1/p^2})$. Esta extensión también es puramente inseparable de grado p porque el polinomio mínimo de t^{1/p^2} sobre L_1 es $x^p - t^{1/p}$, el cual es inseparable.

Continúa construyendo la torre de extensiones. Tome $L_3 = L_2(t^{1/p^3}) = K(t^{1/p}, t^{1/p^2}, t^{1/p^3})$. Esta extensión es nuevamente puramente inseparable de grado p porque el polinomio mínimo de t^{1/p^3} sobre L_2 es $x^p - t^{1/p^2}$, el cual también es inseparable.

En general, para cualquier e , se puede construir la extensión

$$L_e = K(t^{1/p}, t^{1/p^2}, \dots, t^{1/p^e}).$$

Cada paso en esta torre de extensiones es puramente inseparable de grado p .

El exponente de inseparabilidad de la extensión L/K es el mayor número e tal que existe una torre de extensiones $L = L_e \supset L_{e-1} \supset \dots \supset L_1 \supset K$, donde cada $L_i \supset L_{i-1}$ es una extensión puramente inseparable de grado p . En este ejemplo, si tome $L = L_e = K(t^{1/p}, t^{1/p^2}, \dots, t^{1/p^e})$, el exponente de inseparabilidad es e .

Si L/K es una extensión finita, el grado de inseparabilidad es una potencia de p . En nuestro ejemplo, el grado de la extensión L_e/K es p^e , una potencia de p , lo que confirma que el exponente de inseparabilidad es e .

5. Extensiones Puramente Inseparables. Una extensión L/K es puramente inseparable si cada elemento $\alpha \in L$ satisface una ecuación de la forma $\alpha^{p^n} \in K$ para

algún n . Estas extensiones no agregan nuevas raíces en un sentido clásico, ya que cualquier elemento de L es una p -ésima potencia de un elemento de K .

Ejemplo 4.2.6 Sea $K = \mathbb{F}_p(t)$, el cuerpo de funciones racionales en una variable t con coeficientes en el cuerpo finito $\mathbb{F}_p$, donde p es un número primo. Considere una extensión L de K definida por $L = K(t^{1/p})$.

En esta extensión, tome un elemento $\alpha \in L$. Se puede elegir $\alpha = t^{1/p}$. Para verificar que esta extensión es puramente inseparable, necesita mostrar que α satisface una ecuación de la forma $\alpha^{p^n} \in K$ para algún n .

En este caso, $\alpha = t^{1/p}$ satisface $\alpha^p = (t^{1/p})^p = t \in K$. Por lo tanto, $\alpha = t^{1/p}$ es una p -ésima potencia de un elemento de K , lo que confirma que α cumple con la condición para una extensión puramente inseparable.

Más generalmente, considere una extensión $L = K(t^{1/p^n})$. Tome $\alpha = t^{1/p^n}$. Para verificar que α satisface una ecuación de la forma $\alpha^{p^m} \in K$ para algún m , observe que:

$$\alpha^{p^n} = (t^{1/p^n})^{p^n} = t \in K.$$

Así, $\alpha = t^{1/p^n}$ es una p^n -ésima potencia de un elemento de K , lo que muestra que α cumple con la condición de una extensión puramente inseparable.

6. Descomposición de Extensiones Finitas

Toda extensión finita L/K en característica positiva puede descomponerse de manera única en una parte separable y una parte puramente inseparable, es decir, $L = L_s L_i$, donde L_s/K es separable y L_i/K es puramente inseparable.

Ejemplo 4.2.7 Suponga que $K = \mathbb{F}_p(t)$, el cuerpo de funciones racionales en una variable t con coeficientes en el cuerpo finito $\mathbb{F}_p$, donde p es un número primo. Considere la extensión $L = \mathbb{F}_p(t^{1/p}, \sqrt{t+1})$.

Parte Puramente Inseparable. Primero, identifique la parte puramente inseparable de la extensión. Tome $L_i = \mathbb{F}_p(t^{1/p})$. Aquí, L_i es una extensión de K obtenida

añadiendo la raíz p -ésima de t , y es puramente inseparable porque cualquier elemento $\alpha \in L_i$ satisface una ecuación de la forma $\alpha^{p^n} \in K$ para algún n . Por ejemplo, $(t^{1/p})^p = t \in K$.

Parte Separable. Ahora, identifique la parte separable de la extensión. Considere la extensión $L_s = \mathbb{F}_p(t^{1/p}, \sqrt{t+1})$. La adición de $\sqrt{t+1}$ a $\mathbb{F}_p(t^{1/p})$ forma una extensión separable sobre $\mathbb{F}_p(t^{1/p})$ porque el polinomio mínimo de $\sqrt{t+1}$ sobre $\mathbb{F}_p(t^{1/p})$ es $x^2 - (t+1)$, el cual es separable (tiene raíces distintas).

Descomposición de la Extensión Entonces, la extensión total $L = \mathbb{F}_p(t^{1/p}, \sqrt{t+1})$ se puede descomponer en:

$$L = L_i(\sqrt{t+1})$$

donde $L_i = \mathbb{F}_p(t^{1/p})$ es puramente inseparable y $\sqrt{t+1}$ es una raíz de un polinomio separable sobre L_i .

Esta descomposición muestra que cualquier extensión finita L/K en característica positiva se puede descomponer de manera única en una parte separable L_s y una parte puramente inseparable L_i . En este ejemplo, L_i/K es puramente inseparable y L_s/K es separable. Por lo tanto, la extensión total L/K combina ambas partes.

7. Teorema Fundamental de Teoría de Galois en Característica Positiva. En característica positiva, el teorema de Galois se modifica para tener en cuenta extensiones inseparables. En este contexto, el grupo de Galois $\text{Gal}(L/K)$ puede no capturar toda la estructura de la extensión si L/K no es puramente inseparable. Es decir, el grupo de Galois solo describe la parte separable de la extensión.

Ejemplo 4.2.8 Sea $K = \mathbb{F}_p(t)$, el cuerpo de funciones racionales en una variable t con coeficientes en el cuerpo finito $\mathbb{F}_p$, donde p es un número primo. Considere la extensión $L = \mathbb{F}_p(t^{1/p}, \sqrt{t})$.

Parte Puramente Inseparable Primero, identifique la parte puramente inseparable de la extensión. Sea $L_i = \mathbb{F}_p(t^{1/p})$. Esta extensión es puramente inseparable

porque cualquier elemento de L_i satisface una ecuación de la forma $\alpha^{p^n} \in K$ para algún n . Por ejemplo, $(t^{1/p})^p = t \in K$.

Parte Separable Ahora, considere la parte separable de la extensión. Sea $L_s = \mathbb{F}_p(t^{1/p}, \sqrt{t})$. Aquí, $\sqrt{t}$ es una raíz de un polinomio separable sobre L_i , dado que el polinomio mínimo de $\sqrt{t}$ sobre $\mathbb{F}_p(t^{1/p})$ es $x^2 - t$, el cual tiene raíces distintas.

Grupo de Galois y Descripción de la Extensión El grupo de Galois $\text{Gal}(L/K)$ solo describe la parte separable de la extensión L/K . En este caso, considere la extensión separable $L_s = \mathbb{F}_p(t^{1/p}, \sqrt{t})$ sobre $L_i = \mathbb{F}_p(t^{1/p})$.

El grupo de Galois $\text{Gal}(L_s/L_i)$ consiste en automorfismos que fijan L_i y permutan las raíces de los polinomios separables en L_s . Dado que $\sqrt{t}$ es la única raíz del polinomio mínimo $x^2 - t$ en L_s , el grupo de Galois es trivial.

Descomposición de la Extensión Completa. Finalmente, considere la extensión completa $L = \mathbb{F}_p(t^{1/p}, \sqrt{t})$ sobre $K = \mathbb{F}_p(t)$. La parte puramente inseparable es $L_i = \mathbb{F}_p(t^{1/p})$ y la parte separable es $L_s = \mathbb{F}_p(t^{1/p}, \sqrt{t})$. El grupo de Galois $\text{Gal}(L/K)$ describe solo la parte separable L_s/L_i , dejando fuera la estructura puramente inseparable.

4.3. Propiedades fundamentales de los cuerpos infinitos

Las propiedades fundamentales de los cuerpos infinitos son un tema central en la teoría de cuerpos y en diversas ramas de las matemáticas, como el álgebra, la teoría de números y la geometría algebraica. Un cuerpo infinito es uno que contiene un número infinito de elementos, y esta característica le confiere una serie de propiedades y comportamientos únicos que lo distinguen de los cuerpos finitos. La comprensión de los cuerpos infinitos es esencial para desentrañar las estructuras algebraicas subyacentes y para abordar problemas que involucran polinomios, extensiones de cuerpos, y aplicaciones geométricas y aritméticas. A lo largo de esta exploración, examinaremos cómo la infinitud de estos cuerpos influye en su estructura interna, en las extensiones

que pueden formar, y en las simetrías y automorfismos que los caracterizan.

Definición 4.3.1 Un cuerpo K se dice algebraicamente cerrado si todo polinomio no constante con coeficientes en K tiene una raíz en K . Por ejemplo, el cuerpo de los números complejos $\mathbb{C}$ es un cuerpo algebraicamente cerrado. Todo cuerpo K tiene una extensión algebraica mínima $\bar{K}$, llamada el cierre algebraico de K , que es algebraicamente cerrado.

Definición 4.3.2 Un cuerpo K se dice perfecto si cada extensión algebraica de K es separable, lo cual ocurre automáticamente si K tiene característica cero o si es un cuerpo finito de característica p . En cuerpos infinitos de característica p , ser perfecto implica que todo elemento de K es una p -ésima potencia, es decir, $K = K^p$.

Teorema 4.3.1 (Steinitz). Este establece que todos los cuerpos infinitos son isomorfos a una extensión puramente trascendental de un cuerpo perfecto. Es decir, un cuerpo infinito K puede ser visto como una extensión generada por un conjunto de elementos trascendentes (no algebraicos) sobre su cierre perfecto.

Para cuerpos infinitos, la teoría de Galois ofrece una correspondencia entre las extensiones de cuerpos y ciertos subgrupos de automorfismos del cuerpo. Esta teoría se utiliza para estudiar las simetrías de las raíces de polinomios y tiene aplicaciones profundas en álgebra y geometría.

Definición 4.3.3 La dimensión trascendental de un cuerpo K sobre un subcuerpo F es el número de elementos trascendentes independientes en K sobre F . Para cuerpos infinitos, esta dimensión puede ser infinita, y juega un papel crucial en la estructura y clasificación de las extensiones de cuerpos.

Definición 4.3.4 En característica p , una extensión de Artin-Schreier es una extensión de la forma $K(\alpha)$ donde α es raíz de un polinomio de Artin-Schreier $x^p - x - a$ para algún $a \in K$. Estas extensiones son ejemplos fundamentales de extensiones inseparables en cuerpos infinitos.

Definición 4.3.5 Para un cuerpo infinito K , sus subcuerpos también poseen propiedades interesantes. Por ejemplo, si K es un cuerpo de características p (un número primo), entonces cualquier subcuerpo de K también tiene característica p . Esta propiedad afecta la estructura de las extensiones y las relaciones algebraicas dentro del cuerpo.

4.3.1. Propiedades Específicas de los Cuerpos Infinitos

1. Infinitud y Cardinalidad. Los cuerpos infinitos pueden tener distintas cardinalidades. Por ejemplo, los números reales $\mathbb{R}$ tienen la cardinalidad del continuo, mientras que el campo de funciones racionales sobre un cuerpo finito puede tener cardinalidad infinita pero numerable.
2. Subcuerpos Infinitos. Todo cuerpo infinito tiene subcuerpos infinitos. Por ejemplo, dentro del cuerpo de los números reales $\mathbb{R}$, el cuerpo de los números racionales $\mathbb{Q}$ es infinito y denso en $\mathbb{R}$.
3. Automorfismos y Simetrías. Los cuerpos infinitos tienen grupos de automorfismos ricos y complejos. Por ejemplo, el grupo de automorfismos de $\mathbb{C}$ es extremadamente grande y está relacionado con la teoría de Galois y la estructura de las raíces de los polinomios.
4. Topología de Zariski. En la teoría de cuerpos, especialmente en geometría algebraica, se usa la topología de Zariski. En esta topología, los conjuntos cerrados corresponden a los conjuntos de ceros de conjuntos de polinomios. Para cuerpos infinitos, la topología de Zariski es más rica y compleja que en el caso de cuerpos finitos.

Ejemplo 4.3.1 (Infinitud y Cardinalidad). Cuerpo de los Números Reales ($\mathbb{R}$) : Este cuerpo es infinito y tiene la cardinalidad del continuo, es decir, hay tantos números reales como puntos en una recta continua. Esto es una cantidad mucho mayor que la cardinalidad del conjunto de los números naturales, que es infinita pero numerable.

El conjunto de los números reales, denotado por $\mathbb{R}$, es un ejemplo clásico de un conjunto infinito con una propiedad particular de cardinalidad conocida como la

cardinalidad del continuo. Formalmente, esto se expresa diciendo que $\mathbb{R}$ tiene cardinalidad c , donde $c = 2^{\aleph_0}$. Esto significa que la cantidad de elementos en $\mathbb{R}$ es igual a la cantidad de subconjuntos del conjunto de los números naturales $\mathbb{N}$.

Por otro lado, el conjunto de los números naturales $\mathbb{N}$ es también infinito, pero su cardinalidad es $\aleph_0$, que es el cardinal más pequeño de un conjunto infinito. Un conjunto con cardinalidad $\aleph_0$ se denomina "numerable.º contable", lo que implica que existe una biyección entre $\mathbb{N}$ y el conjunto en cuestión. Esto se traduce en que los elementos de $\mathbb{N}$ pueden ser enumerados en una secuencia infinita $1, 2, 3, \dots$.

La cardinalidad del conjunto $\mathbb{R}$ es mayor que la cardinalidad de $\mathbb{N}$. Esta afirmación se puede demostrar mediante el argumento de la diagonalización de Cantor. Suponga que existe una biyección entre $\mathbb{N}$ y $\mathbb{R}$. Esto implicaría que los números reales pueden ser enumerados como una secuencia $r_1, r_2, r_3, \dots$. Cantor mostró que siempre se puede construir un número real que no esté en esta secuencia, contradiciendo así la supuesta biyección. Esto demuestra que no existe una correspondencia uno a uno entre $\mathbb{N}$ y $\mathbb{R}$, confirmando que la cardinalidad de $\mathbb{R}$ es c , un cardinal mayor que $\aleph_0$. Analizar las propiedades fundamentales de los cuerpos infinitos.

Ejemplo 4.3.2 (Infinitud y Cardinalidad). Cuerpo de Funciones Racionales sobre un Cuerpo Finito ($\mathbb{F}_q(x)$) : Sea $\mathbb{F}_q$ un cuerpo finito con q elementos. El cuerpo de funciones racionales $\mathbb{F}_q(x)$ es infinito pero numerable, ya que sus elementos pueden representarse como cocientes de polinomios con coeficientes en $\mathbb{F}_q$.

El cuerpo de funciones racionales sobre un cuerpo finito, denotado como $\mathbb{F}_q(x)$, es un conjunto de interés en álgebra abstracta y teoría de números. Aquí, $\mathbb{F}_q$ representa un cuerpo finito con q elementos. Un cuerpo finito es un conjunto finito de elementos que forma un campo bajo las operaciones de suma y multiplicación. Por ejemplo, $\mathbb{F}_2$ tiene dos elementos, típicamente denotados como $\{0, 1\}$, con las operaciones de suma y multiplicación definidas de manera modular.

El conjunto $\mathbb{F}_q(x)$ consiste en todas las funciones racionales de la forma $\frac{f(x)}{g(x)}$, donde $f(x)$ y $g(x)$ son polinomios con coeficientes en $\mathbb{F}_q$ y $g(x) \neq 0$. Es decir, cada elemento de $\mathbb{F}_q(x)$ puede escribirse como un cociente de dos polinomios en x con coeficientes en $\mathbb{F}_q$.

Para comprender la infinitud y numerabilidad de $\mathbb{F}_q(x)$, observe lo siguiente. Aunque $\mathbb{F}_q$ tiene un número finito de elementos, los polinomios en $\mathbb{F}_q[x]$ pueden tener grados arbitrariamente grandes, lo que implica que hay infinitos polinomios en $\mathbb{F}_q[x]$. Por tanto, los cocientes de estos polinomios, que constituyen $\mathbb{F}_q(x)$, también forman un conjunto infinito.

Sin embargo, a pesar de ser infinito, $\mathbb{F}_q(x)$ es numerable. Esto se debe a que se puede enumerar todos los polinomios en $\mathbb{F}_q[x]$, y por tanto, todos los cocientes de polinomios. Más específicamente, se pueden listar primero todos los polinomios de grado 0, luego todos los de grado 1, y así sucesivamente. Dado que cada polinomio en $\mathbb{F}_q[x]$ puede representarse de una manera finita y ordenada, también se puede enumerar todas las posibles fracciones $\frac{f(x)}{g(x)}$.

Para formalizar esta numerabilidad, considere que se puede establecer una biyección entre $\mathbb{N}$ (el conjunto de los números naturales) y $\mathbb{F}_q(x)$. Enumera todos los pares ordenados de polinomios $(f(x), g(x))$ con $g(x) \neq 0$, lo que nos permite asignar un número natural a cada función racional en $\mathbb{F}_q(x)$. Por lo tanto, hay una correspondencia uno a uno entre los elementos de $\mathbb{F}_q(x)$ y $\mathbb{N}$, confirmando que $\mathbb{F}_q(x)$ es numerable.

Ejemplo 4.3.3 (Subcuerpos Infinitos). Números Complejos ($\mathbb{C}$) y Números Racionales ($\mathbb{Q}$): El cuerpo de los números complejos $\mathbb{C}$ es infinito. Dentro de $\mathbb{C}$, el cuerpo de los números racionales $\mathbb{Q}$ también es infinito. Aunque $\mathbb{Q}$ es mucho "más pequeño" que $\mathbb{C}$, sigue siendo un conjunto infinito y denso en $\mathbb{C}$.

El cuerpo de los números complejos $\mathbb{C}$ es un conjunto infinito que incluye todos los números de la forma $a + bi$, donde a y b son números reales y i es la unidad

imaginaria con la propiedad $i^2 = -1$. Este conjunto tiene la cardinalidad del continuo, lo que significa que su tamaño es igual a la cantidad de puntos en una recta continua, denotada por $\mathfrak{c}$. Esto indica que $\mathbb{C}$ tiene una cardinalidad mucho mayor que la de conjuntos numerables como los números naturales $\mathbb{N}$.

Dentro del cuerpo de los números complejos $\mathbb{C}$, se encuentra el subcuerpo de los números racionales $\mathbb{Q}$. El cuerpo de los números racionales $\mathbb{Q}$ está compuesto por todos los números que pueden expresarse como cocientes $\frac{p}{q}$, donde p y q son enteros y $q \neq 0$. Aunque $\mathbb{Q}$ es un conjunto infinito, su cardinalidad es $\aleph_0$, lo que significa que es numerable. Esto quiere decir que se puede establecer una correspondencia uno a uno entre $\mathbb{Q}$ y $\mathbb{N}$, permitiendo enumerar todos los números racionales.

Aunque $\mathbb{Q}$ es más pequeño que $\mathbb{C}$ en términos de cardinalidad, sigue siendo un conjunto infinito. Además, $\mathbb{Q}$ es denso en $\mathbb{C}$. La densidad de $\mathbb{Q}$ en $\mathbb{C}$ significa que entre cualquier dos números complejos hay un número racional, o más formalmente, en cualquier intervalo abierto en $\mathbb{C}$, por pequeño que sea, siempre se puede encontrar un número racional.

Para ilustrar la relación entre $\mathbb{C}$ y $\mathbb{Q}$ de manera más precisa, considere que cada número complejo puede representarse como $a + bi$ con $a, b \in \mathbb{R}$. Dentro de este contexto, $\mathbb{Q}$ puede verse como el conjunto de todos los números de la forma $\frac{p}{q}$, donde p y q son enteros. La densidad de $\mathbb{Q}$ en $\mathbb{C}$ implica que cualquier número complejo puede aproximarse arbitrariamente cerca por números racionales, reflejando la estructura rica y densa de $\mathbb{Q}$ dentro de $\mathbb{C}$.

En resumen, el cuerpo de los números complejos $\mathbb{C}$ es un conjunto infinito de cardinalidad $\mathfrak{c}$, mientras que el subcuerpo de los números racionales $\mathbb{Q}$, aunque también infinito, tiene una cardinalidad $\aleph_0$ y es numerable. La densidad de $\mathbb{Q}$ en $\mathbb{C}$ subraya la presencia ubicua de los números racionales dentro del conjunto de los números complejos.

Ejemplo 4.3.4 (Automorfismos y Simetrías). Cuerpo de los Números Complejos ($\mathbb{C}$) sobre los Números Reales ($\mathbb{R}$): Un automorfismo del cuerpo $\mathbb{C}$ que fija $\mathbb{R}$ es la conjugación compleja, que envía cada número complejo $a + bi$ a $a - bi$. Este automorfismo muestra una simetría fundamental en la estructura de $\mathbb{C}$.

Un automorfismo de un cuerpo es una función biyectiva de ese cuerpo en sí mismo que preserva las operaciones de suma y multiplicación. En otras palabras, si ϕ es un automorfismo de un cuerpo K , entonces para todos los $x, y \in K$, se tiene que:

1. $\phi(x + y) = \phi(x) + \phi(y)$
2. $\phi(x \cdot y) = \phi(x) \cdot \phi(y)$
3. $\phi(1) = 1$

Un automorfismo del cuerpo $\mathbb{C}$ que fija el subcuerpo $\mathbb{R}$ es la conjugación compleja. La conjugación compleja es una función que toma un número complejo $a + bi$ y lo mapea a su conjugado $a - bi$, donde a y b son números reales y i es la unidad imaginaria con $i^2 = -1$.

Matemáticamente, si defina $\phi : \mathbb{C} \rightarrow \mathbb{C}$ tal que $\phi(a + bi) = a - bi$, entonces ϕ es un automorfismo de $\mathbb{C}$. Verifique que ϕ cumple las propiedades necesarias:

1. Preservación de la suma:

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

2. Preservación de la multiplicación:

$$\begin{aligned}\phi((a + bi) \cdot (c + di)) &= \phi((ac - bd) + (ad + bc)i) = (ac - bd) - (ad + bc)i \\ &= (a - bi) \cdot (c - di) = \phi(a + bi) \cdot \phi(c + di)\end{aligned}$$

3. Preservación del elemento identidad:

$$\phi(1) = 1$$

Este automorfismo, la conjugación compleja, muestra una simetría fundamental en la estructura de $\mathbb{C}$. La conjugación compleja no solo preserva las operaciones algebraicas en $\mathbb{C}$, sino que también refleja una simetría geométrica: cada número complejo y su conjugado son reflejados a través del eje real en el plano complejo. En otras palabras, para cualquier número complejo $z = a + bi$, su conjugado $\bar{z} = a - bi$ es el reflejo de z respecto al eje real.

Además, es importante notar que la conjugación compleja fija los números reales. Esto significa que para cualquier número real r , se cumple que $\phi(r) = r$. Así, los números reales permanecen inalterados bajo la conjugación compleja, subrayando la simetría inherente entre los números reales y complejos dentro de $\mathbb{C}$.

Ejemplo 4.3.5 (Topología de Zariski). Cuerpo de los Números Complejos $\mathbb{C}$) y Variedades Algebraicas: En el contexto del cuerpo $\mathbb{C}$, considere la variedad algebraica definida por el polinomio $f(x, y) = x^2 + y^2 - 1$, que describe un círculo en el plano complejo. En la topología de Zariski, los conjuntos cerrados son los conjuntos de ceros de conjuntos de polinomios. En este caso, el conjunto $\{(x, y) \in \mathbb{C}^2 \mid x^2 + y^2 - 1 = 0\}$ es un conjunto cerrado en la topología de Zariski.

Considere el cuerpo de los números complejos $\mathbb{C}$. En este contexto, una variedad algebraica se puede definir como el conjunto de puntos en $\mathbb{C}^n$ que son soluciones comunes a un conjunto de polinomios. Por ejemplo, considere el polinomio $f(x, y) = x^2 + y^2 - 1$. Este polinomio describe un círculo en el plano complejo, ya que los puntos $(x, y) \in \mathbb{C}^2$ que satisfacen $x^2 + y^2 = 1$ están sobre un círculo cuando x y y son números reales. Sin embargo, en el contexto de $\mathbb{C}^2$, estos puntos pueden tener coordenadas complejas.

En la topología de Zariski, los conjuntos cerrados son definidos como los conjuntos de ceros de conjuntos de polinomios. Es decir, un conjunto cerrado en la topología de Zariski en $\mathbb{C}^n$ es cualquier conjunto de la forma:

$$V(S) = \{(x_1, x_2, \dots, x_n) \in \mathbb{C}^n \mid \forall f \in S, f(x_1, x_2, \dots, x_n) = 0\}$$

donde S es un conjunto de polinomios en $\mathbb{C}[x_1, x_2, \dots, x_n]$. En nuestro ejemplo, el conjunto de ceros del polinomio $f(x, y) = x^2 + y^2 - 1$ es:

$$V(f) = \{(x, y) \in \mathbb{C}^2 \mid x^2 + y^2 - 1 = 0\}$$

Este conjunto $V(f)$ es cerrado en la topología de Zariski en $\mathbb{C}^2$. Geométricamente, esto representa un círculo en el plano complejo, pero en términos algebraicos, está considerando todos los pares (x, y) que satisfacen la ecuación $x^2 + y^2 = 1$.

Es importante destacar que en la topología de Zariski, los conjuntos cerrados pueden ser mucho más grandes y tener una estructura diferente a la intuición geométrica euclidiana. Por ejemplo, cualquier conjunto finito de puntos en $\mathbb{C}^n$ es cerrado en la topología de Zariski, lo cual no es necesariamente el caso en la topología euclidiana.

Además, en la topología de Zariski, el complemento de un conjunto cerrado no necesariamente es un conjunto abierto en el sentido usual. Más bien, los conjuntos abiertos en la topología de Zariski son aquellos cuyo complemento es un conjunto de ceros de algún conjunto de polinomios. Esto significa que los conjuntos abiertos pueden ser muy grandes y no necesariamente conexos.

4.4. Eficacia entre las extensiones inseparables y los cuerpos infinitos

Comparar la eficacia entre extensiones inseparables y cuerpos infinitos es un tema interesante y complejo en la teoría de cuerpos y extensiones de campos.

Definición 4.4.1 Una extensión de cuerpos K/F se dice inseparable si existe un elemento en K que no es una raíz simple de su polinomio mínimo en F . En otras palabras, el polinomio mínimo tiene raíces múltiples. Las extensiones inseparables son características de cuerpos con característica positiva p , y no existen en característica cero. Algunas propiedades y consideraciones sobre extensiones inseparables incluyen:

1. Característica del Cuerpo Base: Las extensiones inseparables ocurren únicamente en cuerpos cuya característica es un número primo p .

2. Polinomios Mínimos: En una extensión inseparables, los polinomios mínimos de algunos elementos tienen raíces repetidas. Esto significa que la derivada del polinomio se anula.
3. Aplicaciones y Limitaciones: Las extensiones inseparables son menos comunes y presentan ciertas dificultades en teoría de cuerpos y geometría algebraica debido a la falta de separación de las raíces.

Definición 4.4.2 Un cuerpo infinito es un cuerpo que contiene un número infinito de elementos. Los cuerpos infinitos pueden tener varias propiedades importantes y se pueden clasificar en diferentes tipos, tales como cuerpos de números algebraicos, cuerpos funcionales, etc. Algunas características de los cuerpos infinitos incluyen:

1. Diversidad y Complejidad: Los cuerpos infinitos pueden tener estructuras mucho más complejas que los cuerpos finitos, permitiendo un análisis más rico en términos de teoría de Galois, teoría de números, y geometría algebraica.
2. Teoría de Galois: La teoría de Galois de cuerpos infinitos puede proporcionar un marco para entender las simetrías de las raíces de polinomios y las extensiones de cuerpos de manera más general.
3. Aplicaciones Amplias: Los cuerpos infinitos tienen aplicaciones en áreas diversas como la teoría de números, geometría algebraica, criptografía y teoría de códigos.

La eficacia de estudiar extensiones inseparables versus cuerpos infinitos depende en gran medida del contexto, considerando:

1. Complejidad Algebraica: Las extensiones inseparables, debido a su naturaleza en características positivas y la presencia de polinomios con raíces múltiples, pueden ser más complicadas de manejar algebraicamente en comparación con extensiones separables. Sin embargo, pueden ofrecer una visión única en contextos donde la inseparabilidad juega un rol crucial.
2. Aplicaciones y Generalidad: Los cuerpos infinitos, por su vasta cantidad de elementos y la riqueza de su estructura, ofrecen una mayor flexibilidad y aplicaciones más amplias en matemáticas y ciencias aplicadas. Los cuerpos infinitos

permiten estudiar problemas de mayor complejidad y profundidad, como las soluciones de ecuaciones algebraicas en geometría algebraica y teoría de números.

3. Herramientas Matemáticas: Las herramientas y técnicas matemáticas desarrolladas para el estudio de cuerpos infinitos, como la teoría de Galois, la cohomología de cuerpos y la teoría de módulos, proporcionan un marco más amplio y poderoso para el análisis matemático, en comparación con las técnicas específicas para manejar extensiones inseparables.

Ejemplo 4.4.1 Considera un cuerpo F con característica $p > 0$ y una extensión inseparable K/F . Por otro lado, considera el cuerpo de funciones racionales $\mathbb{C}(x)$, un cuerpo infinito. Compara la eficacia de estudiar estas estructuras en el contexto de teoría de números.

En el caso de la extensión inseparable K/F , los polinomios mínimos de ciertos elementos en K tienen raíces múltiples, lo que complica la factorización y el análisis de propiedades aritméticas. Estas extensiones son características de cuerpos con característica positiva y son esenciales en la teoría de módulos y cohomología, aunque su manejo en teoría de números puede ser particularmente complicado debido a la inseparabilidad. Por otro lado, el cuerpo de funciones racionales $\mathbb{C}(x)$, un cuerpo infinito, permite un análisis más amplio y flexible gracias a su estructura rica. La teoría de Galois aplicada a cuerpos infinitos proporciona herramientas poderosas para entender las simetrías y extensiones de cuerpos, facilitando el estudio de curvas algebraicas y sus funciones. En resumen, en el contexto de la teoría de números, los cuerpos infinitos como $\mathbb{C}(x)$ resultan más eficaces para un análisis detallado y generalizado, mientras que las extensiones inseparables son útiles en contextos específicos donde la inseparabilidad es relevante.

Ejemplo 4.4.2 Compara la eficacia de usar extensiones inseparables K/F y cuerpos infinitos en el estudio de variedades algebraicas.

En geometría algebraica, las extensiones inseparables K/F en características positivas pueden complicar el estudio de variedades algebraicas debido a la falta de

separación de las raíces. Sin embargo, estas extensiones son esenciales para entender fenómenos como la inseparabilidad de morfismos y la estructura de esquemas. Por otro lado, los cuerpos infinitos permiten un análisis más detallado y generalizado de variedades algebraicas, facilitando la aplicación de la teoría de Galois y la cohomología, que son herramientas clave en este campo. La estructura rica de los cuerpos infinitos facilita la clasificación y el análisis de variedades complejas. En comparación, las extensiones inseparables son más complicadas de manejar debido a la inseparabilidad, mientras que los cuerpos infinitos permiten un análisis más amplio y detallado, ofreciendo más herramientas y técnicas disponibles.

Ejemplo 4.4.3 Compara la eficacia de usar extensiones inseparables K/F y cuerpos infinitos en aplicaciones criptográficas.

En criptografía, las extensiones inseparables K/F son menos comunes debido a la complejidad adicional de manejar polinomios con raíces múltiples. No obstante, pueden ofrecer seguridad adicional en ciertos esquemas criptográficos donde la inseparabilidad introduce una dificultad extra para el atacante. Por otro lado, los cuerpos infinitos, como los cuerpos de funciones, son fundamentales en criptografía para el diseño de curvas elípticas y otras estructuras algebraicas utilizadas en algoritmos criptográficos. La teoría de cuerpos infinitos proporciona una base sólida para construir y analizar esquemas criptográficos robustos y eficientes. En comparación, las extensiones inseparables son más complicadas de manejar, mientras que los cuerpos infinitos ofrecen una estructura más manejable y aplicable en criptografía, siendo más eficaces y ampliamente utilizados debido a su robustez y flexibilidad.

CAPÍTULO V CONCLUSIONES

5.1. Introducción

En este capítulo se presentan los resultados pertinentes sobre el logro de los objetivos planteados al inicio de la investigación, enfocándose específicamente en el análisis de las propiedades fundamentales de las extensiones inseparables y los cuerpos infinitos. Cada objetivo ha sido abordado de manera rigurosa para establecer un entendimiento claro y comparativo de estos conceptos clave en la teoría de cuerpos.

5.2. Conclusiones finales

Luego de examinar los resultados más significativos, se exponen las siguientes conclusiones pertinentes del estudio.

En este estudio se concluyó que las extensiones inseparables son fundamentales en la teoría de cuerpos de característica positiva, al demostrar que una extensión es inseparable si existe un elemento cuyo polinomio mínimo no es separable. Se confirmó que estas extensiones ocurren exclusivamente en cuerpos de característica positiva, y se detallaron los polinomios inseparables, caracterizados por tener raíces múltiples y derivadas con factores comunes. Además, se introdujo el exponente de inseparabilidad y se explicó la descomposición única de extensiones finitas en partes separables y puramente inseparables. Finalmente, se abordó cómo el teorema de Galois se modifica en característica positiva, mostrando que el grupo de Galois solo describe la parte separable de la extensión.

Los resultados de este estudio revelaron que las propiedades fundamentales de los cuerpos infinitos son cruciales en la teoría de cuerpos y otras ramas de las matemáticas. Se determinó que un cuerpo infinito puede ser visto como una extensión puramente trascendental de un cuerpo perfecto, y que estos cuerpos presentan diversas cardinalidades y subcuerpos infinitos con propiedades únicas. Además, se destacó

la riqueza de los grupos de automorfismos y las simetrías en cuerpos infinitos, como se ejemplificó con la conjugación compleja en los números complejos. Por último, se exploró la topología de Zariski, mostrando su complejidad y diferencia respecto a la topología euclidiana. Estos hallazgos no solo cumplieron con los objetivos planteados, sino que también proporcionaron una base sólida para futuras investigaciones en teoría de cuerpos y sus aplicaciones matemáticas.

La investigación comparó la eficacia entre las extensiones inseparables y los cuerpos infinitos en la teoría de cuerpos y extensiones de campos. Las extensiones inseparables, características de cuerpos con característica positiva, presentan dificultades debido a la falta de separación de las raíces en sus polinomios mínimos, lo que complica su manejo algebraico y limita sus aplicaciones en ciertos contextos. En contraste, los cuerpos infinitos, definidos por contener un número infinito de elementos, permiten estructuras más complejas y aplicaciones más amplias, destacándose por su diversidad y la riqueza de su análisis en teoría de Galois, teoría de números y geometría algebraica.

Se concluyó que, aunque las extensiones inseparables son fundamentales en ciertos contextos específicos, su manejo es más complicado debido a la inseparabilidad. Por otro lado, los cuerpos infinitos, con su vasta cantidad de elementos y estructuras ricas, resultaron más eficaces y aplicables en un amplio rango de contextos matemáticos y prácticos. Ofrecen una estructura manejable y herramientas matemáticas robustas, siendo especialmente útiles en el estudio de problemas complejos y en aplicaciones prácticas como la teoría de números, geometría algebraica y criptografía.

5.3. Línea futuras de investigación

Luego de realizar esta investigación, es relevante destacar las siguientes líneas futuras que podrían resultar de interés.

1. Análisis de la Teoría de Galois en Característica Positiva:

$$\text{Gal}(L/K)$$

2. Caracterización de las Extensiones de Artin-Schreier:

$$x^p - x - a = 0$$

3. Aplicaciones de las Extensiones Inseparables:

$$\alpha^{p^{p^n}} \in K$$

4. Análisis sobre la Topología de Zariski en Cuerpos Infinitos:

$$V(f) \subset K[x_1, x_2, \dots, x_n]$$

5. Exploración de la Cohomología de Cuerpos Infinitos:

$$H^n(\text{Gal}(L/K), L^*)$$

Referencias

- Abarca, A., Alpízar, F., Sibaja, G. y Rojas, C. (2013). Técnicas cualitativas de investigación. San José, Costa Rica: UCR.
- Armendia, F. G. H. (2023). Campos Ciclotómicos: Un breve análisis estructural elemental. Journal de Objetos y Objetivos Matemáticos Número 8. Enero-Junio de 2023, 5, 10.
- Artin, E. (1928). Galois Theory. Notre Dame Mathematical Lectures.
- Carl B. Allendoerfer, Cletus O. Oakley. Introducción moderna a la Matemática Superior. Ediciones del Castillo, Madrid, 1967.
- Carrasco, M. P. C. (1986). Complejos hipercruzados: cohomología y extensiones (Doctoral dissertation, Universidad de Granada).
- Castellanos J. (2017). Universidad Complutense de Madrid. Departamento de Álgebra. I Estructuras Algebraicas.
- Dedekind, R., y Weber, H. (1882). Theorie der algebraischen Funktionen einer Veränderlichen. Journal für die reine und angewandte Mathematik.
- Fasano, M. V. (2003). Cuerpos: Separabilidad y extensiones cíclicas.
- Fasano, M. V. (2005). Separabilidad
- Fraleigh, J. B. A First Course in Abstract Algebra. Seventh ed. Pearson, Upper. Saddle River, NJ, 2003
- García, F., Martínez, A., & Rodríguez, P. Año: 2021 Título: Galois Theory for Inseparable Extensions in Infinite Fields.

- Carrasco, M. P. C. (1986). Complejos hipercruzados: cohomología y extensiones (Doctoral dissertation, Universidad de Granada).
- Galois, É. (1832). "Sur la théorie des nombres et la résolution algébrique des équations". Journal de Mathématiques Pures et Appliquées.
- Gómez, D. (2015). Cuerpos Finitos. Trabajo de Grado. Universidad de Murcia.
- Grothendieck, A. (1960). Éléments de géométrie algébrique. Publications Mathématiques de l'IHÉS.
- Hernández Sampieri, R, Fernández, C & Baptista, P. (2010). Metodología de la Investigación. (Quinta Edición). México D.F, México: McGraw-Hill.
- Ivorra, C. C. (2010). Algebra. K-groups of reciprocity functions for and abelian varieties.
- Ivorra, C.C. 2010. TEORÍA DE CUERPOS DE CLASES.
- Lang, S. Algebra, revised third ed., Springer-Verlag, New York, 2002.
- López, E., González, R., y Pérez, C. Año: 2020 Título: Constructing Inseparable Extensions over Infinite Fields.
- Martínez, L., Rodríguez, A., y García, M. Año: 2019 Título: Inseparable Extensions in Infinite Fields: Algebraic Structures and Properties.
- Olalla, M. (2015). Grupo, anillos y cuerpos. Departamento de Álgebra, Universidad de Sevilla.
- Palacios, M. (2002). Grupos, anillos y cuerpos. Departamento de Matemática Aplicada.

Pérez, D., Martínez, G., y González, E. Año: 2023 Título: Inseparable Extensions and Algebraic Geometry over Infinite Fields.

Rodríguez, N., García, L., & Martínez, J. Año: 2022 Título: Applications of Inseparable Extensions in Cryptography.

Sampieri y otros (2010). Metodología de la investigación. Editora Mc Graw Hill. México.

Sánchez, A., Martínez, E., & López, M. Año: 2023 Título: Computational Aspects of Inseparable Extensions in Infinite Fields.

Sabaté, F. M. (2005). El Teorema Fundamental del Algebra. Universidad de Barcelona, España, 1-11.

Salgado, D. R., Fierro, J. O. O., y Lozoya, C. V. V. (2024). Características del Método Delphi Difuso como Extensión del Enfoque Delphi. Excelencia Administrativa Online, 3(6).

Stonek, B. 2012. Teoría de grupos. Teoría de cuerpos y teoría de Galois. Representaciones de grupos finitos.

Witt, E. (1936). Theorie der quadratischen Formen in beliebigen Körpern. Journal für die reine und angewandte Mathematik.

Anexos

Anexo A. Simbología matemática

A continuación se presenta una lista detallada de la simbología matemática utilizada. Esta lista incluye símbolos y notaciones que son fundamentales para la comprensión de conceptos avanzados en álgebra abstracta y teoría de cuerpos. La simbología abarca desde notaciones básicas de operaciones algebraicas hasta definiciones específicas de estructuras y propiedades de extensiones de cuerpos. Cada símbolo es crucial para entender las definiciones, teoremas y ejemplos que se desarrollan a lo largo del marco teórico, proporcionando una base sólida para el estudio y análisis de las propiedades algebraicas presentadas.

1. K : Un cuerpo.
2. F : Un subcuerpo de K .
3. $+$: Operación de adición.
4. $\text{Gal}(E/K)$: Grupo de Galois de la extensión E sobre K .
5. $f \in K[X_1, \dots, X_n]$: Polinomio f en las variables $X_1, \dots, X_n$ con coeficientes en K .
6. $\Phi_n(x)$: Polinomio ciclotómico de grado n .
7. ζ : Raíz primitiva n -ésima de la unidad.
8. $\text{mcd}(k, n)$: Máximo común divisor de k y n .
9. $[E : F]$: Grado de la extensión E sobre F .
10. $\dim_F(E)$: Dimensión de E como espacio vectorial sobre F .
11. $\text{Gal}(E/K) = \{\phi_1, \dots, \phi_n\}$: Conjunto de automorfismos del grupo de Galois de la extensión E sobre K .
12. $f(\phi_1(a), \dots, \phi_n(a)) = 0$: Ecuación que verifica el polinomio f en el grupo de Galois.

13. $f = 0$: Polinomio idénticamente nulo.
14. $p(x) \in k[x]$: Polinomio p en la variable x con coeficientes en k .
15. $p(x) = f(x) \cdot g(x)$: Factorización del polinomio $p(x)$ como producto de $f(x)$ y $g(x)$.
16. $K \subseteq F$: Notación de extensión de cuerpos donde K es un subcuerpo de F .
17. E/K : Notación de extensión de cuerpos E sobre K .
18. $E[x]$: Anillo de polinomios en la variable x con coeficientes en E .
19. $[E : F] = [E : K] \cdot [K : F]$: Relación transitiva del grado de la extensión.
20. $p > 0$: Característica positiva de un cuerpo.
21. $(\text{ap})^n$: Forma de un elemento puramente inseparable.
22. $f(\alpha) = 0$: Ecuación que indica que α es raíz del polinomio f .

Anexo B. Lista de fórmulas utilizadas

A continuación se presenta una lista de fórmulas matemáticas fundamentales utilizadas. Estas fórmulas abarcan diversas propiedades y relaciones algebraicas cruciales en el estudio de cuerpos y extensiones de campos. Desde la propiedad distributiva hasta la estructura de grupos de Galois y polinomios irreducibles, cada una de estas expresiones matemáticas juega un papel esencial en la comprensión y desarrollo de conceptos avanzados en álgebra abstracta.

1. Propiedad distributiva: Esta fórmula indica que la multiplicación es distributiva respecto a la adición en un cuerpo.

$$\forall a, b, c \in A : a \cdot (b + c) = a \cdot b + a \cdot c$$

2. Grupo de Galois: Representa el grupo de automorfismos de una extensión de Galois E sobre un cuerpo K .

$$\text{Gal}(E/K) = \{\phi_1, \dots, \phi_n\}$$

3. Polinomio multivariable: Denota que f es un polinomio en las variables $X_1, \dots, X_n$ con coeficientes en K .

$$f \in K[X_1, \dots, X_n]$$

4. Condición de anulación: Indica que el polinomio f se anula para todas las imágenes de a bajo los automorfismos del grupo de Galois.

$$f(\phi_1(a), \dots, \phi_n(a)) = 0 \text{ para cada } a \in E$$

5. Factorización de polinomio: Representa la factorización de un polinomio $p(x)$ como producto de dos polinomios no constantes $f(x)$ y $g(x)$.

$$p(x) = f(x) \cdot g(x)$$

6. Polinomio ciclotómico: Define el polinomio ciclotómico $\Phi_n(x)$, que se obtiene al tomar el producto de $(x - \zeta^k)$ para los k coprimos con n .

$$\Phi_n(x) = \prod_{\text{mcd}(k,n)=1, 1 \leq k \leq n} (x - \zeta^k)$$

7. Grado de extensión: Representa el grado de la extensión E sobre F , que es la dimensión de E como espacio vectorial sobre F .

$$[E : F] = \dim_F(E)$$

8. Propiedad transitiva del grado de extensión: Indica que el grado de la extensión E sobre F es el producto de los grados de las extensiones intermedias.

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

9. Elemento puramente inseparable: Significa que un elemento a es puramente inseparable sobre k si existe un entero n tal que $(a^p)^n$ está en k .

$$(a^p)^n \in k$$

10. Raíz de un polinomio: Indica que α es una raíz del polinomio f en F .

$$f(\alpha) = 0$$

11. Radical sobre un cuerpo: Indica que un elemento x es radical sobre el cuerpo K si $(x^p)^r$ pertenece a K .

$$(x^p)^r \in K$$

Anexo C. Cronograma de estudios

A continuación, se detalla el cronograma de estudios que guió las diferentes etapas del proyecto. Este cronograma especifica las fechas clave para la entrega y evaluación del anteproyecto, la incorporación de observaciones por parte de los jurados, la elaboración del proyecto completo, la presentación de exámenes de tesis, y la entrega final del proyecto. Cada etapa tiene asignadas fechas específicas para asegurar un flujo de trabajo organizado y eficiente, facilitando así el cumplimiento de los objetivos establecidos para el desarrollo del proyecto.

- Entrega del anteproyecto: 28 al 30 de Junio
- Evaluación del Anteproyecto: 1 al 3 de Julio
- Observaciones de jurados: 4 al 9 de Julio
- Elaboración del proyecto completo: 15 al 20 de Agosto
- Presentaciones de exámenes de tesis: 2 al 3 de septiembre
- Entrega final: 25 al 30 de septiembre