ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

FACULTAD DE CIENCIAS

CARRERA MATEMÁTICA

LA TEORÍA DE CAMPOS APLICADA EN LOS TRES PROBLEMAS GEOMÉTRICOS

Trabajo de Integración Curricular

Tipo: Proyecto de Investigación

Presentado para optar al grado académico de:

MATEMÁTICO

AUTOR: WILMER ANDRES CAGUAS CHAFLA

DIRECTOR: Dr. LEONIDAS ANTONIO CERDA ROMERO, PhD.

Riobamba – Ecuador

2023

Yo, Wilmer Andres Caguas Chafla, declaro que el presente trabajo de titulación 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, 24 de noviembre de 2023

Wilmer Andres Caguas Chafla

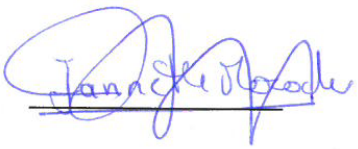
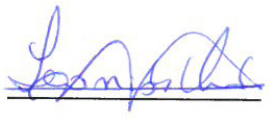
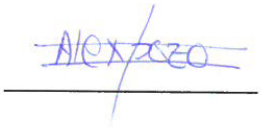
060488742-2

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. **LA TEORÍA DE CAMPOS APLICADA EN LOS TRES PROBLEMAS GEOMÉTRICOS**, realizado por el señor: **WILMER ANDRES CAGUAS CHAFLA**, 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. Janneth del Rocio Morocho **PRESIDENTE DEL TRIBUNAL**		24-11-2023
Dr. Leonidas Antonio Cerda **DIRECTOR DEL TRABAJO DE INTEGRACIÓN CURRICULAR**		24-11-2023
Mgs. Alex Eduardo Pozo **ASESOR DEL TRABAJO DE INTEGRACIÓN CURRICULAR**		24-11-2023

DEDICATORIA

Con profundo cariño y gratitud, dedico esta tesis a mis padres Rosendo y Lourdes, cuyo amor, apoyo y sacrificio han sido el motor impulsor detrás de cada paso que he dado en mi camino académico. A mis queridos hermanos, quienes han sido mi apoyo incondicional. También a Nayely y Jheremy, su compañía y aliento han sido la fuerza que me ha permitido superar los obstáculos y alcanzar mis metas.

Wilmer

AGRADECIMIENTO

Primeramente quiero expresar mi profunda gratitud al Dios eterno por su amor divino y las bendiciones que ha derramado sobre mí y mi familia.

A mis queridos padres, no encuentro palabras suficientes para expresar mi agradecimiento por todo el amor y apoyo que me han brindado. Su dedicación y sacrificio han sido la base para lograr esta meta. Los llevo siempre en mi corazón.

A mis queridos hermanos, quiero expresar mi sincero agradecimiento por el apoyo incondicional que me han brindado a lo largo de este camino. Su respaldo ha sido mi fuente de fortaleza y motivación. Gracias por estar siempre a mi lado.

A Nayely y Jheremy, este trabajo no sería posible sin su amor y apoyo.

A mi tutor, agradezco sinceramente su guía y apoyo durante el desarrollo de esta tesis. Su dedicación y conocimientos compartidos han sido un regalo inestimable para mi crecimiento académico.

A mis grandes amigos, agradezco profundamente el inquebrantable apoyo, las risas compartidas y las horas de estudio juntos.

Wilmer

ÍNDICE DE CONTENIDOS

RESUMEN

En la Escuela Superior Politécnica de Chimborazo no hay evidencia de la existencia de material bibliográfico sobre la teoría de campos aplicada a la demostración de la insolubilidad de problemas geométricos, lo cual dificulta que estudiantes interesados en entender y expandir sus conocimientos matemáticos, puedan iniciar sus investigaciones. Por lo tanto, el objetivo del presente trabajo de investigación fue analizar la teoría de campos, a través de la revisión bibliográfica especializada, con el fin de redactar un documento sobre la insolubilidad de problemas geométricos. Para ello se consideró una investigación de tipo documental, con enfoque cualitativo y nivel descriptivo, para la redacción de la misma se utilizó el editor de texto Latex. Como resultado final se obtuvo una monografía titulada: La teoría de campos aplicada a los tres problemas geométricos, la cual consta de cuatro capítulos. El primero aborda los tópicos de anillos y campos. En el segundo capítulo, se exploran los anillos de polinomios. El tercer capítulo se enfoca en las extensiones de campos y, finalmente, el cuarto capítulo abarca la demostración de la insolubilidad de los tres problemas geométricos. Así podemos concluir que mediante el análisis de la teoría de campos, se logró demostrar la insolubilidad de los tres problemas geométricos clásicos de la antigua Grecia.

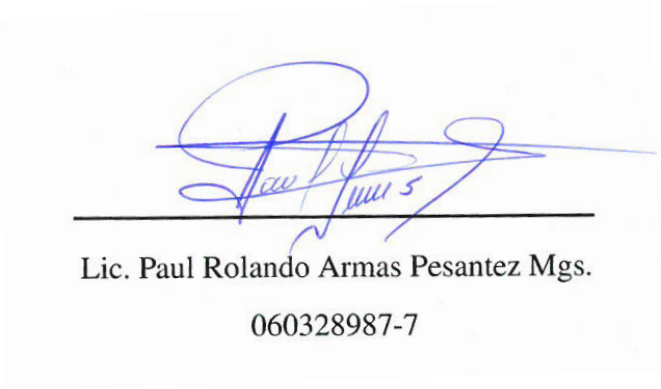
Palabras clave: <ANILLOS>, <CAMPOS>, <EXTENSIÓN DE CAMPOS>, <PROBLEMAS GEOMÉTRICOS>, <INSOLUBILIDAD>.

2059-DBRA-UPT-2023

ABSTRACT

The Escuela Superior Politécnica de Chimborazo does not register any evidence on of the existence of bibliographic material on the field theory which is applied to the demonstration of insoluble geometric problems, which makes it difficult for students interested in understanding and expanding their mathematical knowledge to initiate their research. Therefore, the aim of the current research work was to analyze the field theory, through a specialized bibliographic review, in order to write a paper on the insolubility of geometric problems. For this purpose, documentary-type research with a qualitative approach and descriptive level was considered, as well as Latex text editor for its writing. The final result was a monograph entitled: Field theory applied to the three geometric problems, which consists of four chapters. The first chapter has to do with the rings and fields topics. The second chapter explores polynomial rings. The third chapter focuses on field extensions and finally, the fourth chapter covers the proof of the insolubility of the three geometric problems. Thus, it is concluded that by means of the analysis of the field theory, it was possible to demonstrate the insolubility of the three classical geometric problems of the ancient Greece.

Keywords: <RINGS>, <FIELDS>, <FIELD EXTENSIONS>, <GEOMETRIC PROBLEMS>, <INSOLUBILITY>.



INTRODUCCIÓN

La geometría ha sido una disciplina fundamental en las matemáticas desde tiempos antiguos, y a lo largo de la historia, se han planteado diversos problemas geométricos clásicos que han desafiado a los matemáticos.

En la matemática es frecuente que, al buscar la solución de un problema, los métodos y técnicas utilizadas contribuyen al desarrollo de la matemática. Los tres problemas geométricos planteados por los matemáticos de la antigua Grecia son un buen ejemplo de este tipo de avance matemático. Los tres problemas geométricos planteados por los griegos de la antigüedad son:

1. Construir un cubo con el doble de volumen al de uno dado, este problema se conoce con el nombre de duplicación del cubo.

2. Dividir un ángulo en tres partes iguales, problema conocido con el nombre de trisección del ángulo.

3. Construir un cuadrado que tenga la misma área al de un círculo dado, este problema se conoce con el nombre de cuadratura del círculo.

Es importante notar que, las construcciones que se pueden hacer para la resolución de estos problemas son realizados únicamente con regla no graduada y compás.

Por el año de 1832, la teoría de campos, teoría cuyo desarrollado fue motivado por el afán de resolver los problemas antes mencionados, mostró que estos tres problemas son insolubles.

Uno de los objetivos fundamentales de este documento es proporcionar a los estudiantes de la carrera de matemática de la Escuela Superior Politécnica de Chimborazo (ESPOCH) una fuente bibliográfica de estudio completa y accesible sobre la aplicación de la teoría de campos en los tres problemas geométricos clásicos. En la ESPOCH, existe una falta de recursos bibliográficos específicos que aborden la teoría de campos y su aplicación en la resolución de estos problemas, lo cual puede dificultar el estudio y la comprensión de estos temas por parte de los estudiantes que cursan los cursos de Álgebra Abstracta.

Uno de los mayores desafíos en la enseñanza de un curso de álgebra abstracta es que muchos estudiantes se enfrentan por primera vez a un entorno que les exige realizar demostraciones rigurosas. Estos estudiantes a menudo encuentran difícil visualizar la utilidad del aprendizaje de la demostración de teoremas y proposiciones (Judson, 2012, p. 3).

Por lo tanto, esta investigación busca abordar esta brecha, proporcionando a los estudiantes de la ESPOCH una fuente bibliográfica que les permita comprender la teoría de campos y la

resolución de la insolubilidad de los tres problemas geométricos clásicos. Al proporcionar un recurso completo y accesible, se espera facilitar el estudio y la comprensión de estos conceptos, ayudando a los estudiantes a superar los desafíos que puedan enfrentar al estudiar Álgebra Abstracta y al introducirse en la demostración rigurosa de teoremas.

CAPÍTULO I

1. PROBLEMA DE INVESTIGACIÓN

1.1. Planteamiento del problema

Muchos problemas planteados por civilizaciones antiguas tuvieron que esperar a que la matemática esté lo suficientemente desarrollada para ser resueltos, este es el caso de los tres problemas geométricos planteados por los griegos, que tuvieron que esperar que apareciera la teoría de campos para ser resueltos. En la ESPOCH no hay evidencia de la existencia de material bibliográfico sobre la teoría de campos aplicada a la demostración de la insolubilidad de problemas geométricos, lo cual dificulta que estudiantes interesados en entender y expandir sus conocimientos matemáticos, puedan iniciar sus investigaciones.

1.2. Objetivos

Objetivo general

Analizar la teoría de campos, a través de la revisión bibliográfica especializada, con el fin de redactar un documento sobre la insolubilidad de problemas geométricos.

Objetivos específicos

- Realizar una recopilación bibliográfica mediante técnicas eficaces de búsqueda sobre la teoría de campos para la comprensión de esta teoría.
- Estudiar la aplicación de la teoría de Campos, a través de definiciones y la demostración de teoremas, para determinar la insolubilidad de los tres problemas geométricos clásicos.
- Redactar un documento sobre la insolubilidad de los tres problemas geométricos, mediante la utilización del editor de texto LaTeX, para que los estudiantes de la carrera de matemática de la ESPOCH cuenten con una fuente bibliográfica de estudio.

1.3. Justificación

El desarrollo de los contenidos de este trabajo elevará la formación académica de los futuros matemáticos de la ESPOCH, y ayudará a graduados de la carrera de matemática que estén interesados en continuar estudios de posgrado en este tema.

Por un lado, con la finalidad de complementar los conocimientos recibidos en los cursos de álgebra

abstracta (teoría de grupos, teoría de anillos, y una introducción muy somera a la teoría de campos) impartidos en la carrera de matemática de la ESPOCH, se pretende escribir una monografía que sea comprensible para todos los compañeros de la carrera de matemática que han cursado los dos niveles de Álgebra Abstracta, y personas interesadas en el tema. Por otro lado, se pretende ilustrar la aplicación de la teoría de campos en la demostración de la insolubilidad de los tres problemas geométricos planteados por los griegos.

También, conocer las definiciones y comprender los teoremas de la teoría de campos mejora la comprensión del papel que juega esta teoría en la demostración de la insolubilidad de algunos problemas geométricos; en particular, la insolubilidad de los tres problemas geométricos planteados por los griegos. Así mismo, este trabajo será una valiosa fuente bibliográfica para estudiantes de matemática interesados en la relación entre la teoría de campos y la insolubilidad de construcciones con regla y compás.

CAPÍTULO II

2. MARCO TEÓRICO

2.1. Referencias teóricas

Cuando hablamos de construcciones geométricas nos referimos especialmente al método de los griegos antiguos; es decir, al uso de los únicos dos elementos permitidos: regla no graduada y el compás.

En (Chamizo, 2005, p. 34), Chamizo enuncia a los tres problemas geométricos de la siguiente manera:

1. Dada la arista de un cubo, construir con regla y compás la arista de un cubo de doble volumen.

2. Dado un ángulo, encontrar un método para trisecarlo con regla y compás

3. Dado un círculo, construir con regla y compás un cuadrado que de igual área.

El problema de cuadrar el círculo fue propuesto por Anaxagoras en el año 500 a.C. (Morales, 2002) menciona que en el año 450 a.C., Anaxagoras fue encarcelado por afirmar que el sol no era un Dios, y mientras estuvo en prisión intento resolver el problema antes mencionado. En 1882, el matemático alemán Ferdinand Lindemann demostró que π no es un número racional, lo cual implica la imposibilidad de cuadrar el círculo (ver el anexo de este trabajo).

El problema de la duplicación de un cubo se presentó en Atenas. En (Rodríguez, 1953), Rodríguez A. cuenta que en el año 429 a.C. falleció Pericles, tirano de Atenas, y la ciudad cayó en una profunda crisis; los atenienses se dirigieron al Oráculo de Delfos para preguntar a los dioses sobre la solución a los problemas que les aquejaba. Los dioses respondieron que la crisis desaparecerá si construyen un altar cúbico con el doble de volumen que el existente (dedicado a los dioses). Los atenienses lo intentaron, pero lo que es seguro es que no lograron construir este nuevo cubo, utilizando solo regla y compas.

La trisección de un ángulo es un problema que ya se plantearon los griegos 500 años a.C. Aunque muchos ángulos son trisecables (por ejemplo, los ángulos de 90°, 45°, etc. son trisecables), en 1837, el matemático francés Pierre Wantzel demostró que no es posible trisecar un ángulo arbitrario utilizando solo regla y compas.

Ayala N. en su trabajo de titulación, para optar por el título de profesor de matemática, escribe que el enunciado de los tres problemas geométricos es sencillo de entender, lo cual hace que cualquier persona alejada a las matemáticas pueda comprenderlos; sin embargo, sus demostraciones exigieron el desarrollo de nuevas ramas de la matemática. También argumenta que existen numerosas

soluciones aproximadas con regla y compas, aunque ya se demostró que estos problemas no pueden ser resueltos como pedían los griegos, y que en la actualidad siguen apareciendo trabajos erróneos donde se asegura haber encontrado una solución (Ayala, 2009).

Realizando una búsqueda bibliográfica se encontró el trabajo *"Construcciones con regla y compas"*, de Pan-Collantes, el cual presenta algunos aspectos interesantes acerca de las construcciones con regla y compas a lo largo de la historia. Este texto está dividido en tres partes: en la primera parte se menciona de forma rápida la historia de estas construcciones; en la segunda se hace una breve introducción a la teoría algebraica de campos y extensiones; y la tercera parte, utiliza el contenido de la segunda para demostrar la imposibilidad de los tres problemas clásicos griegos. El autor mensiona que: "La segunda parte del trabajo puede hacerse un poco dura de entenderla, pero al ser un artículo de carácter divulgativo, no debe de buscarse el rigor de un típico escrito de matemáticas" (Collantes, 2005, p. 8).

Analizando la bibliografía hallada, se puede evidenciar que si se demuestra la insolubilidad de los tres problemas geométricos, pero no se hace énfasis en la importancia de la teoría de campos en su solución. Por ejemplo, en (Collantes, 2005), solo se enuncia algunas definiciones y teoremas que ayudan a resolver estos problemas, pero no se realiza un tratamiento matemático adecuado, lo cual ayuda a comprender por completo la resolución de estos problemas.

CAPÍTULO III

3. MARCO METODOLÓGICO

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

Este trabajo de investigación se estructuró con una metodología de enfoque cualitativo, debido a que se interpretó de manera subjetiva los contenidos de la bibliografía seleccionada para describir la insolubilidad de los tres problemas geométricos planteados por los antiguos griegos.

Esta investigación corresponde a un alcance descriptivo, ya que el interés fue generar una monografía, en la cual se describa de manera detallada la teoría de campos y su utilidad en la demostración de los tres problemas geométicos.

La investigación es de tipo documental, con uso de fuentes secundarias, debido a que se basó en la recolección de documentos digitales (libros, revistas, tesis, monografías) especializados en la teoría de campos.

Para la redacción de la monografía se siguieron lineamientos como:

- Búsqueda de material bibliográfico: Se llevó a cabo una exhaustiva búsqueda de fuentes confiables, como libros en línea, tesis y monografías, que abordaran el tema de investigación establecido, centrándose en el estudio de la teoría de Campos.

- Selección y organización del material recolectado: Tras realizar una lectura selectiva de las fuentes recopiladas, se identificaron y destacaron aquellos documentos que resultaban relevantes para el desarrollo y comprensión de los temas que se tratarían en la monografía.

- Pre-escritura de la monografía: Aquí, una vez comprendidos las definiciones y teoremas, se elaboró un borrador a mano en el que se abordó de manera más detallada cada definición, lema, teorema y ejemplos.

- Redacción de la monografía: Se procedió a la redacción propiamente dicha del documento. Durante esta fase, se plasmaron las ideas de manera coherente y se estructuraron los contenidos de forma lógica. Se puso especial énfasis en utilizar un lenguaje claro y accesible, proporcionando explicaciones detalladas cuando fue necesario.

- Finalmente, se llevó a cabo una revisión exhaustiva del documento. Esta etapa permitió verificar la precisión y la coherencia de los contenidos, así como corregir posibles errores gramaticales o de estilo. También se aseguró de que las demostraciones fueran rigurosas y comprensibles, pues

la monografía está dirigida principalmente a los estudiantes de la carrera de Matemática de la ESPOCH.

Para la redacción del cocumento se se utilizó el editor de texto LaTeX, pues está diseñado para producir documentos de alta calidad; especialmente es adecuado para escribir documentos que involucren muchas fórmulas matemáticas. En este sentido, se dejará a los estudiantes de la carrera de matemática de la ESPOCH una referencia bibliográfica de alta calidad tipográfica.

CAPÍTULO IV

4. MARCO DE ANÁLISIS E INTERPRETACIÓN DE RESULTADOS

4.1. Procesamiento, análisis e interpretación de resultados

Como resultado final se obtuvo una monografía titulada: *La teoría de campos aplicada a los tres problemas geométricos*. El propósito de la monografía es facilitar al lector el entendimiento de los conceptos básicos de la teoría de campos, y su aplicación a la resolución de problemas sobre construcciones geométricas. Con este trabajo también se pretende influir en el interés sobre estos tópicos en los estudiantes de la carrera de matemática de la ESPOCH.

4.2. Discusión

La monografía consta de 4 capítulos, en cada uno de los capítulos se encuentran definiciones, teoremas, corolarios, lemas y ejemplos de cada estructura estudiada.

Capítulo 1 (Teoría de Anillos): Este capítulo abarca un primer estudio de la teoría de anillos como lo es: anillos, subanillos, ideales, anillo cociente, campos, campos finitos y homomorfismos de anillos.

Capítulo 2 (Anillos de Polinomios): Continúa con el estudio de la teoría de anillos y se abarca: la estructura algebraica de $F[x]$, el algoritmo de Euclides para polinomios, máximo común divisor y polinomios irreducibles.

Capítulo 3 (Extensiones de Campos): En este capítulo se abarcó el estudio básico relacionado con temas de la Teoría de Campos, los cuales fueron: extensiones finitas y algebraicas, raíces de polinomios, clausuras algebraicas, derivada de un polinomio y campos finitos.

Capítulo 4 (Construcciones con regla y compás): Luego de haber realizado un estudio sobre la teoría de campos, finalmente en este capítulo se abarcó el estudio de la insolubilidad de los tres problemas geométricos clásicos a través de la teoría de campos.

CAPÍTULO V

5. CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

- Mediante el análisis de la teoría de campos, a través de una revisión bibliográfica especializada, se logró comprender y redactar un documento sobre la insolubilidad de los tres problemas geométricos clásicos de la antigua Grecia
- El estudio de la aplicación de la teoría de campos en la insolubilidad de los tres problemas geométricos clásicos proporciona a los estudiantes de matemáticas una oportunidad única para expandir sus conocimientos y explorar un área específica de la matemática que no se aborda con frecuencia en los cursos regulares de pregrado.
- La monografía, resultado de este trabajo de titulación, se convertirá en una valiosa fuente bibliográfica para los estudiantes de la carrera de matemática de la ESPOCH.

RECOMENDACIONES

- Difundir la monografía resultado de este trabajo de titulación. Esto permitirá que los estudiantes de la carrera de matemática de la ESPOCH refuercen su conocimiento, y se beneficien de los resultados de este trabajo.
- Explorar las diversas aplicaciones de la teoría de campos en otros problemas matemáticos. Esto permitirá ampliar los conocimientos y enriquecer las capacidades para abordar desafíos matemáticos complejos
- Considerar la posibilidad de realizar trabajos futuros relacionados con la aplicación de la teoría de campos en otros problemas geométricos o en áreas relacionadas. Esto permitirá ampliar la investigación y explorar nuevos enfoques y aplicaciones de la teoría de campos en contextos matemáticos diferentes.

BIBLIOGRAFÍA

AYALA, N. “Construcciones geométricas con regla y compás: Pasos". Revista argentina de psicopedagogía [En línea], 2009, no 62, p. 4. [Consulta: 19 de junio del 2023]. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=3045267

CHAMIZO, F. *Que bonita es la teoría de Galois* [en línea]. 2005. Madrid. [Consulta:15 de diciembre del 2022]. Disponible en: https://matematicas.uam.es/~fernando.chamizo/libreria/fich/APalgebraII04.pdf

COLLANTES, A. P. Construcciones con regla y compás. *Acta de Mathematica Vulgata*, 2005, vol. 1, p. 29-36.[Consulta:15 de diciembre del 2022]. Disponible en: https://doi.org/10.13140/RG.2.2.24263.04005

CRESPO, L. “Los tres problemas griegos (sin solución)". Revista Tekhné [En línea], 2016, pp 71-74. [Consulta:20 de diciembre del 2022]. Disponible en: https://revistasenlinea.saber.ucab.edu.ve/index.php/tekhne/article/view/2673

DE LA FRAGA, L. Uso del Procesador de Texto LaTeX [En línea]. (2009). [Consulta: 21 de junio del 2023]. Disponible en: http://cs.cinvestav.mx/~fraga/Cursos/Cosnet2002/material/latex.pdf

FRALEIGH, J. *A first course in Abstract Algebra* [en línea]. Seventh edition. Pearson new international edition, 2014. [Consulta: 14 de junio 2023]. Disponible en: https://www.mymathscloud.com/api/download/modules/University/Textbooks/algebra-abstract/5)A%20First%20Course%20in%20Abstract%20Algebra%20Fraleigh%207th%20edition.pdf?id=25323176

GALLIAN, J. *Contemporany Abstract Algebra* [en línea]. Novena edición. USA: Cengage Learning, 2017. [Consulta: 24 de abril 2023]. Disponible en: https://books.google.com.ec/books?id=JMUaCgAAQBAJ&printsec=frontcover&dq=Contempora#v=onepage&q&f=false

HERSTEIN, I. *Álgebra Moderna* [en línea]. Eitorial F trillas, S.A. México, 1970. [Consulta:

14 de junio 2023]. Disponible en: https://www.academia.edu/14931038/Algebra_Moderna_Herstein

JUDSON, T. *Abstract Algebra Theory and Applications* [en línea]. Texas-USA: Orthogonal Publishing, 2012. [Consulta: 19 de ablir 2022]. Disponible en: http://debracollege.dspaces.org/bitstream/123456789/9/1/Thomas%20W.%20Judson.pdf

LABRA, A; SUAZO, A. *Elementos de la teorá de cuerpos* [en línea]. Chile: Jc Sáez Editor, 2011. [Consulta: 17 de abril 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

MORALES, L "La cuadratura del círculo y otros problemas de geometría'". Revista Ciencias [En línea], 2002, pp. 54-65. [Consulta: 03 de julio 2023]. Disponible en: https://www.revistacienciasunam.com/images/stories/Articles/65/CNS06509.pdf

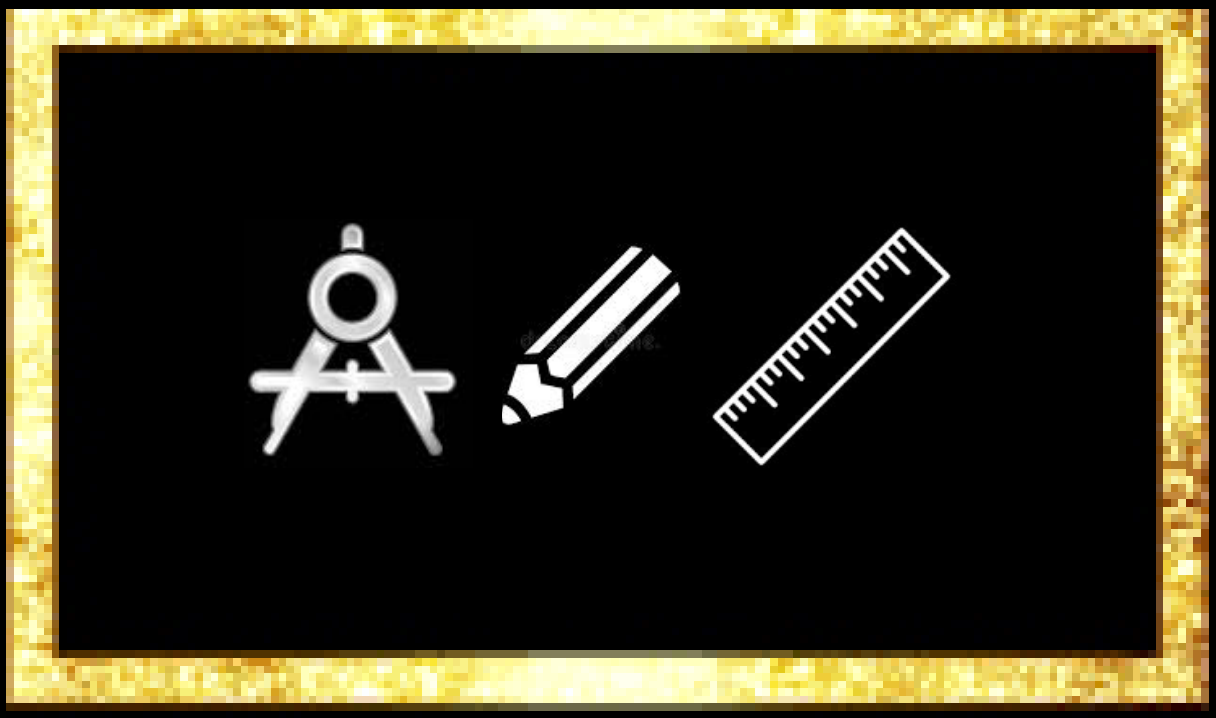
RODRÍGUEZ, A. "El problema de la duplicación del cubo". Revista Colombiana de Matemáticas [En línea], 1953, vol. 2, no 1, p. 8-12. [Consulta: 26 de junio 2023]. Disponible en: https://repositorio.unal.edu.co/bitstream/handle/unal/42908/32749-121224-1-PB.pdf?sequence=1&isAllowed=y

STEWART, I. *Galois Theory* [en línea]. Fourth Edition. CRC Press, 2015. [Consulta:18 de abril 2023]. Disponible en: https://eclass.uoa.gr/modules/document/file.php/MATH594/Stewart%20Galois%204th%20edition.pdf

ANEXO

ANEXO A: MONOGRAFÍA "LA TEORÍA DE CAMPOS APLICADA EN LOS TRES PROBLEMAS GEOMÉTRICOS".

LA TEORÍA DE CAMPOS APLICADA EN LOS TRES PROBLEMAS GEOMÉRTRICOS



WILMER CAGUAS

2023

CARRERA DE MATEMÁTICA
ESPOCH

Contenidos

Introducción

La teoría de anillos y campos es una área esencial del álgebra abstracta que se ocupa del estudio de las estructuras algebraicas como lo son: anillos y campos. Por un lado, los anillos son conjuntos con operaciones internas denotadas como suma y multiplicación, por otro lado, los campos son anillos que cuentan con otras propiedades adicionales, entre ellas la existencia del elemento inverso. Estas estructuras desempeñan un papel fundamental en diversas ramas de las matemáticas, como lo es el álgebra lineal, la teoría de números y la geometría algebraica.

En esta monografía, se analizarán las definiciones, teoremas, junto con sus demostraciones y ejemplos de la teoría de campos de manera rigurosa, para poder la insolubilidad los tres problemas geométricos de la antigua Grecia, utilizando únicamente la regla y compás.

Los tres problemas geométricos a tratar son: la cuadratura del círculo, que consiste en construir un cuadrado con la misma área que un írculo dado; la duplicación del cubo, que consiste en construir un cubo con el doble del volumen de otro cubo dado; y por último, la trisección del ángulo, que busca dividir un ángulo en tres partes iguales.

1

Teoría de Anillos

El estudio de los anillos es una parte fundamental del álgebra abstracta y nos brinda un marco poderoso para comprender estructuras algebraicas más generales. Los anillos son conjuntos dotados de dos operaciones: suma y multiplicación, que interactúan de manera interesante y permiten modelar una amplia gama de conceptos matemáticos y aplicaciones en diferentes disciplinas.

En este capítulo, examinaremos en profundidad las propiedades y características esenciales de los anillos. Comenzamos con la definición formal de lo que es un anillo y analizamos las propiedades básicas de las operaciones de suma y multiplicación.

1.1 Anillos

Definición 1.1 (Anillo)

Sea R un conjunto no vacío junto con dos operaciones binarias $(+)$ y $(\cdot)$. Se dice que $(R, +, \cdot)$ es un anillo o simplemente que R es un anillo si y sólo si:

1. $(R, +)$ es un grupo abeliano.
2. $(R, \cdot)$ es un semigrupo.
3. Para todo $a, b, c \in R$:
   a) $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$
   b) $(b + c) \cdot a = (b \cdot a) + (c \cdot a)$.

Notas. 1. Sean a, b elementos del anillo R, si $ab = ba$ entonces el anillo R se llama *anillo abeliano* o *conmutativo*.

2. Sea $a \in R$, si existe un elemento denotado por 1 en el anillo R tal que $a1 = 1a = a$ entonces el anillo se llama *unitario* o anillo con elemento unidad.

3. Sea R un anillo conmutativo, sea a un elemento no nulo del anillo R. Se dice que a es un *divisor de cero* si existe un elemento b no nulo del anillo R tal que $ab = 0$.

4. Sea R un anillo conmutativo y unitario. Si R no tiene divisores de cero, entonces R se llama *dominio íntegro*.

Definición 1.2 (Campo)
Sea R un anillo conmutativo y unitario, R se llama campo si todos sus elementos no nulos poseen un inverso multiplicativo.

Nota. Denotamos al inverso de a con a^{-1}.

Observación. Sea F un campo, a partir de su definición podemos concluir que $(F, +)$ y $(F^*, \cdot)$ son grupos abelianos. Donde $F^* = F \setminus \{0\}$.

Demostración. Puesto que F es un campo, tenemos que F es un anillo, por tanto, $(F, +)$ es un grupo abeliano.

Mostremos que $(F^*, \cdot)$ es un grupo abeliano.

Por definición tenemos que F^* es el campo F menos el $\{0\}$, con lo cual $(F^*, \cdot)$ hereda todas las propiedades de $(F, \cdot)$, así tenemos que $(F^*, \cdot)$ es un grupo abeliano.

□

Definición 1.3 (Subanillo)
Sea S un subconjunto no vacío de un anillo R. Si S es un anillo con las mismas operaciones de suma y producto del anillo R, entonces se dice que S es un subanillo de R.

Para determinar si un subconjunto S de un anillo R es o no un subanillo de R, el siguiente lema nos ayuda a demostrar de manera rápida este hecho.

Lema 1.1 (Subanillo)
Sea R un anillo y sea S un subconjunto del anillo R. Se dice que S es un subanillo de R si y sólo si:

1. $0 \in S$.
2. Para todo $a, b \in S$:$a - b \in S$.
3. Para todo $a, b \in S$: $ab \in S$.

Demostración.

$\Rightarrow$) Si S es un subanillo de R entonces se tiene que $0 \in S$,y para todo $a, b \in S$: $a - b \in S$ y $ab \in S$, ya que $(S, +)$ es un grupo abeliano y $(S, \cdot)$ es un semigrupo.

$\Leftarrow$)

1. Como la suma en R es conmutativa y S es cerrado bajo la substracción, por la teoría de grupos se tiene que $(S, +)$ es un grupo abeliano.
2. Dado que la multiplicación en R es asociativa y $ab \in S$, tenemos que $(S, \cdot)$ es un semigrupo.
3. Nuevamente, dado que la multiplicación en R es asociativa y distributiva sobre la adición, lo mismo es cierto para S cumpliéndose así la tercera propiedad de ser un anillo.

□

Ejemplos.

1. Mostrar que el conjunto de los números enteros $\mathbb{Z}$, con las operaciones usuales de suma y producto, es un anillo, además $\mathbb{Z}$ es un dominio de integridad.

   Solución. Primero veamos que en efecto $(\mathbb{Z}, +, \cdot)$ es un anillo:

   a) $(\mathbb{Z}, +)$ es un grupo abeliano, ya que por las mismas propiedades de los números enteros la suma está bien definida, además se cumple la propiedad asociativa, conmutativa y la existencia del elemento neutro e inverso.

b) $(\mathbb{Z}, \cdot)$ debe ser un semigrupo.

1) La operación binaria $(\cdot)$ está bien definida, puesto que para todo $a, b \in \mathbb{Z}$ se cumple que: $a \cdot b = c$ donde $c \in \mathbb{Z}$.

2) En el conjunto de los números enteros $\mathbb{Z}$ se cumple la propiedad asociativa respecto al producto.

Por tanto, $(\mathbb{Z}, \cdot)$ es un semigrupo.

c) En los números enteros el producto es distributivo respecto a la suma, así tenemos:

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

2) $(b + c)a = (ba) + (ca)$.

Con lo cual hemos probado que $(\mathbb{Z}, +, \cdot)$ es un anillo.

Ahora probemos que $(\mathbb{Z}, +, \cdot)$ es un dominio íntegro.

Ya que en el conjunto de los números enteros $\mathbb{Z}$ existe el elemento identidad respecto al producto y además cumple con la propiedad conmutativa, tenemos que $\mathbb{Z}$ es un anillo conmutativo y unitario. Luego, en los enteros no existe ningún número distinto de cero, tal que al multiplicarlo con otro número distinto de cero su resultado sea cero. Por tanto, $\mathbb{Z}$ es un dominio íntegro.

2. El conjunto $2\mathbb{Z} = \{2k \mid k \in \mathbb{Z}\}$, con las operaciones usuales de suma y producto, es un anillo conmutativo sin elemento unidad y sin divisores de cero.

Solución. Para este ejercicio usaremos el Lema 1.1.

Podemos ver que $2\mathbb{Z}$ es un subconjunto de $\mathbb{Z}$ por tanto mostremos que:

a) $0 \in 2\mathbb{Z}$.

En efecto, el elemento neutro aditivo está en $2\mathbb{Z}$ ya que se lo puede expresar como $0 = 2 \cdot 0$ con $0 \in \mathbb{Z}$, tal que $a + 0 = a$ donde $a = 2k_1$ con $k_1 \in \mathbb{Z}$.

b) Para todo $a, b \in 2\mathbb{Z}$: $a - b \in 2\mathbb{Z}$.

Sea $a = 2k_1, b = 2k_2 \in 2\mathbb{Z}$ con $k_1, k_2 \in \mathbb{Z}$:

$$\begin{aligned} a - b &= 2k_1 + (-2k_2) \\ &= 2(k_1 - k_2) && \text{(factorando)} \\ &= 2k_3 \in 2\mathbb{Z}. && (k_1 - k_2 = k_3 \in \mathbb{Z}) \end{aligned}$$

c) Para todo $a, b \in 2\mathbb{Z}$: $ab \in 2\mathbb{Z}$.

$$\begin{aligned} ab &= (2k_1)(2k_2) \\ &= 2(k_1 2k_2) && \text{(agrupando)} \\ &= 2k_3 \in 2\mathbb{Z}. && (k_1 2k_2 = k_3 \in \mathbb{Z}) \end{aligned}$$

Como se cumplen las propiedades, tenemos que $2\mathbb{Z}$ es un subanillo de $\mathbb{Z}$ y en particular $2\mathbb{Z}$ es un anillo.

Lo que nos queda por mostrar es que $(2\mathbb{Z}, +, \cdot)$ no sea unitario y que no tenga divisores de cero.

$(2\mathbb{Z}, +, \cdot)$ no es unitario, ya que 1 no es elemento de $2\mathbb{Z}$, pues 1 no se puede expresar de la forma $2k$ con $k \in \mathbb{Z}$. Luego, $(2\mathbb{Z}, +, \cdot)$ no tiene divisores de cero, ya que si a y b son no nulos al multiplicarlos, su resultado será distinto de cero.

3. El conjunto $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$, donde i es el número complejo tal que $i^2 = -1$, con las operaciones usuales de suma y producto de números complejos, es un dominio de integridad.

   Solución. Mostremos que es un anillo, se observa que $\mathbb{Z}[i]$ es un subconjunto de los números complejos, podemos utilizar el Lema 1.1.

   Sean $x, y, z \in \mathbb{Z}[i]$ donde $x = a_1 + b_1 i$, $y = a_2 + b_2 i$ y $z = a_3 + b_3 i$.

   a) $0 \in \mathbb{Z}[i]$.

   En efecto, el elemento neutro aditivo está en $\mathbb{Z}[i]$, pues es $0 = 0 + 0i$.

   b) Para todo $x, y \in \mathbb{Z}[i]$: $x - y \in \mathbb{Z}[i]$.

$$\begin{aligned} x - y &= (a_1 + b_1 i) - (a_2 + b_2 i) \\ &= (\underbrace{a_1 - a_2}_{\in \mathbb{Z}}) + (\underbrace{b_1 - b_2}_{\in \mathbb{Z}})i \\ &= c + di \in \mathbb{Z}[i]. \end{aligned}$$

c) Para todo $x, y \in \mathbb{Z}[i] : ab \in \mathbb{Z}[i]$.

$$\begin{aligned} xy &= (a_1 + b_1 i)(a_2 + b_2 i) \\ &= a_1 a_2 + a_1 b_2 i + b_1 i a_2 + b_1 b_2 i^2 \\ &= (a_1 a_2 - b_1 b_2) + (a_1 b_2 + b_1 a_2) i \qquad (i^2 = -1) \\ &= b + ci \in \mathbb{Z}[i]. \end{aligned}$$

Por tanto, $\mathbb{Z}[i]$ es un subanillo de los complejos, lo que implica que $\mathbb{Z}[i]$ es un anillo.

Ahora probemos que $\mathbb{Z}[i]$ es un dominio íntegro:

Por contradicción, supongamos que $\mathbb{Z}[i]$ tiene divisores de cero.

Consideremos $x = a_1 + b_1 i$ donde a_1 o b_1 es distinto de cero y $y = a_2 + b_2 i$ donde a_2 o b_2 es distinto de cero.

Multiplicando xy tenemos:

$$\begin{aligned} xy &= (a_1 + b_1 i)(a_2 + b_2 i) \\ &= (a_1 a_2 - b_1 b_2) + (a_1 b_2 + b_1 a_2) i. \end{aligned}$$

De esto deducimos que:

$$xy = 0 \Leftrightarrow \begin{cases} a_1 a_2 - b_1 b_2 = 0 \\ a_1 b_2 + b_1 a_2 = 0 \end{cases}$$

multiplicando por b_2 en la primera ecuación y $-a_2$ en la segunda ecuación tenemos:

$$\begin{cases} a_1 a_2 b_2 - b_1 b_2^2 = 0 \\ -a_1 a_2 b_2 - b_1 a_2^2 = 0 \end{cases}$$

Luego, sumando las ecuaciones obtenemos $-b_1 \left(a_2^2 + b_2^2\right) = 0$ y multiplicando por -1 a ambos lados tenemos $b_1 \left(a_2^2 + b_2^2\right) = 0$ de esto se tiene que $b_1 = 0$ ó $a_2^2 + b_2^2 = 0$.

Si $b_1 = 0$ entonces a_1 tiene que ser diferente de cero.

De la ecuación $a_1 a_2 - b_1 b_2 = 0$, si $a_1 a_2 = 0$ entonces $a_2 = 0$ ya que $a_1 \neq 0$.

De la ecuación $a_1 b_2 + b_1 a_2 = 0$, si $a_1 b_2 = 0$ entonces $b_2 = 0$ ya que $a_1 \neq 0$.

Pero esto nos lleva a una contradicción, ya que a_2 y b_2 no pueden ser ambos nulos.

Ahora si $a_2^2 + b_2^2 = 0$, la única manera para que la suma de dos números elevados al cuadrado de cero es que tanto a_2 como b_2 sean cero, lo que nuevamente nos lleva a una contradicción.

Por tanto, podemos concluir que $\mathbb{Z}[i]$ es un dominio íntegro.

Definición 1.4 (Ideal)
Un subconjunto I de un anillo R, se dice que es un ideal de R, sí:

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

Ejemplo. Considere el anillo $(\mathbb{M}_2(\mathbb{Z}), +, \cdot)$, donde $\mathbb{M}_2(\mathbb{Z})$ son las matrices de orden dos con entradas enteras.

Mostrar que el conjunto $I = \left\{ \begin{bmatrix} a_1 & a_2 \\ a_3 & a_4 \end{bmatrix} \mid a_i = 2k \in \mathbb{Z} \right\}$ es un ideal de $(\mathbb{M}_2(\mathbb{Z}), +, \cdot)$

Solución. Sean $A, B \in I$ tales que: $A = \begin{bmatrix} a_1 & a_2 \\ a_3 & a_4 \end{bmatrix}; a_i = 2x_i$. $B = \begin{bmatrix} b_1 & b_2 \\ b_3 & b_4 \end{bmatrix}; b_i = 2y_i$, con $x_i, y_i \in \mathbb{Z}$.

Verifiquemos si se cumplen las tres propiedades:

1. $0 \in I$, pues existe la matriz nula $N = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$.

2.
$$\begin{aligned} A - B &= \begin{bmatrix} a_1 & a_2 \\ a_3 & a_4 \end{bmatrix} - \begin{bmatrix} b_1 & b_2 \\ b_3 & b_4 \end{bmatrix} \\ &= \begin{bmatrix} a_1 - b_1 & a_2 - b_2 \\ a_3 - b_3 & a_4 - b_4 \end{bmatrix}; a_i - b_i = 2(x_i - y_i) \in I \end{aligned}$$

3. Para la mutiplicación utilizaremos la siguiente notación:

   $A = (a_{ij}) \in I; a_{ij} = 2k_{ij}$.

   $B = (b_{ij}) \in \mathbb{M}_2(\mathbb{Z}); b_{ij} \in \mathbb{Z}$.

   $a)\ AB = c_{ij} = \sum_{k=1}^{2} \underbrace{a_{ik}}_{\in 2k_{ij}} b_{kj} \in \mathbb{M}_2(\mathbb{Z})$.

   $b)\ BA = d_{ij} = \sum_{k=1}^{2} b_{ik} \underbrace{a_{kj}}_{\in 2k_{ij}} \in \mathbb{M}_2(\mathbb{Z})$.

Por tanto, I es un ideal del anillo $(\mathbb{M}_2(\mathbb{Z}), +, \cdot)$.

Observación. A partir de la definición se puede observar que todo ideal I de un anillo R es también un subanillo de R.

Consideremos el conjunto $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ con las operaciones de suma y producto en los complejos, mostraremos que no todo subanillo de R es un ideal de R.

Demostración. Debemos mostrar las propiedades de ser un ideal. Como $\mathbb{Z}[i]$ es un subanillo de $\mathbb{C}$ la primera y segunda propiedad de ser un ideal se cumplen.

Nos falta por mostrar que: $rz \in \mathbb{Z}[i]$ y $zr \in \mathbb{Z}[i]$ para todo $z \in \mathbb{Z}[i]$ y $r \in \mathbb{C}$.

Sean: $r = \frac{a}{b} + \frac{c}{d}i \in \mathbb{C}$ donde $\frac{a}{b}, \frac{c}{d} \in \mathbb{Q}$ y $z = a_1 + b_1 i \in \mathbb{Z}[i]$.

Multiplicando:

$$\begin{aligned} rz &= \left(\frac{a}{b} + \frac{c}{d}i\right)(a_1 + b_1 i) \\ &= \left(\frac{a}{b}a_1 - \frac{c}{d}b_1\right) + \left(\frac{a}{b}b_1 + \frac{c}{d}a_1\right) i \\ &= \left(\frac{aa_1d - cbb_1}{bd}\right) + \left(\frac{ab_1 - a_1bc}{bd}\right) i \notin \mathbb{Z}[i]. \end{aligned}$$

Por tanto, $\mathbb{Z}[i]$ no es un ideal de $\mathbb{C}$. □

Teorema 1.1

Sea R un anillo conmutativo y unitario, sean $a_1, \ldots, a_k$ elementos de R. Entonces el conjunto $I = \{a_1x_1 + \cdots + a_kx_k \mid x_1, \ldots, x_k \in \mathbb{R}\}$ es un ideal de R. Se dice que I es el ideal de R generado por los elementos $a_1, \ldots, a_k$ y se denota $I = \langle a1, \ldots, ak \rangle$.

Demostración. Debemos mostrar que se cumplen las 3 propiedades de un ideal.

1. $0 \in I$.

   Como R es un anillo tenemos que $0 \in R$, así: $0 = (a_10 + \cdots + a_k0)$, por tanto $0 \in I$.

2. $c - d \in I$ para todo $c, d \in I$.

   Sea $c = (a_1x_1 + \cdots + a_kx_k)$ y $d = (a_1y_1 + \cdots + a_ky_k)$ con $a_n, x_n, y_n \in R$ para todo $n = 1, \ldots, k$.

$$\begin{aligned} c - d &= (a_1x_1 + \cdots + a_kx_k) - (b_1y_1 + \cdots + b_ky_k) \\ &= (a_1x_1 - a_1y_1) + \cdots + (a_kx_k - a_ky_1) \\ &= a_1(\underbrace{x_1 - y_1}_{\in R}) + \cdots + a_k(\underbrace{x_k - y_1}_{\in R}) \in I \end{aligned}$$

   Por tanto, $c - d \in I$.

3. $cr \in I$ y $rc \in I$ para todo $c \in I$ y $r \in R$.

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

   Así, $rc \in R$, luego, como R es conmutativo $rc = cr$.

Por tanto, concluimos que I es un ideal. □

Definición 1.5 (Ideal principal)
Sea R un anillo conmutativo y unitario. R será un anillo de ideales principales si para cada ideal I de R existe $a \in R$ tal que $I = \langle a \rangle = \{ar \mid r \in R\}$.

El siguiente ejemplo que presentamos, muestra que todo ideal de $\mathbb{Z}$ es de la forma $n\mathbb{Z}$.

Ejemplo. Mostrar que $\mathbb{Z}$ es un anillo de ideales principales.

Demostración. Sea I un ideal de $\mathbb{Z}$. Si $I = \{0\}$ entonces I es un ideal principal, pues $\langle 0 \rangle = \{0r \mid r \in \mathbb{Z}\}$.

Supongamos que $I \neq \{0\}$, definimos $I^* = \{a \in I \mid a > 0\}$, así tenemos que $I^* \subset \mathbb{N}$, luego, por el principio del buen orden de los números naturales existe $d \in I^*$ tal que $d = \min(I^*)$.

Ahora debemos mostrar que $I = \langle d \rangle$.

1. $\langle d \rangle \subseteq I$.

   Sea $x \in \langle d \rangle$ entonces $x = rd \in I$ pues $d \in I$ y $r \in \mathbb{Z}$ con lo cual $\langle d \rangle \subseteq I$.

2. $I \subseteq \langle d \rangle$.

   Sea $x \in I$, por el algoritmo de Euclides existen $r, q \in \mathbb{N}$ tal que:

$$x = qd + r \text{ con } 0 \leq r < d.$$

   Luego, $r = \underbrace{x}_{\in I} - \underbrace{qd}_{\in I} \in I$. Dado que d es el entero positivo más pequeñõ y $r < d$ tenemos qué $r = 0$.

Así $x = qd \in \langle d \rangle$, por tanto $I \subseteq \langle d \rangle$. □

Lema 1.2
Sean I, H dos ideales de un anillo R, entonces $I + H = \{i + h \mid i \in I, h \in H\}$ es un ideal de R.

Demostración. Mostremos que se cumplen las tres propiedades de un ideal.

1. Como I y H son ideales, tenemos que el 0 está en cada uno de ellos, así:

$$0 = 0 + 0 \in I + H.$$

2. Sean $a, b \in I + H$ tal que: $a = i_1 + h_1$ y $b = i_2 + h_2$.

$$\begin{aligned} a - b &= (i_1 + h_1) - (i_2 + h_2) \\ &= (\underbrace{i_1 - i_2}_{\in I}) + (\underbrace{h_1 - h_2}_{\in H}) \in I + H. \end{aligned}$$

3. Sea $r \in$R y sea $a \in I + H$. Tengamos presente que I, H son ideales.

   a)

$$\begin{aligned} ar &= (i_1 + h_1)r \\ &= (\underbrace{i_1 r}_{\in I}) + (\underbrace{h_1 r}_{\in H}) \in I + H \end{aligned}$$

   b)

$$\begin{aligned} ra &= r(i_1 + h_1) \\ &= (\underbrace{ri_1}_{\in I}) + (\underbrace{rh_1}_{\in H}) \in I + H \end{aligned}$$

Por tanto, podemos concluir que la suma de dos ideales de R es un ideal de R. □

Ejemplo. Si R es un anillo unitario e I es un ideal de R tal que $1 \in I$, entonces $I = R$.

Solución. Debemos mostrar que se cumplen las dos inclusiones:

1. $I \subseteq R$:

   Por definición sabemos que I es un ideal de R, eso implica qué $I \subseteq R$.

2. $R \subseteq I$:

   Consideremos un elemento $a \in R$ entonces $a = a1$ y como la tercera propiedad de ser un ideal nos afirma que si $a \in R$ y $b \in I$ entonces $ab \in R$. Es decir que $a = a1 \in I$, lo que implica que $R \subseteq I$.

Por tanto, $I =$R.

Definición 1.6 (Subcampo)
Si un subconjunto K de un campo F cerrado respecto a las operaciones de suma y producto de F, es un campo, entonces diremos que K es un subcampo de F (denotado por $K \leq F$).

Al igual que en el caso de un subanillo, existe un lema que nos ayuda a demostrar cuando K es un subcampo de F.

Lema 1.3
Sea F un campo y K un subconjunto de F. Entonces K es un subcampo de F, si y sólo si:

1. $0 \in K$.
2. para todo $a, b \in K : a - b \in K$ y $ab \in K$.
3. $1 \in F$ es un elemento en K.
4. Para todo elemento no nulo de K su inverso también está en K.

Demostración.

$\Rightarrow$) Si K es un subcampo, por definición K es también un campo, por tanto, las cuatro propiedades se cumplen.

$\Leftarrow$) Por las dos primeras propiedades se puede observar que K es un subanillo, por tanto, K es también un anillo. Dado que K es un subconjunto de F, entonces K es un anillo conmutativo, pues en F se cumple qué $ab = ba$. Finalmente, las dos últimas propiedades nos aseguran que en efecto K es un campo. □

Ejemplo. Consideremos el conjunto $\mathbb{Q}(i) = \{a + bi \mid a, b \in \mathbb{Q}\}$, donde i es el número complejo tal que $i^2 = -1$, mostrar que $\mathbb{Q}(i)$ es un campo.

Solución. Por el Lema 1.3 solo debemos probar que $\mathbb{Q}(i)$ sea un subcampo de $\mathbb{C}$. Así,

a) $0 = 0 + 0i \in \mathbb{Q}(i)$.

b) sean $x = a + bi, y = c + di \in \mathbb{Q}(i)$ donde $a, b, c, d \in \mathbb{Q}$.

$$\begin{aligned} x - y &= (a + bi) - (c + di) \\ &= (\underbrace{a - c}_{\in \mathbb{Q}}) + (\underbrace{b - d}_{\in \mathbb{Q}})i \in \mathbb{Q}(i). \end{aligned}$$

Luego:

$$\begin{aligned} xy &= (a + bi)(c + di) \\ &= (\underbrace{ac - bd}_{\in \mathbb{Q}}) + (\underbrace{ac + bd}_{\in \mathbb{Q}})i \in \mathbb{Q}(i). \end{aligned}$$

c) $1 = 1 + 0i \in \mathbb{Q}(i)$.

d) Sea $x = a + bi \neq 0 \in \mathbb{Q}(i)$ con $a, b \in \mathbb{Q}$, entonces a es no nulo o b es no nulo, así:

$$\begin{aligned} x^{-1} &= (a + bi)^{-1} \\ &= \left(\frac{1}{a + bi}\right)\left(\frac{a - bi}{a - bi}\right) \qquad \text{(racionalizando)} \\ &= \frac{a}{a^2 + b^2} - \frac{b}{a^2 + b^2}i \in \mathbb{Q}(i). \end{aligned}$$

Por tanto, $\mathbb{Q}(i)$ es un campo.

Teorema 1.2 (Anillo cociente)

Sea R un anillo, y sea I un ideal de R. El conjunto $R/I = \{a + I \mid a \in R\}$ es un anillo con las operaciones:

1. $(a + I) + (b + I) = (a + b) + I$ para todo $a, b \in R$.
2. $(a + I)(b + I) = (ab) + I$ para todo $a, b \in R$.

Demostración.

1. Desde la teoría de grupos el conjunto R/I es un grupo bajo la adición. Además $(a + I) + (b + I) = (a + b) + I = (b + a) + I$ ya que R es un anillo, Por tanto $(R/I, +)$ es un grupo conmutativo.

2. Probemos que $(a+I)(b+I) = (ab)+I$ esté bien definido. Es decir, debemos mostrar que:

$$\begin{aligned}(a+I)(b+I) &= (a'+I)(b'+I)\\ (ab)+I &= (a'b')+I.\end{aligned}$$

Sea $a+I = a'+I$ y $b+I = b'+I$, se tiene que $a-a' \in I$ 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 $b = b'+t$.

$$\begin{aligned}ab+I &= (a'+s)(b'+t)+I\\ &= a'b' + (\underbrace{a't+sb'+st+I}_{\in I})\\ &= a'b'+I.\end{aligned}$$

Así, el producto está bien definido.

Ahora probemos que el producto es asociativo:

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

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

3. Nos falta mostrar que el producto sea distributivo respecto a la suma.

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

a)

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

b)

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

Por tanto, R/I es un anillo. □

Definición 1.7 (Ideal maximal)
Sean R un anillo e I un ideal de R con $I \neq R$. El ideal I 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 $J = R$.

Ejemplo. Mostremos que el ideal $\langle 3 \rangle = 3\mathbb{Z}$ es un ideal maximal de $\mathbb{Z}$.

Solución. Sea J un ideal de $\mathbb{Z}$ tal que $3\mathbb{Z} \subset J \subset \mathbb{Z}$. Como $\mathbb{Z}$ es un anillo de ideales principales, ya que existe $1 \in \mathbb{Z}$ tal que $\langle 1 \rangle = \{1x \mid x \in \mathbb{Z}\} = \mathbb{Z}$, y $J \neq \{0\}$ pues $3 \in J$, entonces existe un $n \in \mathbb{Z}^+$ tal que $J = n\mathbb{Z}$. Dado que $3\mathbb{Z} \subset n\mathbb{Z}$, existe $q \in \mathbb{Z}^+$ tal que $3 = nq$. Como $3 = nq$ implica que $n = 3$ ó $n = 1$. Si $n = 3$, entonces $3\mathbb{Z} = J$ ó si $n = 1$, entonces $J = \mathbb{Z}$. Por tanto, $3\mathbb{Z}$ es un ideal maximal de $\mathbb{Z}$.

Teorema 1.3
Si p es un número primo, entonces $p\mathbb{Z}$ es un ideal maximal del anillo $\mathbb{Z}$.

Demostración. Sea $n\mathbb{Z}$ un ideal del anillo $\mathbb{Z}$ tal que $p\mathbb{Z} \subset n\mathbb{Z}$.

Si $p\mathbb{Z} \subset n\mathbb{Z}$ entonces $n \mid p$, luego, por el lema de Euclides $p = nk$ con $k \in \mathbb{Z}$.

Como p es primo tenemos:

$$n = p \quad \text{o} \quad n = 1$$

Si $n = p \Rightarrow p\mathbb{Z} = n\mathbb{Z}$.

Si $n = 1 \Rightarrow n\mathbb{Z} = \mathbb{Z}$.

Por tanto, podemos concluir que $p\mathbb{Z}$ es un ideal maximal de $\mathbb{Z}$. □

Teorema 1.4
Sean R un anillo conmutativo y unitario, I un ideal de R. Entonces I es un ideal maximal de R si y sólo si R/I es un campo.

Demostración.

$\Rightarrow$)Si I es un ideal maximal de R, entonces R/I es un campo.

Sea $a \in R$ tal que $a \notin I$. Consideremos el conjunto $J = \{ar + b \mid r \in R, b \in I\}$ tal que $I \subset J$.

Probemos que J es un ideal de R.

a) $0 \in J$ ya que R es un anillo e I un ideal.

b) Sean $x, y \in J$ tales que $x = a_1r + b_1$ y $y = a_2r + b_2$.

$$\begin{aligned} x - y &= (a_1r + b_1)(a_2r + b_2) \\ &= (a_1r - a_2r) + (b_1 - b_2) \\ &= (\underbrace{a_1 - a_2}_{\in R})r + (\underbrace{b_1 - b_2}_{\in I}) \in J. \end{aligned}$$

c) Para el producto.

Sea $r' \in R$, entonces:

$$\begin{aligned} r'x &= r'(a_1 + b_1) \\ &= r'a_1 r + r'b_1 \\ &= a_1(\underbrace{r'r}_{\in R}) + (\underbrace{r'b_1}_{\in J}) \in J. \end{aligned}$$

Como R es conmutativo $r'x = xr'$.

Así, concluimos que J es un ideal de R.

Como I es un ideal maximal entonces $J = R$, por tanto, existe $r_1 \in R$ y $b' \in I$ tal que $1 = ar + b'$.

Así,

$$\begin{aligned} 1 + I &= ar_1 + \underbrace{b' + I}_{\in I} \\ &= ar_1 + I \\ &= (a + I)(r_1 + I). \end{aligned}$$

Mostrando así que para todo elemento no nulo de R/I su inverso también está en R/I. Luego R/I es conmutativo y unitario, ya que R también lo es, así, R/I es un campo.

$\Leftarrow$) Si R/I es un campo, entonces I es un ideal maximal.

Consideremos un ideal J del anillo R tal que $I \subsetneq J \subseteq R$. Luego, sea $a \in J$, pero $a \notin I$, lo que implica que $a + I \neq I$.

Ya que R/I es un campo existen $b + I \in R/I$ tal que:

$$\begin{aligned} 1 + I &= (a + I)(b + I) \\ &= ab + I. \end{aligned}$$

Luego $1 - ab \in I \subseteq J$.

Así $1 = (1 - ab) + ab \in J$.

Lo que implica que $J = R$, por tanto, I es maximal. □

Lema 1.4
Si p es un número primo, entonces $\mathbb{Z}/p\mathbb{Z}$ es un campo formado por p elementos.

Demostración.

Por el Teorema 1.3 tenemos que $p\mathbb{Z}$ es un ideal maximal de $\mathbb{Z}$, luego, por el Teorema 1.4, $\mathbb{Z}/p\mathbb{Z}$ es un campo. Lo único que nos falta mostrar es que $\mathbb{Z}/p\mathbb{Z}$ tiene p elementos.

Por definición de anillo cociente tenemos que: $\mathbb{Z}/p\mathbb{Z} = \{a + p\mathbb{Z}\}$.

De lo cual, los elementos de $\mathbb{Z}/p\mathbb{Z} = \{\{0 + p\mathbb{Z}\}, \{1 + p\mathbb{Z}\}, \{2 + p\mathbb{Z}\} + \cdots + \{p - 1 + p\mathbb{Z}\}\}$.

Si consideramos:

$\{p + p\mathbb{Z}\} = p\mathbb{Z} = \{0 + p\mathbb{Z}\}$.

$\{p + 1 + p\mathbb{Z}\} = (p + p\mathbb{Z}) + (1 + p\mathbb{Z}) = (0 + p\mathbb{Z}) + (1 + p\mathbb{Z}) = 1 + p\mathbb{Z}$.

Los elementos se repiten, con lo cual $\mathbb{Z}/p\mathbb{Z}$ tiene p elementos. □

Definición 1.8 (Homomorfismo de anillos)
Sean R, S anillos. Una función $f : R \to S$ es un homomorfismo de anillos, si y sólo si:

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

Ejemplo. La función $\phi : \mathbb{C} \to \mathbb{C}$ definida por $\phi(a + bi) = a - bi$ es un homomorfismo de anillos.

Solución. Consideremos $x, y \in \mathbb{C}$, definidos como: $x = a_1 + b_1 i$, $y = a_2 + y_2 i$.

- Suma.

$$\begin{aligned}\phi(x+y) &= \phi[(a_1+b_1i)+(a_2+y_2i)]\\ &= \phi[(a_1+a_2)+(b_1+b_2)i]\\ &= (a_1+a_2)-(b_1+b_2)i\\ &= (a_1-b_1i)+(a_2-b_2i)\\ &= \phi(a_1+b_1)+\phi(a_2+b_2i)\\ &= \phi(x)+\phi(y).\end{aligned}$$

- Producto.

$$\begin{aligned}\phi(xy) &= \phi[(a_1+b_1i)(a_2+y_2i)]\\ &= \phi[(a_1a_2-b_1b_2)+(a_1b_2+a_2b_1)i]\\ &= (a_1a_2-b_1b_2)-(a_1b_2+a_2b_1)i\\ &= a_1a_2-b_1b_2-a_1b_2i-a_2b_1i. \qquad (1)\end{aligned}$$

Por otro lado, tenemos:

$$\begin{aligned}\phi(x)\phi(y) &= \phi(a_1+b_1)\phi(a_2+b_2i)\\ &= (a_1-b_1i)(a_2-b_2i)\\ &= a_1a_2-b_1b_2-a_1b_2i-a_2b_1i. \qquad (2)\end{aligned}$$

Como las ecuaciones (1) y (2) coinciden, podemos concluir que ϕ es un homomorfismo de anillos.

Teorema 1.5

Sean R, S anillos. $\phi : R \to S$ un homomorfismo de anillos. Se satisfacen las siguientes propiedades:

1. $\phi(R) = \{\phi(r \mid r \in R\}$ es un subanillo de S.
2. Ker(ϕ) es un ideal de R.
3. $\phi : R \to S$ es un homomorfismo inyectivo de anillos si y sólo si

$$Ker(\phi) = \{r \in R \mid \phi(r) = 0\}.$$

Demostración.

1. Para el primero debemos mostrar que se cumplan las propiedades del Lema 1.1.

   a) $0 \in \phi(R)$.

   Como $0 \in R$ entonces $\phi(0) + 0 = \phi(0) = \phi(0+0) = \phi(0) + \phi(0)$ por la propiedad cancelativa tenemos que $\phi(0) = 0$.

   b) Sean $x, y \in \phi(R)$. Existen $r, s \in R$ tales que $\phi(r) = x$ y $\phi(s) = y$.

   Así, $x - y = \phi(r) - \phi(s) = \phi(r - s)$ ya que ϕ es un homomorfismo. Luego, $\phi \underbrace{(r-s)}_{\in R} \in \phi(R)$, con lo cuál $x - y \in \phi(R)$.

   c) $xy = \phi(r)\phi(s) = \phi(rs)$, ya que ϕ es un homomorfismo. Luego, $\phi \underbrace{(rs)}_{\in R} \in \phi(R)$, con lo cuál $xy \in \phi(R)$.

   Por tanto, $\phi(R) = \{\phi(r \mid r \in R\}$ es un subanillo de S.

2. Mostremos que se cumplen la las propiedades de ser un ideal.

   a) $0 \in \text{Ker}(\phi)$ pues $\phi(0) = 0$.

   b) Sean $x, y \in \text{Ker}(\phi)$. Se tiene qué $\phi(x) = 0, \phi(y) = 0$.

   Así, $\phi(x - y) = \phi(x) - \phi(y) = 0 - 0 = 0$. Luego $x - y \in \text{Ker}(\phi)$.

   c) Sea $r \in R$, $\phi(rx) = \phi(r)\phi(x) = \phi(r)0 = 0$. Luego $rx \in \text{Ker}(\phi)$.

   De manera similar tenemos que $xr \in \text{Ker}(\phi)$.

   Por tanto, $\text{Ker}(\phi)$ es un ideal de R.

3. $\Rightarrow$) Sean $r, s \in R$. Si:

$$\begin{aligned} \phi(r) &= \phi(s) \\ \phi(r) - \phi(s) &= 0 \\ \phi(r - s) &= 0. \end{aligned}$$

   Entonces $r - s \in Ker(\phi)$, implica que $r - s = 0$, con lo cual $r = s$.

   $\Leftarrow$) Supongamos que $\text{Ker}(\phi) \neq \{0\}$.

Sean $a, b \in \text{Ker}(\phi)$ no nulos, entonces $\phi(a) = \phi(b) = 0$, de lo cual, ϕ no es inyectiva, ya que $\phi(a) \neq a$ y $\phi(b) \neq b$. Por tanto, Ker(ϕ)= $\{0\}$ para que ϕ sea inyectiva.

Con lo cual hemos mostrado que $\phi : R \to S$ es un homomorfismo inyectivo de anillos si y sólo si $Ker(\phi) = \{r \in R \mid \phi(r) = 0\}$.

□

Definición 1.9
Sean R, S anillos.

1. Si $f : R \to S$ es un homomorfismo biyectivo de anillos, diremos que $f : R \to S$ es un isomorfismo de anillos.
2. Si existe un isomorfismo de anillos $f : R \to S$, diremos que R y S son anillos isomorfos. La cual la denotaremos por $R \approx S$.
3. Si $f : R \to S$ es un isomorfismo de anillos, diremos que f es un automorfismo dé R.
4. Si $f : R \to S$ es un homomorfismo inyectivo de anillos, diremos que f es un monomorfismo de anillos.

Teorema 1.6 (Primer teorema de isomorfismo de anillos)
Sean R, S anillos. Si $f : R \to S$ es un homomorfismo de anillos, entonces los anillos $R/\text{Ker}(f)$ y $f(R)$ son isomorfos $R/\text{Ker}(f) \approx f(R)$.

Demostración. Ya que $\text{Ker}(f)$ es un subgrupo normal de R, por el primer teorema de isomorfía de grupos tenemos que $\psi : R/\text{Ker}(f) \to f(R)$ definida como $\psi(r + \text{Ker}(f)) = f(r)$ es un isomorfismo de grupos.

Lo único que nos falta mostrar es que ψ conserva la mutiplicación. Para lo cual,

sean $(r_1 + \text{Ker}(f)), (r_2 + \text{Ker}(f)) \in R/\text{Ker}(f)$.

$$\begin{aligned}\psi((r_1 + \text{Ker}(f))(r_2 + \text{Ker}(f))) &= \psi(r_1 r_2 + \text{Ker}(f)) \\ &= f(r_1 r_2) \\ &= f(r_1) f(r_2) \\ &= \psi(r_1 + \text{Ker}(f))\psi(r_2 + \text{Ker}(f)).\end{aligned}$$

Por tanto $(R/\text{Ker}(f) \approx f(R))$. □

Teorema 1.7

Sean R, S, A anillos:

1. Si $\phi : R \to S$ es un isomorfismo de anillos, entonces $\phi^{-1} : S \to R$ también lo es.
2. Si $\phi : R \to S$ y $\sigma : S \to A$ son homomorfismos de anillos, entonces $\sigma \circ \phi : R \to A$ es un homomorfismo de anillos.

Demostración. 1. Para el primero: Por hipótesis tenemos que ϕ es biyectivo, entonces esto implica que ϕ^{-1} también en biyectivo, lo único que nos falta probar es que ϕ^{-1} sea un homomorfismo. Para lo cual:

Sean $x, y \in S$, existen $a, b \in R$ tales que $\phi(a) = x$ y $\phi(b) = y$, entonces:

a)

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

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

b)

$$\begin{aligned}\phi(\phi^{-1}(xy)) &= xy \\ &= \phi(a)\phi(b) \\ &= \phi(ab).\end{aligned}$$

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

Por tanto, podemos concluir que $\phi^{-1} : S \to R$ es un isomorfismo.

2. Para el segundo; sean $x, y \in S$, existen $a, b \in R$ tales que: $\phi(a) = x$ y $\phi(b) = y$, también, sean $r, s \in A$ tales que: $\sigma(x) = r$ y $\sigma(y) = s$.

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

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

   Por tanto, $\sigma \circ \phi : R \to A$ es un homomorfismo de anillos.

□

Lema 1.5
Sean D, D' dominios de integridad. Si $\phi : D \to D'$ en un monomorfismo de anillos, entonces $\phi(1) = 1'$, donde $1'$ es el elemento neutro de D'.

Demostración. Primero mostremos que $\phi(0) = 0'$.

Sea $a \in D$ y $0' \in D'$, entonces $\phi(a) + 0' = \phi(a) = \phi(a + 0) = \phi(a) + \phi(0)$. Así por la propiedad cancelativa tenemos que $\phi(0) = 0'$.

Por hipótesis sabemos que $\phi(1) \neq 0'$, luego $\phi(1)\phi(1) = \phi(1 \cdot 1) = \phi(1)$, entonces $\phi(1)(\phi(1) - 1) = 0'$. Como D' no tiene divisores de cero y $\phi(1) \neq 0'$, entonces $\phi(1) = 1'$. □

Lema 1.6
Sea K un subcampo de los números complejos y ϕ: $\mathbb{Z} \to K$ un monomorfismo de anillos. Entonces $\phi(x) = x$ para todo $x \in \mathbb{Z}$.

Demostración. Sea $1 \in \mathbb{Z}$, por el Lema 1.5 y dado que ϕ es un monomorfismo tenemos $\phi(1) = 1 + 0i = 1$. Sea $n \in \mathbb{Z}^+$ y supongamos como hipótesis de inducción que $\phi(n) = n$. Entonces mostremos que se cumple para $n + 1 \in \mathbb{Z}$, recordemos que ϕ es un homomorfismo; $\phi(n + 1) = \phi(n) + \phi(1) = n + 1$.

Ahora, para $n \in \mathbb{Z}^-$, como $\phi(0) = 0$, tenemos:

$$\begin{aligned} 0 &= \phi(0) \\ &= \phi(n + (-n)) && \phi \text{ es un homomorfismo} \\ &= \phi(n) + \phi(-n) \end{aligned}$$

de lo cual tenemos: $\phi(-n) = -\phi(n)$.

Finalmente $\phi(-n) = -\phi(n) = -n$.

Por tanto, $\phi(x) = x$ para todo $x \in \mathbb{Z}$. □

Teorema 1.8
Si D es un dominio íntegro, entonces existe un campo K tal que $D \subset K$.

Demostración. Sea D un dominio íntegro, Consideremos un campo K que contenga a D. Partimos definiendo el conjunto $U = \{(a, b) \mid a, b \in D \text{ y } b \neq 0\}$ en el que se define la relación $\sim$ por: $(a, b) \sim (c, d)$ si y solo si $ad = bc$.

Esta relación resulta ser de equivalencia, en efecto:

- Reflexividad:$(a, b) \sim (a, b) \Leftrightarrow ab = ba$.
- Simetría: $(a, b) \sim (c, d) \Leftrightarrow ad = bc \Leftrightarrow cb = da \Leftrightarrow (c, d) \sim (a, b)$.
- Transitividad:$(a, b) \sim (c, d)$ y $(c, d) \sim (e, f) \Leftrightarrow ad = bc$ y $ef = de \Leftrightarrow adf = cbf = bcf = bde \Leftrightarrow cf = de \Leftrightarrow (c, d) \sim (e, f)$. Con lo cual hemos probado que $\sim$ es una relacíon de equivalencia.

Con el resultado obtenido, tenemos que existe la clase de equivalencia $[(a,b)] = \{(x,y) \in U \mid (x,y) \sim (a,b)\}$ para cualquier elemento $(a,b) \in U$. Sabemos que las clases de equivalencias particionan al conjunto U. Sea K el conjunto de todas las clases de equivalencia $[(a,b)]$ con $a, b \in D$ y $b \neq 0$. Para que K sea un campo definimos las siguientes operaciones:

$$[(a,b)] + [(c,d)] = [(ad+bc, bd)] \text{ y } [(a,b)][(c,d)] = [(ac, bd)].$$

Entonces primero debemos mostrar que la adición y el producto están bien definidos:

a) Adición.

Suponemos que:

$$[(a,b)] = [(a',b')] \Rightarrow ab' = ba' \qquad (1)$$
$$[(c,d)] = [(c',d')] \Rightarrow cd' = dc' \qquad (2)$$

luego multiplicamos dd' y bb' respectivamente, y sumando tenemos que:

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

agrupando los sumandos tenemos

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

lo que implica que $[(ad+bc), bd] = [(a'd' + b'c'), b'd']$. Por tanto, la adición está bien definida.

b) Producto.

$$[(a,b)] = [(a',b')] \Rightarrow ab' = ba'$$
$$[(c,d)] = [(c',d')] \Rightarrow cd' = dc'$$

Multiplicando los términos tenemos

$$ab'cd' = ba'dc'$$
$$cb'd' = a'c'bd.$$

Entonces

$[(ac, bd)] = [a'c', b'd')]$, con lo cual el producto también está bien definido.

Ahora mostremos que en efecto K es un campo con las operaciones de suma y producto definidas.

1. $(K, +)$ tiene que ser un grupo abeliano.

   a) Cerradura, como la adición está bien definida, esta propiedad se cumple.

   b) Asociatividad.

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

   c) Elemento neutro.

   Sean $0, 1 \in D$ entonces:

$$\begin{aligned}[(0,1)] + [(a,b)] &= [(0b + 1a, 1b)] \\ &= [(a,b)].\end{aligned}$$

   d) Elemento inverso.

   Como $a \in D$ entonces $-a \in D$

$$\begin{aligned}[(a,b)] + [(-a,b)] &= [(ab + (-ab), bb)] \\ &= [(0, bb)] \\ &= [(0,1)].\end{aligned}$$

e) Conmutatividad.

$$\begin{aligned}
[(a,b)] + [(c,d)] &= [(ad+bc, bd)] \\
&= [(da+cb, db)] && \text{(D es conmutativo)} \\
&= [(cb+da, db)] && \text{(D es conmutativo)} \\
&= [(c,d)] + [(a,b)].
\end{aligned}$$

Por tanto, K es un grupo conmutativo.

2. $(K, \cdot)$ debe ser un semigrupo.

a) Cumple la cerradura, pues el producto está bien definido.

b) Asociatividad.

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

Así, $(K, \cdot)$ es un semigrupo.

3. El producto debe ser distributivo respecto a la adición.

a)

$$\begin{aligned}
([(a,b)] + [(c,d)])[(e,f)] &= ([(ad+bc, bd)])[(e,f)] \\
&= [((ad+bc)e, bdf)] \\
&= [(ade+bce, bdf)] \\
&= [(ade, bdf) + (bce, bdf)] \\
&= [(ae, bf)] + [(ce, df)] \\
&= [(a,b)][(e,f)] + [(c,d)][(e,f)].
\end{aligned}$$

b)

$$\begin{aligned}[(e,f)]([(a,b)]+[(c,d)]) &= [(e,f)]([(ad+bc,bd)]) \\ &= [(e(ad+bc),fbd)] \\ &= [(ead+ebc,fbd)] \\ &= [(ead,fbd)+(ebc,fbd)] \\ &= [(ea,fb)]+[(ec,fd)] \\ &= [(e,f)][(a,b)]+[(e,f)][(c,d)].\end{aligned}$$

Ahora lo que nos falta probar es que para cada elemento no nulo de K su inverso multiplicativo también está en K. Para lo cual notemos que $1 \in D$, así,

a) Elemento neutro.

Sean $1 \in D$ entonces:

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

b) elemento inverso.

Sean $a, b \in D$ no nulos.

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

Por tanto, podemos concluir que $(K,+,\cdot)$ es un campo.

Denotando $[(a,b)] = \dfrac{a}{b}$, obtenemos qué $K = \left\{\dfrac{a}{b} \mid a,b \in D \ y \ b \neq 0\right\}$. Notemos que, sí $\dfrac{a}{b}, \dfrac{c}{d} \in K$, entonces

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

y

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

Donde la función $h : D \to K$ definida por $h(a) = \dfrac{a}{1}$ para todo $a \in D$, es un monomorfismo de anillos. Podemos identificar $a \in D$ con $h(a) = \dfrac{a}{1} \in K$ y escribir $a = \dfrac{a}{1}$. Por lo tanto, $D \subset K$. □

Observación. El campo K, construido a partir del dominio íntegro D, se dice que es el campo de fracciones del dominio íntegro D. Además, K resulta ser el campo más pequeño que contiene a D, es decir: si F es un campo que contiene a D, entonces $K \subset F$. En efecto, si $\frac{a}{b} \in K$ con $a, b \in D$ y $b \neq 0$, entonces $a, b \in F$. Como $b \neq 0$ y F es un campo, entonces $b^{-1} \in F$. Así, $\frac{a}{b} = ab^{-1} \in F$, lo que demuestra $K \subset F$.

Definición 1.10 (Caracterísica del anillo)
Sea R un anillo conmutativo y unitario. Si $n \in \mathbb{Z}^+$, $n \cdot 1$ denotará a los n sumandos $1 + 1 + \cdots + 1 \in R$. Para $n \in \mathbb{Z}^-$, $n \cdot 1$ denotará a los $(-n)$ sumandos $(-1) + (-1) + \ + (-1) = (-n)(-1)$ y $0_z 1 = 0$, donde 0_z es el cero en $\mathbb{Z}$. El menor entero positivo n (en caso de que exista) tal que $n1 = 0$, se dice que el anillo R es de característica n. Si tal entero positivo n no existe, se dice que R es de característica cero.

Teorema 1.9
Sea K un campo.

1. Si la característica de K es $n > 1$, entonces $n = p$ es un número primo y K contiene un subcampo isomorfo a $\mathbb{Z}/p\mathbb{Z}$.
2. Si la característica de K es cero, entonces K contiene un subcampo isomorfo a $\mathbb{Q}$ y luego, K es infinito.
3. Si K es un conjunto finito, entonces K tiene característica p con p primo y luego, K contiene un subcampo isomorfo a $\mathbb{Z}/p\mathbb{Z}$.

Demostración. Denotamos por 1_k al elemento neutro de K. Primero vamos a mostrar que $\phi : \mathbb{Z} \to K$ definido por $\phi(m) = m1_k$ para todo $m \in \mathbb{Z}$, es un homomorfismo de anillos. Entonces:

- Sean $m, n \in \mathbb{Z}$

$$\begin{aligned}\phi(m+n) &= (m+n)1_k && (\mathbb{Z}\text{,K son anillos})\\ &= m1_k + n1_k\\ &= \phi(m) + \phi(n).\end{aligned}$$

-

$$\begin{aligned}\phi(mn) &= (mn)1_k\\ &= mn(1_k 1_k) && (\mathbb{Z}\text{,K son conmutativos})\\ &= m1_k n1_k\\ &= (m1_k)(n1_k)\\ &= \phi(m)\phi(n).\end{aligned}$$

Por tanto, ϕ es un homomorfismo.

Ahora, continuamos con la demostración:

1. Supongamos que la característica de K es $n > 1$. Por definición de característica, $\phi(n) = n1_K = 0$, con lo cual $\text{Ker}(\phi) \neq \{0\}$. Como $\text{Ker}(\phi)$ es un ideal de $\mathbb{Z}$ y $\mathbb{Z}$ es un anillo de ideales principales, existe $n_0 \in \mathbb{Z}^+$ tal que $\text{Ker}(\phi) = n_0\mathbb{Z}$. Dado que $\phi(n) = n1_K = 0$ y n es el menor entero positivo tal que $n1_K = 0$, entonces tenemos que $n \leq n_0$. Luego, como$n \in Ker(\phi) = n_0\mathbb{Z}$, 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, $\phi(\mathbb{Z})$ es un subanillo del campo K y K al ser un campo es un dominio íntegro, es decir, no tiene divisores de cero. Por tanto, no existen divisores del cero en $\phi(\mathbb{Z})$. Con lo cual necesariamente $n = p$ es un número primo.

2. De la demostración anterior, si la característica de K es cero, entonces $\text{Ker}(\phi) = \{0\}$. Así $\phi : \mathbb{Z} \to K$ es inyectiva, por lo tanto, existe un subanillo $\phi(\mathbb{Z})$ contenido en K, el que resulta ser isomorfo a $\mathbb{Z}$. Los campos de fracciones de $\mathbb{Z}$ y de $\phi(\mathbb{Z})$ son isomorfos. De acuerdo a la observación dada luego del Teorema 1.8, el campo de fracciones de $\mathbb{Z}$ es $\mathbb{Q}$ y el campo de fracciones de $\phi(\mathbb{Z})$ está contenido en el campo K.

3. Si K tiene m elementos, entonces $(K, +)$ es un grupo finito con m elementos. De los resultados de la teoría de grupos tenemos que, para $a \in K$, $ma = 0$ donde ma denota los m sumandos $a + a + \cdots + a$ y, por lo tanto, $m1_K = 0$. Existe un menor entero positivo p tal que $p1_K = 0$ que es la característica de K. De (1), p es un número primo y K contiene un subcampo isomorfo a $\mathbb{Z}/p\mathbb{Z}$.

□

1.2 Algunos campos finitos

Definición 1.11 (Campo finito)
Sea F un campo, F se dice que es un campo finito, si este tiene un número finito de elementos.

El anillo $\mathbb{Z}/p$ esta formado por las clases de equivalencia de números enteros módulo p. Es decir; $\mathbb{Z}/p = \{k \in \mathbb{Z} \mid k \equiv a \ (mod\ p)\}$, con $a \in \mathbb{Z}$.

Nota. Las clases de equivalencias están representadas como: $[a]$, con $a \in \mathbb{Z}$. En caso de no haber confusión las clases de equivalencia las podemos representar como: a.

Teorema 1.10
Sea p primo. $\mathbb{Z}/p = \{[0], [1], [2], \ldots, [p-1]\}$ es un dominio íntegro.

Demostración. Sabemos que $\mathbb{Z}/p$ es un anillo conmutativo y unitario, por tanto, lo único que nos falta mostrar es que $\mathbb{Z}/p$ no tenga divisores de cero.

$$\begin{aligned}
&\text{Si } [a][b] = [0] \text{ entonces } [ab] = [0] \\
&\Rightarrow ab \equiv 0(\mathrm{mod}p), \text{utilizando el lema de euclides :} \\
&\text{Si } p \mid ab \text{ entonces } p \mid a \text{ ó } p \mid b \\
&\Rightarrow a \equiv 0(\mathrm{mod}p) \quad \text{ó} \quad b \equiv 0(\mathrm{mod}p) \\
&\Rightarrow [a] = [0] \quad \text{ó} \quad [b] = [0].
\end{aligned}$$

Como ninguno de ellos no puede ser cero, entonces concluimos que $\mathbb{Z}/p$ no tiene divisores de cero. Por tanto, $\mathbb{Z}/p$ es un dominio íntegro. □

Teorema 1.11
Todo campo F es un dominio íntegro.

Demostración. Por hipótesis tenemos que F es un anillo conmutativo y unitario, por tanto, lo que nos falta mostrar que F no tenga divisores de cero. Sean $a, b \in F$ y supongamos que $ab = 0$ con $a \neq 0$, mostremos que $b = 0$. Dado que $ab = 0$ y $a \neq 0$ entonces el inverso de a, al cuál lo denotamos por a^{-1} existe. Así:

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

Con lo cual F es un dominio íntegro. □

Teorema 1.12
Todo dominio íntegro finito es un campo.

Demostración. Como D es un dominio íntegro finito, D ya es un anillo conmutativo y unitario, por tanto, lo único que nos falta probar es que para todo elemento no nulo su inverso existe.

Sea $a \in D - \{0\}$, entonces mostremos que a es invertible.

Si $a = 1$, 1 es invertible.

Consideremos a $a \neq 0$. Tomemos las potencias de a : $a^1, a^2, a^3, \ldots$.

Existen i, j con $i > j$ tal que $a^i = a^j$, ya que D es finito, entonces:

$$a^{i-j} = a^i a^{-j} = a^j a^{-j} = 1$$

Así, el inverso de a es a^{i-j-1}, pues $a(a^{i-j-1}) = 1$. □

Observación. 1. A partir de los Teoremas 1.10 y 1.11 tenemos que, para p primo, $\mathbb{Z}/p$ es un campo.

2. Los campos $\mathbb{Z}/p\mathbb{Z}$ y $\mathbb{Z}/p$ que se construyen en apariencias diferentes resultan ser algebraicamente iguales.

Ejemplo. Los campos $\mathbb{Z}/3\mathbb{Z}$ y $\mathbb{Z}/3$ son algebraicamente iguales.

Solución. Mostremos como son los elementos de cada campo.

1. $\mathbb{Z}/3\mathbb{Z} = \{a + pk \mid k \in \mathbb{Z}\} = \{a + 3k \mid k \in \mathbb{Z}\}$. Entonces:

   $0 + 3\mathbb{Z} = \{0 + 3k \mid k \in \mathbb{Z}\} = \{\ldots, \text{-6, -3, 0, 3, 6}, \ldots\}$

   $1 + 3\mathbb{Z} = \{1 + 3k \mid k \in \mathbb{Z}\} = \{\ldots, \text{-5, -2, 1, 4, 7}, \ldots\}$

   $2 + 3\mathbb{Z} = \{2 + 3k \mid k \in \mathbb{Z}\} = \{\ldots, \text{-4, -1, 2, 5, 8}, \ldots\}$

   $3 + 3\mathbb{Z} = \{3 + 3k \mid k \in \mathbb{Z}\} = \{\ldots, \text{-3, 0, 3, 6, 9}, \ldots\} = 0 + 3\mathbb{Z}$

   $4 + 3\mathbb{Z} = \{4 + 3k \mid k \in \mathbb{Z}\} = \{\ldots, \text{-2, 1, 4, 7, 11}, \ldots\} = 1 + 3\mathbb{Z}$

   Así: $\mathbb{Z}/3\mathbb{Z} = \{0 + 3\mathbb{Z}, 1 + 3\mathbb{Z}, 2 + 3\mathbb{Z}\}$

2. $\mathbb{Z}/3 = \{k \in \mathbb{Z} \mid k \equiv a \ (mod\ 3)\}$

   Así, $\mathbb{Z}/3 = \{0, 1, 2\}$

Por tanto, concluimos que $\mathbb{Z}/3\mathbb{Z}$ y $\mathbb{Z}/3$ son algebraicamente iguales.

2

Anillos de Polinomios

Los anillos de polinomios desempeñan un papel esencial en el álgebra abstracta al proporcionar una estructura algebraica que combina las operaciones de suma y multiplicación con el mundo de los polinomios. Comenzaremos por definir de manera rigurosa lo que es un anillo de polinomios y analizaremos cómo sus operaciones se relacionan con las operaciones usuales en el conjunto de polinomios.

2.1 La estructura algebraica de $F[x]$

En este capítulo consideraremos a F un campo. Una expresión de la forma $\sum_{i=0}^{n} a_i x^i = a_0 + a_1 x + \cdots + a_n x^n$ donde n es un entero no negativo y $a_0, a_1, \ldots, a_n$ son elementos en F, la llamaremos un *polinomio con coeficientes en F* en la variable x. Denotaremos por $F[x]$ al conjunto formado por todos los polinomios con coeficientes en un campo F y utilizaremos los símbolos $f(x), g(x), \ldots, etc.$, para denotar los elementos de $F[x]$.

Definición 2.1

Sean $f(x) = \sum_{i=0}^{n} a_i x^i$ y $g(x) = \sum_{i=0}^{n} b_i x^i$ elementos en $F[x]$.

1. $f(x) = g(x)$, si y sólo si, $a_i = b_i$ para todo $i \geq 0$.
2. definimos $(f+g)(x) = \sum_{i=0}^{n} (a_i + b_i) x^i$. Entonces $(f+g)(x)$ es un elemento de $F[x]$.
3. 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 un elemento de $F[x]$.

Ejemplo. Sean $f(x) = 2x^3 + x^2 + 2x + 2$ y $g(x) = 2x^2 + 2x + 1$ polinomios de $\mathbb{Z}/_3[x]$. Determinar $f(x) + g(x)$ y $f(x)g(x)$.

Solución. Notemos que los coeficientes del polinomio $f(x)$ son:
$a_0 = 2, a_1 = 2, a_2 = 1, a_3 = 2, a_4 = 0, a_5 = 0$ y para el polinomio $g(x)$ tenemos:
$b_0 = 1, b_1 = 2, b_2 = 2, b_3 = 0, b_4 = 0, b_5 = 0$.

1.
$$\begin{aligned}(f+g)(x) &= \sum_{i=0}^{3}(a_i + b_i)x^i \\ &= (2+1) + (2+2)x + (1+2)x^2 + (2+0)x^3 \\ &= 3 + 4x + 3x^2 + 2x^3 \\ &= 0 + x + 0 + 2x^2 \\ &= 2x^2 + x.\end{aligned}$$

2.
$$\begin{aligned}(f \cdot g)(x) &= \sum_{i=0}^{5} c_i x^i, \text{ donde } c_k = \sum_{i=0}^{k} a_i b_{k-i} \\ &= (2\cdot 1) + (2\cdot 1 + 2\cdot 2)x + (2\cdot 2 + 2\cdot 2 + 1\cdot 1)x^2 + \\ &+ (2\cdot 0 + 2\cdot 2 + 1\cdot 2 + 2\cdot 1)x^3 + (2\cdot 0 + 2\cdot 0 + 1\cdot 2 + 2\cdot 2 + 0\cdot 1)x^4 + \\ &+ (2\cdot 0 + 2\cdot 0 + 1\cdot 0 + 2\cdot 2 + 0\cdot 2 + 0\cdot 1)x^5 \\ &= 2 + 6x + 9x^2 + 8x^3 + 6x^4 + 4x^5 \\ &= x^5 + 2x^3 + 2.\end{aligned}$$

Lema 2.1
$F[x]$ es un anillo unitario y conmutativo, bajo las operaciones definidas anteriormente.

Demostración.

- $(F[x], +)$ tiene que ser un grupo abeliano.
  Sean $f(x) = \sum_{i=0}^{n} a_i x^i$, $g(x) = \sum_{i=0}^{m} b_i x^i$ y $h(x) = \sum_{i=0}^{p} c_i x^i$ elementos en $F[x]$, con $n \leq m \leq p$.

a) Por definición la suma es cerrada.

b) Asociatividad.

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

c) Elemento neutro.

Para todo $f(x) \in F[x]$ existe el polinomio nulo $p(x) = \sum_{i=1}^{n} 0x_i = 0$ tal que $f(x)+p(x) = f(x)$.

En efecto,

$$\begin{aligned}
f(x)+p(x) &= \sum_{i=0}^{n} a_i x^i + \sum_{i=1}^{n} 0x_i = \sum_{i=0}^{n} (a_i+0)x^i \\
&= \sum_{i=0}^{n} a_i x^i \\
&= f(x).
\end{aligned}$$

d) Elemento inverso.

Como $a_i \in F$, entonces existe el inverso aditivo $-a_i$, lo que implica que para cada $f(x)$ existe $-f(x) \in F[x]$. Así

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

e) Conmutatividad.

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

Por tanto, $(F[x], +)$ es un grupo abeliano.

- $(F[x], \cdot)$ tiene que ser un semigrupo.

  a) Por definición la multiplicación es cerrada.

  b) Asociatividad.

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

  c) Elemento neutro.

  Existe el polinomio $p(x) = 1$, tal que $f(x)p(x) = f(x)$.

En efecto, pues $f(x)p(x) = f(x)1 = f(x)$

d) conmutatividad.

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

- La suma debe ser distributiva respecto al producto, entonces, debemos demostrar que:

$$f(x)(g(x) + h(x)) = f(x)g(x) + f(x)h(x)$$

y

$$(g(x) + h(x))f(x) = g(x)f(x) + h(x)f(x).$$

Entonces:

a)

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

b)

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

Como todas las propiedades se cumplen, entonces concluimos que $F[x]$ es un anillo conmutativo y unitario. □

Definición 2.2

Sea $f(x) = \sum_{i=0}^{n} a_i x^i \in F[x]$ y $a_n \neq 0$.

- Decimos que el grado de $f(x)$ es n, denotado como $\deg(f) = n$ o también por $\deg(f(x)) = n$.
- El coeficiente a_n se llama coeficiente principal del polinomio $f(x)$.

Nota. Para un polinomio $f(x) \in F[x]$ se tiene la equivalencia:

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

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

Teorema 2.1

Si $f(x), g(x)$ son polinomios no nulos de $F[x]$ entonces $\deg(fg) = \deg(f) + \deg(g)$.

Demostración. Sea $n = \deg(f)$ y $m = \deg(g)$ donde:

$f(x) = a_0 + a_1x + \cdots + a_nx^n$ con $a_n \neq 0$ y $g(x) = b_0 + b_1x + b_mx^m$ con $b_m \neq 0$.

De la definición del producto de polinomios tenemos:

$f(x)g(x) = fg(x) = c_0 + c_1 + \cdots + c_{n+m}x^{n+m}$.

Donde $c_{n+m}x^{n+m} = (a_nx^n)(b_mx^m) = a_nb_mx^{n+m}$ con $c_{n+m} \neq 0$ pues $a_n \neq 0$ y $b_m \neq 0$

Así, $\deg(fg) = n + m = \deg(f) + \deg(g)$. □

Corolario 2.1
El anillo $F[x]$ es un dominio íntegro.

Demostración. Como $F[x]$ es un anillo conmutativo y unitario, lo único que nos falta mostrar es que $F[x]$ no tiene divisores de cero.

Sea $f(x) = a_0 + a_1x + \cdots + a_nx^n$ con $a_n \neq 0$ y $g(x) = b_0 + b_1x + \cdots + b_mx^m$ con $b_m \neq 0$.

Multiplicando $f(x)g(x)$ tenemos que el coeficiente principal es $a_nb_m \neq 0$ lo que implica que $f(x)g(x) \neq 0$, es decir, su resultado es distinto del polinomio nulo.

Así, $F[x]$ no tiene divisores de cero. Por tanto, $F[x]$ es un dominio íntegro. □

Observación. Ya que $F[x]$ es un dominio íntegro, de acuerdo a la observación dada en el Teorema 1.8 existe el campo de fracciones de $F[x]$ denotado por $F(x)$. El cual está definido por:

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

2.2 Algoritmo de Euclides

El Algoritmo de Euclides para números enteros dice que, dados dos enteros a, b con $b > 0$, existen únicos enteros q, r tales que $a = bq + r$, donde $0 \leq r < b$. Este resultado también es válido en el anillo de polinomios $F[x]$.

Teorema 2.2 (Algoritmo de la división)
Sean $f(x), g(x) \in F[x]$ con $g(x) \neq 0$ entonces existen únicos polinomio $q(x), r(x) \in F[x]$ tales que $f(x) = g(x)q(x) + r(x)$, donde $r(x) = 0$ ó $\deg(r) < \deg(g)$. El polinomio $r(x)$ se llama resto y $q(x)$ cociente de la división de $f(x)$ por $g(x)$.

Demostración. La demostración la realizaremos por inducción sobre el grado de $f(x)$.

Si $\deg(f) = 0$ entonces $f(x) = a$, podemos considerar $q(x) = 0$ y $r(x) = a$, así,

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

Ahora consideremos:

$$f(x) = a_0 + a_1x + \cdots + a_nx^n \text{ con } a_n \neq 0 \text{ y } g(x) = b_0 + b_1x + b_mx^m \text{ con } b_m \neq 0.$$

Si $n < m$, consideramos $q(x) = 0$ y $r(x) = f(x)$, así,

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

Si $n \geq m$, supongamos por hipótesis de inducción que el teorema es válido para todos los polinomios de grado menor que n.

Consideremos:

$$\begin{aligned} a_nb_m^{-1}x^{n-m}g(x) &= a_nb_m^{-1}x^{n-m}(b_0 + b_1x + b_mx^m) \\ &= a_nb_m^{-1}b_0x^{n-m} + \cdots + a_nx^n. \end{aligned}$$

Entonces, se puede observar que $a_nb_m^{-1}x^{n-m}g(x)$ tiene el mismo grado y coeficiente principal que $f(x)$.

Luego, $f(x) - a_nb_m^{-1}x^{n-m}g(x) = h(x)$ tal que $\deg(h) < \deg(f)$, por hipótsis de inducción existen $q_1(x), r(x)$ tales que:

$$h(x) = q_1(x)g(x) + r(x) \qquad \text{y} \qquad r(x) = 0 \text{ ó } \deg(r) < \deg(g)$$

Con lo cuál, $h(x) = f(x) - a_n b_m^{-1} x^{n-m} g(x) = q_1(x)g(x) + r(x)$,

entonces,

$$\begin{aligned} f(x) &= a_n b_m^{-1} x^{n-m} g(x) + q_1(x)g(x) + r(x) \\ &= (a_n b_m^{-1} x^{n-m} + q_1(x))g(x) + r(x) \\ &= q_2(x)g(x) + r(x). \end{aligned}$$

donde $r(x) = 0$ ó $\deg(r) < \deg(g)$. Así, queda demostrado que existen los polinomios $q(x), r(x)$.

Lo que nos falta mostrar es que $q(x), r(x)$ son únicos.

Supongamos que existen $q(x), r(x), q_1(x), r_1(x) \in F[x]$ tales que:

$$\begin{aligned} f(x) = q(x)g(x) + r(x) \quad &\text{donde} \quad r(x) = 0 \text{ ó } \deg(r) < \deg(g). \\ f(x) = q_1(x)g(x) + r_1(x) \quad &\text{donde} \quad r_1(x) = 0 \text{ ó } \deg(r_1) < \deg(g). \end{aligned}$$

Igualando y agrupando los polinomios tenemos

$$r(x) - r_1(x) = (q_1(x) - q(x))g(x).$$

Supongamos que $r(x) - r_1(x) \neq 0$.

De donde tenemos que:

$$\begin{aligned} \deg(r - r_1) &= \deg((q_1 - q)g) \\ &= \deg(q_1 - q) + \deg(g) > \deg(g). \end{aligned}$$

Pero, por hipótesis $\deg(r) < \deg(g)$ y $\deg(r_1) < \deg(g)$ lo que implica que $\deg(r - r_1) < \deg(g)$. Con lo cual llegamos a una contradicción.

Por tanto, $r(x) = r_1(x)$, luego $0 = (q_1(x) - q(x))g(x)$ de donde obtenemos que $q(x) = q_1(x)$. □

Ejemplo. Sea $f(x) = 3x^4 + x^3 + 2x^2 + 1$ y $g(x) = x^2 + 4x + 2$ en $\mathbb{Z}_5[x]$. Encontrar el cociente $q(x)$ y el resto $r(x)$

Solución. Recordemos que $f(x), g(x)$ están en $\mathbb{Z}_5[x]$.

$$\begin{array}{rrrrr|l}
3x^4 & +x^3 & +2x^2 & & +1 & x^2+4x+2 \\
\cline{6-6}
-3x^4 & +3x^3 & +4x^2 & & & 3x^3+4x \\
\cline{1-3}
 & +4x^3 & +x^2 & & +1 & \\
 & -4x^3 & +x^2 & +2x & & \\
\cline{2-4}
 & & 2x^2 & +2x & +1 &
\end{array}$$

Así, $3x^4+x^3+2x^2+1=(3x^2+4x)(x^2+4x+2)+2x^2+2x+1$.

De donde: $q(x)=3x^2+4x$ y $r(x)=2x^2+2x+1$.

Ejemplo. Sea $f(x)=5x^5-2x^4+2x^3-5x^2+2x+1$ y $g(x)=3x^3+x^2-5x+2$ en $\mathbb{Z}_7[x]$. Encontrar el cociente $q(x)$ y el resto $r(x)$.

Solución. La división es en $\mathbb{Z}_7$

$$\begin{array}{rrrrrr|l}
5x^5 & -2x^4 & +2x^3 & -5x^2 & +2x & +1 & 3x^3+x^2-5x+2 \\
\cline{7-7}
-5x^5 & +3x^4 & +6x^3 & +6x^2 & & & 4x^2+5x+1 \\
\cline{1-4}
 & +x^4 & +x^3 & +x^2 & +2x & & \\
 & -x^4 & +2x^3 & +4x^2 & +4x & & \\
\cline{2-5}
 & & +3x^3 & +5x^2 & +6x & +1 & \\
 & & -3x^3 & +6x^2 & +5x & +5 & \\
\cline{3-6}
 & & & 4x^2 & +4x & +6 &
\end{array}$$

Tenemos que $q(x)=4x^2+5x+1$ y $r(x)=4x^2+4x+6$.

Definición 2.3
Sea $f(x)\in F[x]$ y $\alpha\in F$. Se dice que α es una raíz o un cero de $f(x)$, si $f(\alpha)=0$.

Corolario 2.2
Sea $f(x)\in F[x]$ no nulo y $\alpha\in F$. Entonces, α es una raíz de $f(x)$, si y solo si, existe un polinomio $q(x)\in F[x]$ tal que $f(x)=(x-\alpha)q(x)$.

Demostración. $\Rightarrow$) Si $f(\alpha) = 0$ entonces $f(x) = (x - \alpha)q(x)$.

Por el algoritmo de la división existen $q(x), r(x) \in F[x]$ tal que el polinomio $f(x) = (x - \alpha)q(x) + r(x)$, donde $r(x) = 0$ ó $\deg(r) < \deg(x - \alpha) = 1$.

Dado que $\deg(x - \alpha) = 1$ tenemos $\deg(r) = 0$ por tanto $r(x) = a \in F$.

Luego, como α es una raíz tenemos que $0 = f(\alpha) = (\alpha - \alpha)q(x) + r(x)$ es decir:

$f(\alpha) = r(\alpha) = a = 0$. Así, $f(x) = (x - \alpha)q(x)$

$\Leftarrow$) Si $f(x) = (x - \alpha)q(x)$ entonces $f(\alpha) = 0$.

Como $\alpha \in F$ tenemos:

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

Por tanto, $f(\alpha) = 0$. □

Definición 2.4
Un campo F es algebraicamente cerrado, si todo polinomio de grado $n \geq 1$ en $F[x]$ tiene a lo menos una raíz en F.

Corolario 2.3
Sea F un campo algebraicamente cerrado. $Sif(x) \in F[x]$ y $\deg(f) = n \geq 1$, entonces existen elementos $d, \alpha_1, \alpha_2, \ldots, \alpha_n$ en F tales que:

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

Demostración. La demostración la realizaremos por inducción sobre el grado de $f(x)$.

Si $\deg(f) = 1$, tenemos que $f(x) = ax + b$ con $a \neq 0$, entonces

$$f(x) = ax + b = \underbrace{a}_{d}(x - (\underbrace{-a^{-1}b}_{\alpha})).$$

Supongamos como hipótesis de inducción que el corolario se satisface para todo polinomio de grado menor que n.

Sea $f(x) \in F[x]$ de grado n. Como F es algebraicamente cerrado existe $\alpha_n \in F$ tal que $f(\alpha_n) = 0$, así por el Corolario 2.2, existe $q(x) \in F[x]$ tal que:

$f(x) = (x-\alpha)q(x)$. Luego, como $\deg(q) = n-1$, pues $(x-\alpha)$ tiene grado 1, entonces por la hipótesis de indución, existen $d, \alpha_1, \alpha_2, \ldots \alpha_{n-1}$ tal que:

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

Por tanto,

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

□

Teorema 2.3

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

Demostración. La demostración la realizaremos por inducción sobre el grado del polinomio $f(x)$.

Si $\deg(f) = 1$ tenemos que $f(x) = ax + b$ con $a \neq 0$, entonces la única raíz de $f(x)$ es $\alpha = -a^{-1}b$.

Supongamos como hipótesis de inducción que el teorema se cumple para todo polinomio de grado menor que n.

Sea $\alpha \in F$ una raíz de $f(x)$, entonces por el Corolario 2.2 existe un polinomio $q(x) \in F[x]$ tal que: $f(x) = (x-\alpha)q(x)$ con $\deg(q) = n-1$.

Consideremos $\beta \in F$ una raíz de $f(x)$ tal que $\beta \neq \alpha$.

Entonces, $f(\beta) = (\beta-\alpha)q(\beta) = 0$ implica que $q(\beta) = 0$, luego, las raíces de $f(x)$ son raíces de $q(x)$ y dado que $q(x)$ tiene a lo más $n-1$ raíces, $f(x)$ tiene a lo más n raíces. □

Definición 2.5

Sea $f(x)$ un polinomio con coeficientes en F y $\alpha \in F$. Decimos que α como raíz de $f(x)$ tiene multiplicidad $m \geq 1$, si existe $q(x) \in F[x]$ tal que

$$f(x) = (x-\alpha)^m q(x) \text{ con } q(\alpha) \neq 0.$$

El siguiente teorema que enunciaremos lo admitiremos sin demostración.

Teorema 2.4 (Teorema fundamental del Álgebra)
Si $f(x)$ es un polinomio no constante tal que $f(x) \in \mathbb{C}$, entonces $f(x)$ tiene a lo menos una raíz en $\mathbb{C}$.

La demostración de este teorema se encuentra en ([6], pág. 41).

2.3 Máximo Común Divisor

Teorema 2.5
$F[x]$ es un anillo de ideales principales. Es decir, si J es un ideal de $F[x]$, entonces existe un polinomio $g(x) \in F[x]$ que es un generador de J.

Demostración. Sea J un ideal de $F[x]$. Si $J = \{0\}$, entonces 0 es el generador de J, es decir $J = \langle 0 \rangle$.

Supongamos que $J \neq \{0\}$, sea $g(x) \in J$ un polinomio no nulo de grado minimal. Podemos hacer esta elección, ya que los grados de los polinomios son números enteros, así por el principio del buen orden de los números enteros se garantiza la existencia de este mínimo. Mostremos que $J = \langle g(x) \rangle$.

1. $\langle g(x) \rangle \subseteq J$.

   Sea $h(x) \in \langle g(x) \rangle$ entonces $h(x) = g(x)q(x) \in J$, pues $q(x) \in F[x]$ y $g(x) \in J$. Por tanto, $\langle g(x) \rangle \subseteq J$.

2. $J \subseteq \langle g(x) \rangle$.

   Sea $f(x) \in J$. Por el algoritmo de la división existen $q(x), r(x) \in F[x]$ tales que $f(x) = q(x)g(x) + r(x)$ donde $r(x) = 0$ ó $\deg(r) < \deg(g)$ de donde:

$$r(x) = \underbrace{f(x)}_{\in J} - \underbrace{q(x)g(x)}_{\in J} \in J$$

Como $g(x)$ es un polinomio de grado minimal tenemos que $r(x) = 0$, con lo cual $f(x) = q(x)g(x)$ es decir que $J = \langle g(x) \rangle$. □

Observación. Si $g_1(x)$, $g_2(x)$ son generadores de un ideal no nulo J de $F[x]$, entonces existe un polinomio no nulo $q(x) \in F[x]$ tal que $g_1(x) = g_2(x)q(x)$. Dado que $\deg(g_1) = \deg(g_2) + \deg(q)$, entonces $\deg(g_1) \geq \deg(g_2)$. Utilizando el mismo argumento, obtenemos que $\deg(g_2) \geq \deg(g_1)$. Así, $\deg(g_1) = \deg(g_2)$ y $q(x) = a \in F$ con $a \neq 0$. En consecuencia, $g_1(x) = ag_2(x)$. Si suponemos que $g_1(x) = a_0 + a_1x + \cdots + a_nx^n$ con $a_n \neq 0$, entonces $a_n^{-1}g_1(x)$ es también generador de J. Notemos que $a_n^{-1}g_1(x)$ es de la forma $c_0 + c_1x + \cdots + c_{n-1}x^{n-1} + x^n$, tales polinomios se llaman *mónicos*. De este modo, dado un ideal no nulo J de $F[x]$, siempre podemos encontrar un polinomio mónico que es un generador de J. Este generador es único.

Definición 2.6

Sean $f(x), g(x) \in F[x]$ con $f(x)g(x) \neq 0$. Se dice que $g(x)$ divide a $f(x)$, que se denota $g(x)|f(x)$, si existe un polinomio $h(x) \in F[x]$ tal que

$$f(x) = g(x)h(x).$$

En forma análoga a la definición de máximo común divisor dada para dos números enteros, es posible definir un máximo común divisor para dos polinomios no nulos en el anillo entero $F[x]$.

Definición 2.7

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 solo si,

1. $g(x)|f_1(x)$ y $g(x)|f_2(x)$,

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

Teorema 2.6

Sean $f_1(x), f_2(x) \in F[x]$ 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 $q(x), t(x) \in F[x]$ tales que $g(x) = f_1(x)q(x) + f_2(x)t(x)$.

Demostración.

1. Mostremos que se cumple la primera propiedad de la definición 2.7. Consideremos el ideal $\langle f_(x), f_2(x)\rangle$. Por el Teorema 2.5 $F[x]$ es un anillo de ideales principales, por tanto, existe un polinomio generador $g(x)$ del ideal $\langle f_(x), f_2(x)\rangle$.

   Como $\langle g(x)\rangle = \langle f_1(x), f_2(x)\rangle$ entonces $f_1(x) \in \langle g(x)\rangle$ y $f_2(x) \in \langle g(x)\rangle$ con lo cual existen $q_1(x), q_2(x) \in F$ tales que:

   $f_1(x) = q_1(x)g(x)$ y $f_2(x) = q_2(x)g(x)$

   Por tanto, $g(x)|f_1(x)$ y $g(x)|f_2(x)$.

2. Mostremos que se cumple la segunda propiedad.

   Dado que $\langle g(x)\rangle \in \langle f_(x), f_2(x)\rangle$, existen polinomios $p(x), t(x) \in F[x]$ tales que: $\langle g(x)\rangle = \langle f_1(x)p(x) + f_2(x)t(x)\rangle$.

   Luego, para concluir que $h(x)|g(x)$, supongamos que $h(x)$ es un divisor común de $f_1(x)$ y $f_2(x)$, lo que implica que existen $w(x), z(x) \in F[x]$ tales que:

   $$f_1(x) = h(x)w(x) \text{ y } f_2(x) = h(x)z(x)$$

   Multiplicando $p(x)$ y $t(x)$ respectivamente tenemos que

   $$f_1(x)p(x) = \alpha(x)w(x)p(x) \text{ y } f_2(x)z(x) = h(x)z(x)t(x)$$

   Sumando ambas ecuaciones tenemos:

   $$\begin{aligned} \underbrace{f_1(x)p(x) + f_2(x)z(x)}_{=g(x)} &= h(x)w(x)p(x) + \alpha(x)z(x)t(x) \\ &= h(x)[w(x)p(x) + z(x)t(x)] \end{aligned}$$

   Lo que implica que $h(x)|g(x)$.

□

Observación. Sean $f(x), g(x) \in F[x]$ ambos no nulos. Utilizando el algoritmo de Euclides sucesivamente se tiene que:

$f(x) = g(x)q1(x) + r_1(x)$, donde $r_1(x) = 0$ ó $\deg(r1) < \deg(g)$,

$g(x) = r_1(x)q_2(x) + r_2(x)$, donde $r_2(x) = 0$ 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 $\deg(r_3) < \deg(r_2)$,

$\vdots \qquad\qquad \vdots \qquad\qquad\qquad\qquad \vdots$

$r_{n-1}(x) = r_n(x)q_{n+1}(x) + r_n + 1(x)$, **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. Determinar el máximo común divisor entre los polinomios $f(x) = 2x^3 + 3x^2 + 3x + 2$ y $g(x) = x^2 + 6x + 5$ sobre el campo de los números racionales.

Solución. Utilizaremos el algoritmo de Euclides, así:

$$\begin{array}{rrrr|l} 2x^3 & +3x^2 & +3x & +2 & x^2+6x+5 \\ \cline{5-5} -2x^3 & -12x^2 & -10x & & 2x-9 \\ \cline{1-3} & +9x^2 & -7x & +2 & \\ & -9x^2 & +54x & +45 & \\ \cline{2-4} & & 47x & +47 & \end{array}$$

De donde tenemos que $2x^3 + 3x^2 + 3x + 2 = (x^2 + 6x + 5)(2x - 9) + (47x + 47)$.

Luego,

$$\begin{array}{rrr|l} x^2 & +6x & +5 & 47x+47 \\ \cline{4-4} -x^2 & -x & -10x & \frac{1}{47}x + \frac{5}{47} \\ \cline{2-3} & 5x & +5 & \\ & -5x & -5 & \\ \cline{3-3} & & 0 & \end{array}$$

De donde $x^2 + 6x + 5 = (47x + 47)(\frac{1}{47}x + \frac{5}{47})$

Por tanto, podemos concluir que el máximo común divisor de $f(x)$ y $g(x)$ es el polinomio $h(x) = 47x + 47$.

2.4 Polinomios irreducibles

Definición 2.8

Sea $f(x)$ un polinomio en $F[x]$ con $\deg(f) \geq 1$. El polinomio $f(x)$ se llama *irreducible* en $F[x]$, o irreducible sobre F si no existen polinomios $g(x)$, $h(x) \in F[x]$ tales que:

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

Si tales polinomios existen, $f(x)$ se dice que es *reducible* en $F[x]$, o reducible sobre F.

Ejemplo. El polinomio $f(x) = x^2 + 2$ es irreducible en $\mathbb{R}[x]$.

Notamos que $x^2 + 2 = (x + \sqrt{2}i)(x - \sqrt{2}i)$, con lo cual existen 2 polinomios de grado menor a 2. Pero $\pm\sqrt{2}i \notin \mathbb{R}$ por tanto $f(x) = x^2 + 2$ es irreducible en $\mathbb{R}[x]$.

Ejemplo. El polinomio $f(x) = x^2 + 2$ no es irreducible en $\mathbb{C}[x]$.

Del ejemplo anterior tenemos que: $x^2 + 2 = (x + \sqrt{2}i)(x - \sqrt{2}i)$ donde $\pm\sqrt{2}i \in \mathbb{C}$ y $(x + \sqrt{2}i)$, $(x - \sqrt{2}i)$ son dos polinomios de grado menor a dos. Por tanto, $f(x) = x^2 + 2$ no es irreducible en $\mathbb{C}[x]$.

Ejemplo. El polinomio $f(x) = x^2 - 2$ es irreducible en $\mathbb{Q}[x]$. Factorando el polinomio tenemos: $x^2 - 2 = (x + \sqrt{2})(x - \sqrt{2})$. Pero $\pm\sqrt{2} \notin \mathbb{Q}$. Así, $f(x) = x^2 - 2$ es irreducible en $\mathbb{Q}[x]$.

Lema 2.2

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

Demostración. $\Rightarrow$) Supongamos que $h(x)$ es reducible en $F[x]$, entonces existen $g(x), q(x) \in F[x]$ tal que $h(x) = g(x)q(x)$, donde $g(x) = ax + b$ y $q(x)$ es de grado 1 o 2. Dado que $g(x) = ax + b$ entonces $\alpha = -a^{-1}b$ es una raíz de $h(x)$, pues $h(\alpha) = a(-a^{-1}b) + b = 0$.

$\Leftarrow$) Sea α una raíz de $h(x)$, por el Corolario 2.2 existe un polinomio $q(x) \in F[x]$, tal que $h(x) = (x - \alpha)q(x)$, donde $q(x)$ es de grado 1 o 2. Puesto que hemos encontrado dos polinomios de grado menor al grado de $h(x)$, podemos concluir que $h(x)$ es reducible en $F[x]$. □

Ejemplo. El polinomio $g(x) = x^3 + 4x^2 + 4x + 1 \in \mathbb{Z}_5[x]$ es reducible sobre $\mathbb{Z}/5$. Por el lema anterior debemos mostrar que $g(x)$ tenga alguna raíz en $\mathbb{Z}/5$.

$$g(0) = 0 + 0 + 0 + 1 = 1$$
$$g(1) = 1 + 4 + 4 + 1 = 5 + 5 = 0 + 0 = 0$$

Como $\alpha = 1$ es una raíz de $g(x)$, tenemos que $g(x)$ es reducible sobre $\mathbb{Z}/5$.

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

Por el Lema 2.2 podemos afirmar que si $p(x)$ no tiene una raíz entonces este es irreducible. Así,

$$p(0) = 0 + 0 + 2 = 0$$
$$p(1) = 1 + 1 + 2 = 4 = 1$$
$$p(2) = 8 + 4 + 2 = 2 + 1 + 2 = 2$$

Como $p(x)$ no tiene raíces concluimos que $p(x)$ es irreducible sobre $\mathbb{Z}/3$.

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.

El teorema es equivalente a tener: Sea $p(x) \in F[x]$ con $\deg(p) \geq 1$. Entonces, $\langle p(x) \rangle$ no es un ideal maximal de $F[x]$, si y sólo si, $p(x)$ es reducible sobre F.

Demostración. $\Rightarrow$) Supongamos que $\langle p(x) \rangle$ no es un ideal maximal de $F[x]$. Entonces existe un ideal $J \in F[x]$ 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 anillo de ideales principales, existe $g(x) \in F[x]$ tal que $J = \langle g(x) \rangle$, dado que $\langle p(x) \rangle \subset J$ entonces $\langle p(x) \rangle \subset \langle g(x) \rangle$. Así:

$$\text{Si } g(x) \text{ es constante, entonces } J = F[x].$$
$$\text{Si } h(x) \text{ es constante, entonces } J = \langle p(x) \rangle.$$

En ambos casos llegamos a una contradicción, ya que por hipótesis $\langle p(x) \rangle \neq J$ y $J \neq F[x]$. Con lo cual vemos que necesariamente $\deg(g) \geq 1$ y $\deg(h) \geq 1$. Por tanto, $p(x) = g(x)h(x)$ con $\deg(g) < \deg(p)$ y $\deg(h) < \deg(p)$, así, $p(x)$ es reducible.

$\Leftarrow$) Supongamos que $p(x)$ es reducible sobre $F[x]$. Entonces $p(x) = g(x)h(x)$ con $\deg(g) < \deg(p)$ y $\deg(h) < \deg(p)$, además $\deg(g) > 0$ y $\deg(h) > 0$, de lo contrario $\deg(g) = \deg(p)$ ó $\deg(h) = \deg(p)$. Como $p(x) = g(x)h(x)$ tenemos $\langle p(x) \rangle \subset \langle g(x) \rangle$ y $\langle g(x) \rangle \neq F[x]$, pues $1 \notin \langle g(x) \rangle$ ya que $\deg(g) > 0$. También $g(x) \notin \langle p(x) \rangle$, pues si suponemos que $g(x) \in \langle p(x) \rangle$ entonces:

$g(x) = p(x)q(x)$ con $q(x) \in F[x]$.

Así, $p(x) = g(x)h(x) = p(x)q(x)h(x)$, entonces $p(x) = p(x)q(x)h(x)$ de donde obtenemos que $q(x)h(x) = 1$. Esto implica que $\deg(q) = \deg(h) = 0$, lo cual es una contradicción, ya que $\deg(h) > 0$. Entonces $g(x) \in \langle p(x) \rangle$.

Por tanto, $\langle g(x) \rangle \neq \langle p(x) \rangle$ es decir, $\langle p(x) \rangle$ no es maximal. □

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. $\Rightarrow$) Si $p(x)$ es irreducible, entonces por el Teorema 2.7, $\langle p(x) \rangle$ es un ideal maximal de $F[x]$, luego por el Teorema 1.4, $F[x]/\langle p(x) \rangle$ es un campo.

$\Leftarrow$) Si $F[x]/\langle p(x) \rangle$ es un campo, entonces por el Teorema 1.4 $\langle p(x) \rangle$ es un ideal maximal de $F[x]$. Luego, por el Teorema 2.7 $p(x)$ es irreducible en $F[x]$. □

Lema 2.3
Sea F campo, $p(x) \in F[x]$ irreducible sobre F y $\deg(p)=n$. Entonces $F[x]/\langle p(x)\rangle = \{a_0 + a_1x + \cdots + a_{n-1}x^{n-1} + \langle p(x)\rangle \mid a_0, a_1, \ldots, a_{n-1} \in F\}$.

Demostración. Sea $f(x) + \langle p(x)\rangle$ un elemento de $F[x]/\langle p(x)\rangle$. Por el algoritmo de la división, existen $q(x), r(x) \in F[x]$ tales que $f(x) = p(x)q(x) + r(x)$, donde $r(x) = 0$ ó $\deg(r) < \deg(p)$. Luego, $f(x) - r(x) = p(x)r(x) \in \langle p(x)\rangle$. Como $f(x) + \langle p(x)\rangle = r(x) + \langle p(x)\rangle$ con $r(x) = 0$ ó $\deg(r) < n$, entonces $r(x)$ es un polinomio de la forma $a_0 + a_1x + \cdots + a_{n-1}x^{n-1} \in F[x]$.

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

Ejemplo. Sea $p(x) = x^2 + x + 1 \in \mathbb{Z}/5$. Demostrar que el anillo cociente $\mathbb{Z}/5/\langle p(x)\rangle$ es un campo y encontrar el inverso multiplicativo del elemento $x + 1 + \langle p(x)\rangle \in \mathbb{Z}/5/\langle p(x)\rangle$.

Solución. Por el Corolario 2.4, para que $\mathbb{Z}/5/\langle p(x)\rangle$ sea un campo debemos mostrar que $p(x)$ sea irreducible.

Ahora por el Lema 2.2 $p(x)$ es irreducible si $p(x)$ no tiene raíces en $\mathbb{Z}/5$.

Entonces evaluemos los elementos de $\mathbb{Z}/5$ en $p(x)$.

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

Por tanto, podemos concluir que $p(x)$ es irreducible, ya que no tiene raíces en $\mathbb{Z}/5$. Lo que implica que $\mathbb{Z}/5/\langle p(x)\rangle$ es un campo, por lo tanto, es posible encontrar el elemento inverso de $x + 1 + \langle p(x)\rangle$. Ahora por el lema anterior, tenemos que los elementos del campo $\mathbb{Z}/5/\langle p(x)\rangle$ son de la forma $a_0 + a_1x + a_2x^2 + \langle p(x)\rangle$. Así, debemos encontrar:

$$((a_0 + a_1x) + \langle p(x)\rangle)((x + 1) + \langle p(x)\rangle = 1 + \langle p(x)\rangle).$$

Así:

$$\begin{array}{rrr|l} x^2 & +x & +1 & x+1 \\ \cline{4-4} -x^2 & -x & & \mathrm{x} \\ \cline{1-2} & 0 & +1 & \end{array}$$

Entonces:

$$\begin{aligned} x^2+x+1 &= x(x+1)+1+\langle p(x)\rangle \text{ de donde:} \\ 1 &= (x^2+x+1)-x(x+1)+\langle p(x)\rangle \qquad (-1=4 \text{ en } \mathbb{Z}/5) \\ &= (x^2+x+1)+4x(x+1)+\langle p(x)\rangle \\ &= 4x(x+1)+\underbrace{(x^2+x+1)+\langle p(x)\rangle}_{\langle p(x)\rangle} \\ 1 &= 4x(x+1)+\langle p(x)\rangle \end{aligned}$$

De donde concluimos que el inverso multiplicativo de $x+1$ en $\mathbb{Z}/5/\langle p(x)\rangle$ es $4x$.

Definición 2.9

Sea $f(x)=a_0+a_1x+\cdots+a_nx^n \in \mathbb{Z}[x]$.

1. El contenido del polinomio $f(x)$ es el máximo común divisor de $a_0, a_1, \ldots, a_n$.
2. Se dice que $f(x)$ es un polinomio primitivo si el máximo común divisor de $a_0, a_1, \ldots, a_n$ es 1.

Lema 2.4

Si $f(x), g(x) \in \mathbb{Z}[x]$ son polinomios primitivos, entonces $f(x)g(x)$ es un polinomio primitivo.

Demostración. Sean $f(x)=a_0+a_1x+\cdots+a_nx^n$ y $g(x)=b_0+b_1x+\cdots+b_mx^m$ dos polinomios primitivos. Supongamos que $f(x)g(x)$ no es un polinomio primitivo, esto implica que todos los coeficientes de $f(x)g(x)$ serán divisibles por un número entero p. Consideremos un primo p como un divisor de los coeficientes

de $f(x)g(x)$. Como $f(x)$ es primitivo, p no divide a alguno de los coeficientes de a_i, con $i \in \{0, \ldots, n\}$. Sea a_k el primer coeficiente al que p no divide. De manera análoga, sea b_k el primer coeficiente al que p no divide.

En $f(x)g(x)$ el coeficiente de x^{j+k}, es c_{j+k} definida como:

$$c_{j+k} = a_j b_k + (a_{j+1}b_{k-1} + a_{j+2}b_{k-2} + \cdots + a_{j+k}b_0) + (a_{j-1}b_{k+1}a_{j-2}b_{k+2} + \cdots + a_0 b_{j+k}).$$

Luego, por la elección realizada de b_k, tenemos que $p \mid b_{k-1}, b_{k-2}, \ldots$, de modo que $p \mid (a_{j+1}b_{k-1} + a_{j+2}b_{k-2} + \ldots)$. Análogamente, por la elección de a_j tenemos que $p \mid a_{j-1}, a_{j-2}, \ldots$, de modo que $p \mid (a_{j-1}b_{k+1}a_{j-2}b_{k+2} + \cdots + a_0 b_{j+k})$. También, como por suposición $f(x)g(x)$ no es un polinomio primitivo, tenemos que, $p \mid c_{j+k}$, pero esto implica que $p \mid a_j b_k$, lo cual es imposible, ya que $p \nmid a_j$ y $p \nmid b_k$. Por tanto, $f(x)g(x)$ tiene que ser un polinomio primitivo. □

Ejemplo. Sean $f(x) = 1 + 4x^2 + x^3$ y $g(x) = 2 + 3x + x^2$ dos polinomios primitivos en $\mathbb{Q}[x]$, Verificar si $f(x)g(x)$ es un polinomio primitivo.

Solución. Los coeficientes de $f(x)$ son $a_0 = 1, a_2 = 0, a_3 = 1, a_4 = 0, a_5 = 0$ y para $g(x)$ tenemos $b_0 = 2, b_1 = 3, b_2 = 1, b_3 = 0, b_4 = 0, b_5 = 0$. Luego, por definición del producto de polinomios tenemos:

$$\begin{aligned}
f(x)g(x) &= h(x) \\
&= (a_0b_0) + (a_0b_1 + a_1b_0)x + (a_0b_2 + a_1b_1 + a_2b_0)x^2 \\
&+ (a_0b_3 + a_1b_2 + a_2b_1 + a_3b_0)x^3 + (a_0b_4 + a_1b_3 + a_2b_2 + a_3b_1 + a_4b_0)x^4 \\
&+ (a_0b_5 + a_1b_4 + a_2b_3 + a_3b_2 + a_4b_1 + a_5b_0)x^5 \\
&= 2 + (3+0)x + (1+0+8)x^2 + (0+0+12+2)x^3 \\
&+ (0+0+4+3+0)x^4 + (0+0+1+0+0)x^5 \\
&= 2 + 3x + 9x^2 + 14x^3 + 7x^4 + x^5.
\end{aligned}$$

De donde tenemos que el máximo común divisor de $\{2, 3, 9, 14, 7, 1\}$ es 1. Así, $f(x)g(x) = h(x)$ es un polinomio primitivo.

Lema 2.5 (Lema de Gauss)
Si el polinomio primitivo $f(x)$ puede factorizarse como el producto de dos polinomios de coeficientes racionales, entonces puede factorizarse como el producto de dos polinomios con coeficientes enteros.

Demostración. Supongamos que $f(x) = g(x)h(x)$ con $g(x), h(x) \in \mathbb{Q}[x]$. Sea a el mínimo común múltiplo de los denominadores de $g(x)$ y b el mínimo común múltiplo de los denominadores de $h(x)$. Así, tenemos que $abf(x) = ag(x)bh(x)$ con $ag(x), bh(x) \in \mathbb{Z}[x]$. Luego, sea t_1 el contenido de $abf(x)$ y t_2 el contenido de $bg(x)$, de lo cual tenemos que $ag(x) = t_1 g_1(x)$ y $bh(x) = t_2 h_1(x)$. Puesto que $f(x)$ es primitivo, su contenido es ab. Por el lema anterior, $g_1(x), h_1(x)$ son polinomios primitivos, así,

$$ab(f(x)) = t_1 t_2 g_1(x) h_1(x)$$

Lo que implica $ab = t_1 t_2$. Por tanto, $f(x) = g_1(x)h_1(x) \in \mathbb{Z}[x]$. □

Ejemplo. Consideremos el polinomio $f(x) = 6x^2 + x - 2 \in \mathbb{Z}[x]$, el cual es un polinomio primitivo. Ilustremos la demostración del Lema.

Solución. Determinamos una factorización de $f(x)$ en $\mathbb{Q}[x]$.

$$6x^2 + x - 2 = \underbrace{\left(2x + \frac{4}{3}\right)}_{=g(x)} \underbrace{\left(3x - \frac{3}{2}\right)}_{=h(x)}$$

Luego, sacando el mínimo común múltiplo de cada denominador tenemos:

$$(3 \cdot 2)(6x^2 + x - 2) = \underbrace{3\left(2x + \frac{4}{3}\right)}_{=g_1(x)} \underbrace{2\left(3x - \frac{3}{2}\right)}_{=h_1(x)}$$

Determinamos el contenido de $g_1(x), h_1(x)$.

$g_1(x) = 6x + 4$ por tanto, su contenido es 2 con lo cual $g_1(x) = 2(3x + 2)$.

$h_1(x) = 6x - 3$ por tanto, su contenido es 3 con lo cual $g_1(x) = 3(2x - 1)$.

Como $f(x)$ es un polinomio primitivo, entonces $(3 \cdot 2)f(x)$ tiene por contenido $3 \cdot 2$. Así, $(3 \cdot 2)6x^2 + x - 2 = 2(3x + 2)3(2x - 1)$.

Entonces $6x^2 + x - 2 = (3x + 2)(2x - 1)$

Lo cual muestra que $f(x)$ tiene una factorización en $\mathbb{Z}[x]$.

Observación. El lema implica que si un polinomio $f(x) \in \mathbb{Z}[x]$ es reducible en $\mathbb{Q}[x]$, puesto que cumple con la definicíon de reducibilidad, entonces $f(x)$ es reducible en $\mathbb{Z}[x]$.

Teorema 2.8 (Criterio de Schöneman-Eisenstein)
Sea $f(x) = a_0 + a_1x + \cdots + a_nx^n \in \mathbb{Z}[x]$. Si existe un primo p tal que:

1. $p \nmid a_n$ y $p^2 \nmid a_0$.

2. $p \mid a_{n-1}$, $p \mid a_{n-2}, \ldots, p \mid a_0$.

Entonces $f(x)$ es irreducible en $\mathbb{Q}[x]$.

Demostración. Sin pérdida de generalidad podemos suponer que $f(x)$ es un polinomio primitivo, pues al sacar el máximo común divisor de sus coeficientes no se modifica la hipótesis, ya que $p \nmid a$. Supongamos que $f(x)$ se factoriza como un producto de dos polinomios racionales, por el lema de Gauss, se factoriza también como el producto de dos polinomios de coeficientes enteros. Luego, si suponemos que $f(x)$ es reducible, entonces $f(x) = g(x)h(x)$ estará definido como: $f(x) = (b_0 + b_1x + \cdots + b_rx^r)(c_0 + c_1x + \cdots + c_sx^s)$.

Donde, b_i, c_j son enteros y $r > 0$, $s > 0$. Comparando los coeficientes de ambos miembros tenemos que $a_0 = b_0c_0$. Como $p \mid a_0$ entonces $p \mid b_0$ ó $p \mid c_0$. Además, dado que $p^2 \nmid a_0$, p no puede dividir a b_0 y c_0 a la vez. Supongamos que $p \mid b_0$ y que $p \nmid c_0$. No todos los coeficientes b_0, b_r pueden ser divisibles por p; de otro modo todos los coeficientes de $f(x)$ serían divisibles por p, lo que es contradictorio, ya que $p \nmid a_n$. Sea b_k el primer coeficiente de $g(x)$ al que p no divide, con $k < r < n$. Tenemos entonces que $p \mid b_{k-1}$, $p \mid b_{k-2}, \ldots$. Pero $a_k = \sum_{i=0}^{k} b_{k-i}c_i$, y $p \mid a_k$ y $p \mid b_j$ para todo $j \in \{o, 1, \ldots, k-1\}$, de modo que $p \mid b_kc_0$. ya que $p \mid c_0$ y $p \mid b_k$, lo cual es una contradicción. Así, $f(x)$ no puede factorizarse. Por tanto, $f(x)$ es irreducible en $\mathbb{Q}[x]$. □

Ejemplo. El polinomio $f(x) = 16x^5 - 9x^4 + 3x^2 + 6x - 21$ es irreducible en $\mathbb{Q}[x]$.

Solución. Por el criterio de Eisenstein basta con encontrar un primo p tal que se satisfagan las condiciones. Consideremos $p = 3$:

a) $3 \nmid 16$ y $3^2 \nmid$ -21.

b) 3|-9, 3|3, 3|6 y 3|-21

Como las condiciones se cumplen, podemos concluir que $f(x)$ es irreducible en $\mathbb{Q}[x]$.

Ejemplo. El polinomio $f(x) = 3x^5 + 15x^4 - 20x^3 + 10x + 20$ es irreducible sobre $\mathbb{Q}$.

Solución. Por el criterio de Eisenstein basta con encontrar un primo p tal que se satisfagan las condiciones. Consideremos $p = 5$:

a) $5 \nmid 3$ y $5^2 \nmid 20$.

b) 5|15, 5|-20, 5|10 y 5|20

Como las condiciones se cumplen, concluimos que $f(x)$ es irreducible sobre $\mathbb{Q}$.

3

Extensiones de campos

Las extensiones de campos nos permiten ampliar la noción de números y estructuras algebraicas más allá de los campos familiares, como los números racionales o reales. Estas extensiones desvelan conexiones profundas entre distintos campos y tienen aplicaciones cruciales en áreas que van desde la teoría de números hasta la geometría algebraica.

Antes de adentrarnos en el estudio de las extensiones de campos, enunciaremos algunas definiciones del álgebra lineal. Esto nos proporcionará las herramientas esenciales para comprender y analizar las estructuras algebraicas más avanzadas que exploraremos en el contexto de las extensiones de campos.

3.1 Espacios Vectoriales

Definición 3.1 (Espacio vectorial)

Se dice que un conjunto V es un espacio vectorial sobre un campo F si V es un grupo abeliano bajo suma (indicado por $+$) y, si para cada $\alpha \in F$ y $v \in V$, hay un elemento αv en V tal que las siguientes condiciones se cumplen para todo $\alpha, \beta \in F$ y todo $u, v \in V$.

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

Los elementos pertenecientes a un espacio vectorial reciben el nombre de vectores,

mientras que los elementos pertenecientes a un campo se denominan escalares. La operación de combinar un escalar α y un vector v para formar el vector αv se conoce como multiplicación escalar. En general, utilizaremos letras del final del alfabeto como u, v, w para representar los vectores, y letras minúsculas griegas como α, β, γ para representar los escalares.

Definición 3.2 (Subespacio)
Sea V un espacio vectorial sobre un campo F y sea U un subconjunto de V. Se dice que U es un subespacio de V, si U es un espacio vectorial sobre F bajos las operaciones de V.

Definición 3.3
Sea V un espacio vectorial sobre un campo F y $v_1, \ldots, v_n \in V$. Cualquier elemento de la forma $\alpha_1 v_1 + \cdots + \alpha_n v_n$ donde los $\alpha_i \in F$ se llama combinación lineal sobre F de $v_1, \ldots, v_n$.

Definición 3.4 (Independencia lineal)
Sea $S = \{v_1, \ldots, v_n\}$ un conjunto de vectores de V. Si existen $\alpha_1, \ldots, \alpha_n \in F$ de manera que no todos los α_i son ceros y

$$\alpha_1 v_1 + \cdots + \alpha_n v_n = 0$$

entonces S se dice *linealmente dependiente* sobre el campo F.
S se dice *linealmente independiente* sobre el campo F si:

$$\alpha_1 v_1 + \cdots + \alpha_n v_n = 0$$

Implica que $\alpha_1 = \alpha_2 = \cdots = \alpha_n = 0$.

Definición 3.5 (Base)
Sea V un espacio vectorial sobre F. Un subconjunto B de V es llamado base para V si B es linealmente independiente sobre F y todo elemento de V es una combinación lineal de elementos de B (o también B genera todo V).

Definición 3.6 (Dimensión)
Si $\{\alpha_1, \ldots, \alpha_n\}$ es una base del espacio vectorial V, entonces la dimensión de V es n.

3.2 Extensiones Finitas y Algebraicas

La teoría de campos que se estudiara en este capítulo nos permitirá deducir si un problema geométrico se puede resolver utilizando solamente regla y compás. En el capítulo 1 mostramos que $\mathbb{Q}(i) = \{a + bi \mid a, b \in \mathbb{Q}\}$ es un campo. Además se puede observar que $\mathbb{Q}(i)$ contiene a $\mathbb{Q}$. También, vemos a $\mathbb{Q}(i)$ como un espacio vectorial sobre $\mathbb{Q}$. Los vectores $\{1, i\}$ son una base de $\mathbb{Q}(i)$ sobre $\mathbb{Q}$. En efecto, si $a \cdot 1 + bi = 0$ con $a, b \in \mathbb{Q}$, entonces $a = b = 0$. Es decir, los vectores $1, i$ son linealmente independientes sobre $\mathbb{Q}$. Como, $\{a \cdot 1 + bi \mid a, b \in \mathbb{Q}\} = \mathbb{Q}(i)$, entonces los vectores $1, i$ son generadores de $\mathbb{Q}(i)$ como espacio vectorial sobre $\mathbb{Q}$. Por tanto, $\mathbb{Q}(i)$ es un espacio vectorial de dimensión 2 sobre $\mathbb{Q}$.

Si F es un subcampo de un campo K, entonces podemos mirar a K como un espacio vectorial sobre F. Así, en K podemos hablar de vectores linealmente dependientes, vectores linealmente independientes, bases, dimensión, etc.

Definición 3.7
Diremos que K 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 denotamos por $[K : F]$. Adema cuando $[K : F]$ sea finito, diremos que K es una extensión finita.

Ejemplo. $\mathbb{Q}(i)$ es una extensión de $\mathbb{Q}$ y $[\mathbb{Q}(i) : \mathbb{Q}] = 2$.

Puesto que al inicio de este capítulo vimos que el campo $\mathbb{Q}(i)$ contiene al campo $\mathbb{Q}$, implica que $\mathbb{Q}(i)$ es una extensión del campo $\mathbb{Q}$. Además, vimos que $\{1, i\}$ es una base de $\mathbb{Q}(i)$ la cual es finita, pues tiene grado dos, por lo tanto, $[\mathbb{Q}(i) : \mathbb{Q}] = 2$.

Las extensiones de campos muchas veces se indican con diagramas. Si E es una extensión de un campo K y K es una extensión de un campo F, entonces representamos esta situación por:

$$\begin{array}{c} E \\ | \\ K \\ | \\ F \end{array}$$

Teorema 3.1

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

1. Si $[E : K]$ y $[K : F]$ son finitos, entonces $[E : F]$ es finito. Además, $[E : F]=[E : K][K : F]$.

2. Si $[E : F]$ es finito, entonces $[E : K]$ y $[K : F]$ son finitos.

Demostración.

1. Sean $[E : K]=m$ y $[K : F]=n$. Sea $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ una base de K sobre F y $\{\beta_1, \ldots, \beta_m\}$ una base de E sobre K. Basta con mostrar que los mn vectores $\alpha_i\beta_j$, forman una base para E considerado como espacio vectorial sobre F, para que esta primera parte del teorema quede demostrado.

   Recordemos que $\alpha_i\beta_j$ es una base si $\alpha_i\beta_j$ son generadores del espacio vectorial E sobre F y además son linealmente independientes sobre F.

   i) Mostremos que $\alpha_i\beta_j$, son generadores del espacio vectorial E sobre F.

   Sea γ cualquier elemento de E, como los β_j forman una base para E sobre K tenemos

$$\begin{aligned} \gamma &= b_1\beta_1 + b_2\beta_2 + \cdots + b_m\beta_m \\ &= \sum_{j=1}^{m} b_j\beta_j \qquad \text{con } b_j \in K. \end{aligned}$$

Como cada $b_j \in K$ y $\{\alpha_1, \ldots, \alpha_n\}$ es una base de E sobre K, tenemos que para cada b_j existen $a_{1j}, a_{2j}, \ldots, a_{nj}$, así

$$\begin{aligned} b_j &= a_{1j}\alpha_1 + a_{2j}\alpha_2 + \cdots + a_{nj}\alpha_n \\ &= \sum_{i=1}^{n} a_{ij}\alpha_i \qquad \text{con } a_{ij} \in F. \end{aligned}$$

Entonces

$$\begin{aligned} \gamma &= b_1\beta_1 + b_2\beta_2 + \cdots + b_m\beta_m \\ &= (a_{11}\alpha_1 + a_{21}\alpha_2 + \cdots + a_{n1}\alpha_n)\beta_1 + (a_{12}\alpha_1 + a_{22}\alpha_2 + \cdots + a_{n2}\alpha_n)\beta_2 + \\ &+ \cdots + (a_{1m}\alpha_1 + a_{2m}\alpha_2 + \cdots + a_{nm}\alpha_n)\beta_m \\ &= \left(\sum_{i=1}^{n} a_{i1}\alpha_i\right)\beta_1 + \left(\sum_{i=1}^{n} a_{i2}\alpha_i\right)\beta_2 + \cdots + \left(\sum_{i=1}^{n} a_{im}\alpha_i\right)\beta_m \\ &= \sum_{j=1}^{m}\left(\sum_{i=1}^{n} a_{ij}\alpha_i\right)\beta_j \\ &= \sum_{i,j} a_{ij}(\alpha_i\beta_j) \qquad \text{con } a_{ij} \in F. \end{aligned}$$

Con lo cual hemos mostrado que los mn vectores $\alpha_i\beta_j$ generan E sobre F.

ii) Mostremos que los mn vectores $\alpha_i\beta_j$ son linealmente independientes sobre F.

Supongamos que:

$$\sum_{i,j} c_{ij}(\alpha_i\beta_j) = 0 \text{ con} \qquad c_{ij} \in F$$

Entonces

$$\sum_{j=1}^{m}\left(\sum_{i=1}^{n} c_{ij}\alpha_i\right) b_j = 0 \qquad \text{con} \sum_{i=1}^{n} c_{ij}\alpha_i \in K$$

Como los elementos β_j son linealmente independientes sobre K, tenemos que:

$$\sum_{i=1}^{n} c_{ij}\alpha_i = 0 \qquad \text{para todo } j \in \{1, \ldots m\}.$$

Ahora, puesto que α_i son linealmente independientes sobre F, implica que $\sum_{i=1}^{n} c_{ij}\alpha_i = 0$, de donde podemos concluir que $c_{ij} = 0$ para todo

$i \in \{1, \ldots, n\}$ y $j \in \{1, \ldots, m\}$. Por tanto, $\alpha_i \beta_j$ son linealmente independientes.

2. Por hipótesis, $[E : F]$ es finito, dado que K es un subespacio vectorial de E, entonces $[K : F]$ es finito.

   Ahora mostremos que $[E : K]$ es finito.

   Supongamos que $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ una base de E como espacio vectorial sobre F. Para cualquier $\gamma \in E$ tenemos

$$\gamma = \sum_{i=1}^{n} a_i \alpha_i \qquad \text{con } a_i \in F.$$

   Pero, F es un subconjunto de K lo que implica que $a_i \in K$, así

$$\gamma = \sum_{i=1}^{n} a_i \alpha_i \qquad \text{con } a_i \in K.$$

Por lo tanto, los vectores α_n son generadores de E como espacio vectorial sobre K, esto implica que $[E : K]$ es finito. □

Corolario 3.1

Si $F_1, F_2, \ldots, F_r$ 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,

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

Demostración. La demostración la realizamos por inducción.

i) Considerando $r = 3$.

   Por el literal a) del teorema anterior tenemos que F_3 es una extensión finita de F_1 y además,

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

ii) Supongamos que se cumple para $r = i$.

   F_i es una extensión finita de F_1 y

$$[F_i : F_1] = [F_i : F_{i-1}][F_{i-1} : F_{i-2}] \dots\dots [F_2 : F_1].$$

iii) Ahora mostremos que se cumple para $r = i + 1$.

Por hipótesis F_{i+1} es una extensión finita de F_i, luego, por el literal a) del teorema anterior tenemos que F_{i+1} es una extensión finita de F_1 y

$$[F_{i+1} : F_i] \underbrace{[F_{i-1} : F_{i-2}] \dots\dots [F_2 : F_1]}_{[F_i:F_1]} = [F_{i+1} : F_i][F_i : F_1]$$
$$= [F_{i+1} : F_1].$$

Con lo cuál, F_r es una extensión finita de F_1, y además,

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

□

Consideremos el real $\alpha = \sqrt{2} + \sqrt{7}$. Nos interesa encontrar un polinomio no nulo $f(x) \in \mathbb{Q}[x]$ (si es que existe) tal que $f(\alpha) = 0$. Entonces:

$$\alpha^2 = (\sqrt{2} + \sqrt{7})^2 = 2 + 2\sqrt{14} + 7$$
$$\alpha^2 = 9 + 2\sqrt{14}$$
$$\alpha^2 - 9 = 2\sqrt{14}$$
$$(\alpha^2 - 9)^2 = (2\sqrt{14}^2)$$
$$\alpha^4 - 18\alpha^2 + 81 = 56$$
$$\alpha^4 - 18\alpha^2 + 25 = 0.$$

Por tanto, $\alpha = \sqrt{2} + \sqrt{7}$ es una raíz del polinomio $f(x) = x^4 - 18x^2 + 25 \in \mathbb{Q}[x]$. Es decir, α es un número algebraico.

De acuerdo a la definición que sigue, los número algebraicos son los números complejos algebraicos sobre $\mathbb{Q}$.

Definición 3.9

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

Nota. Diremos que K es una extensión algebraica de F, si todo elemento de K es algebraico sobre F.

Ejemplos. 1. $\sqrt{2} \in \mathbb{R}$ es algebraico sobre $\mathbb{Q}$, dado que $\sqrt{2}$ es una raíz del polinomio $f(x) = x^2 - 2 \in \mathbb{Q}[x]$.

2. $\alpha = 1 + i \in \mathbb{C}$ es algebraico sobre $\mathbb{Q}$, dado que $1 + i$ es una raíz del polinomio $f(x) = x^2 - 2x + 2$. En efecto,

$$\begin{aligned} f(x) &= (1+i)^2 - 2(1+i) + 2 \\ &= 1 + 2i - 1 - 2 - 2i + 2 \\ &= 0. \end{aligned}$$

3. Si F es un campo, entonces $\alpha \in F$ es algebraico sobre F.

   En efecto, sea $f(x) = x - \alpha \in F[x]$, luego $f(\alpha) = (\alpha) - \alpha = 0$.

4. $\mathbb{Q}(i) = \{a + bi \mid a, b \in \mathbb{Q}\}$ es una extensión algebraica de $\mathbb{Q}$. Pues, dado que $\mathbb{Q}(i)$ es una extensión del campo $\mathbb{Q}$, nos queda mostrar que todo $z \in \mathbb{Q}(i)$ es algebraico sobre $\mathbb{Q}$.

   Sea $z = a + bi \in \mathbb{Q}(i)$

$$\begin{aligned} z - a &= bi \\ (z-a)^2 &= (bi)^2 \\ z^2 - 2az + a^2 &= -b^2 \\ z^2 - 2az + a^2 + b^2 &= 0. \end{aligned}$$

   Por lo tanto, $z = a + bi$ es una raíz del polinomio $f(x) = x^2 - 2ax + a^2 + b^2$, con lo cual, $\mathbb{Q}(i)$ es una extensión algebraica sobre $\mathbb{Q}$.

Observación. Ya conocemos que los números complejos que son algebraicos sobre $\mathbb{Q}$, son los números algebraicos. En 1844, Liouville demostró que existían números reales trascendentes sobre $\mathbb{Q}$. En 1873, Charles Hermite demostró que el número e es trascendente sobre $\mathbb{Q}$. En 1882, Carl Louis Ferdinand von Lindemann demostró que π es trascendente sobre $\mathbb{Q}$. En 1934, Gelfond y Schneider demostraron, en forma independiente, que si a, b son reales algebraicos sobre $\mathbb{Q}$

y b es irracional, entonces a^b es trascendente sobre $\mathbb{Q}$. Así, $2^{\sqrt{2}}$ es trascendente sobre $\mathbb{Q}$. El descubrimiento de estos números reales trascendentes sobre $\mathbb{Q}$, ha permitido la demostración de la imposibilidad de resolver algunos antiguos problemas geométricos. Dichos problemas serán abordados en el capítulo 4 de esta monografía.

Teorema 3.2
Si K es una extensión finita de un campo F, entonces K es una extensión algebraica sobre F.

Demostración. Sea $[K : F]$=n y α un elemento cualquiera en K. Mostremos que α es algebraico sobre F.

Notemos que $\alpha, \alpha^2, \ldots \alpha^n, \alpha^{n+1}$ son vectores en K. Dado que la dimensión de K como espacio vectorial sobre F es n, entonces por el algebra lineal sabemos que los $n+1$ vectores $\alpha, \alpha^2, \ldots \alpha^n, \alpha^{n+1}$ son linealmente dependientes sobre F. Luego, existen elementos $a_1, a_2, \ldots, a_n, a_{n+1}$ en F, no todos cero, tales que $a_1\alpha + a_2\alpha^2 + \cdots + a_n\alpha^n + a_{n+1}\alpha^{n+1} = 0$. Así, α es una raíz del polinomio $f(x) = a_1x + a_2x^2 + \cdots + a_nx^n + a_{n+1}x^{n+1} \in F[x]$. Por lo tanto α es algebraico sobre F. □

Observación. El reciproco del teorema anterior no es necesariamente válido.

Lema 3.1
Sea K una extensión de un campo F y $\alpha \in K$ algebraico sobre F. Entonces

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

2. Existe un único polinomio mónico $p(x) \in F[x]$ irreducible sobre F tal que $p(\alpha) = 0$.

Demostración.

1. Primero mostremos que en efecto $J = \{f(x) \in F[x] \mid f(\alpha) = 0\}$ es un ideal del anillo de polinomios $F[x]$.

   i) Notemos que $p(x) = 0 = 0 + 0x + \ldots 0x^n$, luego al evaluar α en $p(x)$ tenemos, $p(\alpha) = 0 + 0\alpha + \ldots 0\alpha^n = 0$. Por tanto $0 \in J$.

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

   $$\begin{aligned} f(x) + g(x) &= (f+g)(x) \\ &= f(\alpha) + g(\alpha) \qquad \text{(evaluamos } \alpha\text{)} \\ &= 0 + 0 \in J. \end{aligned}$$

   iii) Sea $h(x) \in F[x]$ y $g(x) \in J$, tenemos

   $$\begin{aligned} h(x)g(x) &= (hg)(x) \\ &= h(\alpha)g(\alpha) \qquad \text{(evaluamos } \alpha\text{)} \\ &= h(\alpha)0 \\ &= 0 \in J. \end{aligned}$$

   Puesto que $F[x]$ es conmutativo, $g(x)h(x) \in J$.

   Por tanto, J es un ideal de $F[x]$.

   Ahora, demostraremos que $q(x)$ es irreducible sobre F. Supongamos que $q(x)$ es reducible sobre F. Existen polinomios $g(x), h(x)$ en $F[x]$ tales que $q(x) = g(x)h(x)$ con $\deg(g) < \deg(q)$ y $\deg(h) < \deg(q)$.

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

   $$\begin{aligned} g(x)(1 - h(x)r(x)) &= g(x) - (g(x)h(x))r(x) \\ &= g(x) - q(x)r(x) = g(x) - g(x) = 0. \end{aligned}$$

   Dado que, $g(x)(1 - h(x)r(x)) = 0, g(x) \neq 0$ y $F[x]$ no tiene divisores del cero, concluimos que $h(x)r(x) = 1$. Luego, $h(x) = a \in F$ con $a \neq 0$ y $r(x) = a^{-1}$. Por lo tanto, $q(x) = g(x)a$, de donde

   $$\deg(q) = \deg(g \cdot a) = \deg(g) + \deg(a) = \deg(g) + 0 = \deg(g)$$

lo que es una contradicciń. 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, $J = \langle p(x) \rangle$. Luego, $p(x)$ es irreducible sobre F, dado que $q(x)$ lo es.

2. Sea $t(x) \in F[x]$ un polinomio irreducible mónico tal que $t(\alpha) = 0$. Entonces $t(x) \in J = \langle p(x) \rangle$ y así, $t(x) = p(x)r(x)$ con $r(x) \in F[x]$. Si $\deg(r) \geq 1$, luego, dado que $\deg(p) = n \geq 1$, se obtiene que $t(x)$ es reducible, una contradicción. Por lo tanto, $\deg(r) = 0$ y así, $r(x) = c \in F$. Como $t(x) = cp(x)$, 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, 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. Encontrar el polinomio irreducible de $\sqrt{3} + \sqrt{7}$ sobre $\mathbb{Q}$.

Solución. Sea $\alpha = \sqrt{3} + \sqrt{7}$, luego

$$\begin{aligned}(\alpha)^2 &= (\sqrt{3} + \sqrt{7})^2 \\ \alpha^2 &= 3 + 2\sqrt{21} + 7 \\ \alpha^2 &= 10 + 2\sqrt{21} \\ (\alpha^2 - 10)^2 &= (2\sqrt{21})^2 \\ \alpha^4 - 20\alpha^2 + 16 &= 0.\end{aligned}$$

Entonces $\alpha = \sqrt{3} + \sqrt{7}$ es una raíz del polinomio $p(x) = x^4 - 20x^2 + 16$.

Nos queda por mostrar que $p(x)$ es irreducible sobre $\mathbb{Q}$.

Supongamos que $p(x)$ es reducible, luego por el Lema de Gauss, $p(x)$ se puede factoriar como el producto de dos polinomios con coeficientes en $\mathbb{Z}$. Así:

$$\begin{aligned} x^4 - 20x^2 + 16 &= (x^2 + ax + b)(x^2 + cx + d) \\ &= x^4 + (a+c)x^3 + (b + d + ac)x^2 + (ad + bc)x + bd. \end{aligned}$$

De donde tenemos

$$\begin{cases} a + c = 0 \\ b + d + ac = -20 \\ ad + bc = 0 \\ bd = 16 \end{cases}$$

De las ecuaciones $ad + bc = 0$ y $a = -c$, tenemos $0 = ad - ab = a(d - b)$.

Si $a = 0$, entonces $b + d + 20 = 0$ y $bd = 16$, luego

$$\begin{aligned} 0 = &\quad b(b + d + 20) \\ = &\quad b^2 + bd + 20b \\ = &\quad b^2 + 20b + 16 \\ = &\quad (b + 10)^2 - 84. \end{aligned}$$

De donde $(b + 10)^2 = 84$ con $b \in \mathbb{Z}$, lo que es una contradicción, puesto que

$$b = \sqrt{84} - 10 \notin \mathbb{Z}.$$

Si $d = b$, entonces $b^2 = 16$, así, $b = 4$ ó $b = -4$.

Si $d = b = 4$, tenemos $d + b + ac = 8 + ac = -20$ con lo cuál $ac = -28$ y como $a = -c$ tenemos que $a^2 = 28$ con $a \in \mathbb{Z}$, lo que es una contradicción, puesto que

$$a = \pm\sqrt{28} \notin \mathbb{Z}.$$

Si $d = b = -4$, tenemos $d + b + ac = -8 + ac = -20$ con lo cuál $ac = -12$ y como $a = -c$ tenemos que $a^2 = 12$ con $a \in \mathbb{Z}$, lo que es una contradicción, puesto que

$$a = \pm\sqrt{12} \notin \mathbb{Z}.$$

Con lo cual vemos que no es posible factorizar $p(x)$. Por tanto, $p(x)$ es irreducible sobre $\mathbb{Q}$.

De esta manera tenemos que el polinomio irreducible de $\sqrt{3}+\sqrt{7}$ es:

$$p(x) = x^4 - 20x^2 + 16.$$

Ejemplo. Encontrar el polinomio irreducible de $\beta = a + bi$ con $a, b \in \mathbb{R}$ y $b \neq 0$ sobre $\mathbb{R}$.

Solución. Tenemos que:

$$\begin{aligned}(\beta - a)^2 &= (bi)^2\\ \beta^2 - 2a\beta + a^2 &= -b^2\\ \beta^2 - 2a\beta + a^2 + b^2 &= 0\end{aligned}$$

Por tanto, β es una raíz del polinomio $p(x) = x^2 - 2ax + a^2 + b^2 = (x-a)^2 + b^2$. Ahora mostremos que $p(x)$ es irreducible sobre $\mathbb{Q}$.

Como $p(x) = (x-a)^2 + b^2$, tenemos que $p(x)$ no tiene raíces, en efecto, ya que $b \neq 0$, tenemos que $b^2 > 0$ y $p(x) > 0$. Al no tener raíces $p(x)$ y dado que su grado es 2, podemos concluir que $p(x)$ es irreducible sobre $\mathbb{Q}$.

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

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

$F[\alpha]$ es un dominio íntegro, su demostración es análoga a como se demuestra que el conjunto $F[x]$ es un dominio íntegro. Denotaremos por $F(\alpha)$ al campo de fracciones de $F[\alpha]$. Luego,

$$F(\alpha) = \left\{ \tfrac{f(\alpha)}{g(\alpha)} \mid f(\alpha), g(\alpha) \in F(\alpha) \text{ y } g(\alpha) \neq 0 \right\}.$$

Además $F(\alpha)$ es el campo más pequeño que contiene a F y α.

Teorema 3.3

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

a) $\phi_\alpha : F[x] \to F[\alpha]$ definida por $\phi_\alpha(f(x)) = f(\alpha)$ para todo $f(x) \in F[x]$, es un homomorfismo de anillos.

b) Si $\alpha \in K$ es trascendente sobre F, entonces $F[x]$ y $F[\alpha]$ son dominios íntegros isomorfos.

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

Demostración. a) Mostremos que en efecto se cumplen las dos propiedades para ser un homomorfismo.

Sean $f(x), g(x) \in F[x]$

i) Adición

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

ii) Producto

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

Por tanto, ϕ_α es un homomorfismo de anillos.

b) Como $\alpha \in K$ es trascendente sobre F, por definición de trascendente sabemos que no existe un polinomio no nulo $f(x) \in F[x]$ tal que $f(\alpha) = 0$. Luego

$$\begin{aligned}\text{Ker}(\phi) &= \{f(x) \in F[x] \mid \phi_\alpha(f(x)) = 0\}\\ &= \{f(x) \in F[x] \mid f(\alpha) = 0\}\\ &= \{0\} \qquad \text{puesto que } \alpha \text{ es trascendente.}\end{aligned}$$

Por el Teorema 1.5 (3) implica que $\phi_\alpha : F[x] \to F[\alpha]$ es una función inyectiva, lo único que nos falta mostrar es que ϕ_α sea sobreyectiva, pero por definición $F[\alpha] = \{f(\alpha) \in F \mid f(x) \in F[x]\}$, lo que nos garantiza que ϕ_α es sobreyectiva, entonces obtenemos que $F[x]$ y $F[\alpha]$ son dominios de integridad isomorfos.

c) Como $\alpha \in K$ es algebraico sobre F y $p(x)$ es el polinomio irreducible de α sobre F, entonces por el Lema 3.1, literal (a), $p(x)$ es un generador del ideal $J = \{f(x) \in F[X] \mid f(\alpha) = 0\}$ del anillo $F[x]$. Dado que $J = \text{Ker}(\phi)$, entonces por el primer teorema de isomorfismo de anillos, los anillos $F[x]/\langle p(x)\rangle$ e $\text{Im}(\phi_\alpha) = F[\alpha]$ son isomorfos. Pero, $F[x]/\langle p(x)\rangle$ es un campo, dado que $p(x)$ es irreducible sobre F. Por lo tanto, $F[\alpha]$ es un campo, luego $F[\alpha]$ es un campo que contiene a F y α, en efecto:

   a) $\alpha \in F[\alpha]$.

   Consideremos el polinomio $f(x) = x \in F[x]$. Entonces, $f(\alpha) = \alpha$ lo que implica que α esta en $F[\alpha]$.

   b) $F \in F[\alpha]$.

   Consideremos cualquier elemento $a \in F$. Podemos representar a como el polinomio constante $f(x) = a$ en $F[x]$. Luego, $f(\alpha) = a$, lo que implica que a está en $F[\alpha]$, con lo cual obtenemos que $F \in F[\alpha]$.

Por tanto $F(\alpha) = F[\alpha]$.

□

Ejemplo. Los campos $\mathbb{Q}(\pi)$ y $\mathbb{Q}(x)$ son isomorfos. En efecto, puesto que $\pi \in \mathbb{R}$ es un elemento trascendente sobre $\mathbb{Q}$, entonces por el teorema anterior, literal b, tenemos que $\mathbb{Q}[\pi]$ y $\mathbb{Q}[x]$ son dominios íntegros isomorfos, lo que implica que sus respectivos campos de fracciones $\mathbb{Q}(\pi)$ y $\mathbb{Q}(x)$ son isomorfos.

Si p es un número primo, por el criterio de Schoneman-Eisenstein, el polinomio $p(x) = x^n - p$ es irreducible sobre $\mathbb{Q}$. El siguiente teorema permitirá afirmar que $\{1, \sqrt[n]{p}, \sqrt[n]{p^2}, \ldots, \sqrt[n]{p^{n-a}}\}$ es una base del campo $\mathbb{Q}(\sqrt[n]{p})$ como espacio vectorial

sobre $\mathbb{Q}$. En consecuencia,

$$\mathbb{Q}(\sqrt[n]{p}) = \{a_0 + a_1\sqrt[n]{p} + \cdots + a_{n-1}\sqrt[n]{p^{n-1}} \mid a_0, a_1, \ldots, a_{n-1} \in \mathbb{Q}\}.$$

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 irreducible 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 $1, \alpha, \ldots, \alpha^{n-1}$. Además, $[F(\alpha) : F] = n$.

Demostración. Debemos demostrar que

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

y que los vectores $1, \alpha, \ldots, \alpha^{n-1}$ son linealmente independientes sobre F.

Denotemos por U al conjunto $\{a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} / a_0, a_1, \ldots, a_{n-1} \in F\}$.

Para demostrar que $F(\alpha) = U$, por el Teorema 3.3, basta probar que $U = F[\alpha]$. Se cumple 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 la división existen polinomios $q(x), r(x)$ en $F[x]$ tales que $f(x) = p(x)q(x) + r(x)$, donde $r(x) = 0$ ó $\deg(r) < \deg(p) = n$. Luego,

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

Pues el $\deg(r) < \deg(p) = n$, lo que implica que el grado de $r(x)$ puede ser a lo más $n - 1$. Por lo tanto,

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

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

Para demostrar que $[F(\alpha) : F] = n$, basta probar que $1, \alpha, \ldots, \alpha^{n-1}$ son linealmente independientes sobre F. Sea $a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} = 0$ con $a_0, a_1, \ldots, a_{n-1} \in F$. Definiendo el polinomio $g(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1}$,

obtenemos que $g(x)$ es un elemento del ideal J de $F[x]$, considerado en el Lema 3.1 (1). Como $J = \langle p(x) \rangle$, existe $q(x) \in F[x]$ tal que $g(x) = p(x)q(x)$.

Si suponemos que $g(x) \neq 0$, entonces $\deg(g) \leq n-1$ y además, $\deg(g) = \deg(p) + \deg(q) = n + \deg(q)$, lo cual implica que $\deg(g) \geq n$, una contradicción. Por lo tanto, $g(x) = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} = 0$, de donde $a_0 = a_1 = \cdots a_{n-1} = 0$. Así, $1, \alpha, \ldots, \alpha^{n-1}$ son linealmente independientes sobre F. □

Sean K una extensión de un campo F y $\alpha, \beta \in K$ 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 de un campo F y $\alpha, \beta \in K$ algebraicos sobre 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. Por el Teorema 3.4, $[F(\alpha) : F]$ 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 un extensión finita de $F(\alpha)$. De esta manera tenemos:

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

Luego, dado que $[F(\alpha, \beta) : F(\alpha)]$ y $[F(\alpha) : F]$ son finitos, del Teorema 3.1 obtenemos que $[F(\alpha, \beta) : F] = [F(\alpha, \beta) : F(\alpha)][F(\alpha) : F]$ es finito. □

Observación. Si en el teorema anterior tenemos que $[F(\alpha) : F] = n$ y que $[F(\alpha)(\beta) : F(\alpha)] = m$, entonces por el Teorema 3.1, $\{1, \ldots, a^{n-1}\}$ es una

base de $F[a]$ sobre F y $\{1, \ldots, \beta^{m-1}\}$ es una base de $F(\alpha)(\beta)$ sobre $F(\alpha)$. Así. $\{\beta^i n^j \mid i \in \{0, \ldots, n-1\},\ j \in \{0, \ldots, m-1\}\}$ es una base de $F(\alpha)(\beta)$ sobre F. Como cada producto $\beta^i \alpha^j \in F(\beta)(\alpha)$, entonces $F(\alpha)(\beta) \subset F(\beta)(\alpha)$. Utilizando el mismo argumento, obtenemos que $F(\beta)(\alpha) \subset F(\alpha)(\beta)$. Por lo tanto, $F(\alpha, \beta) = F(\beta, \alpha)$.

Ahora, si K es una extensión de un campo F y $\alpha_1, \alpha_2, \ldots, a_n \in K$ son algebraicos sobre F, entonces denotaremos

$$F(\alpha_1, \alpha_2) = (F(\alpha_q)(\alpha_2), F(\alpha_1, \alpha_2, \alpha_3) = (F(\alpha_1, \alpha_2))(\alpha_3)$$

y, en general, $F(\alpha_1, \alpha_2, \ldots, \alpha_n) = F(\alpha_1, \alpha_2, \ldots, a_{n-1})(\alpha_n)$.
Además, si $\sigma : \{1, 2, \ldots, n\} \to \{1, 2, \ldots .n\}$ es una biyección, entonces

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

Corolario 3.2
Sea K una extensión de un campo F y $\alpha_1, \alpha_2, \ldots, \alpha_n \in K$ algebraicos sobre F. Entonces $F(\alpha_1, \alpha_2, \ldots, \alpha_n)$ es una extensión finita de F y además,

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

Teorema 3.6
Si E es una extensión finita de un campo F, entonces existen elementos $\alpha_1, \alpha_2, \ldots, \alpha_n \in E$ tales que $E = F(\alpha_1, \alpha_2, \ldots, \alpha_n)$.

Demostración. Si $[E : F] = 1$, entonces $E = F(1) = F$. Si $E \neq F$, entonces existe $\alpha_1 \in E$ tal que $\alpha_1 \notin F$. Como α_1 es algebraico sobre F, entonces por el Teorema 3.4, $[F(\alpha_1) : F]$ 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 se obtiene el teorema. Si $E \neq F(\alpha_1)$, 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, $[F(\alpha_1, \alpha_2) : F] > 2$. Nuevamente, si $E = F(\alpha_1, \alpha_2)$ se obtiene el teorema. Este proceso debe ser finito, de no ser así encontraríamos un conjunto infinito de vectores en E linealmente

independientes sobre F, contradiciendo la hipótesis. En consecuencia, continuando con este proceso, deben existir $\alpha_1, \ldots, \alpha_n \in E$ tales que $E = F(\alpha_1, \ldots, \alpha_n)$. □

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 α un elemento cualquiera en K. Debemos de mostrar que α es algebraico sobre F.

Por hipótesis, K es algebraico sobre E. Luego, existe un polinomio no nulo $g(x) = b_0 + b_1x + \cdots + b_nx^n$ con $b_0, b_1, \ldots, b_n \in E$ tal que $g(\alpha) = 0$. Como E es algebraico sobre F, los elementos $b_0, b_1, \ldots, b_n \in E$ son algebraicos sobre F y por el Corolario 3.2, $F(b_1, b_2, \ldots, b_n)$ es una extensión finita de F. Notemos que $g(x) = b_0 + b_1x + \cdots + b_nx^n \in (F(b_1, b_2, \ldots, b_n))[x]$ y $g(\alpha) = 0$, por lo tanto, α es algebraico sobre $F(b_1, b_2, \ldots, b_n)$ y por el Teorema 3.4, $F(b_1, b_2, \ldots, b_n)(\alpha)$ es una extensión finita de $F(b_1, b_2, \ldots, b_n)$. En consecuencia, tenemos

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

Finalmente, $[F(b_1, b_2, \ldots, b_n)(\alpha) : F(b_1, b_2, \ldots, b_n)]$, $[F(b_1, b_2, \ldots, b_n) : F]$ son finitos, lo que implica que $[F(b_1, b_2, \ldots, b_n)(\alpha) : F]$ es finito. Así, por el Teorema 3.2 α es algebraico sobre F. □

Ejemplo. Se tiene que $p(x) = x^4 - 20x^2 + 16$ es el polinomio irreducible de $\sqrt{3} + \sqrt{7}$ sobre $\mathbb{Q}$, Luego $[\mathbb{Q}(\sqrt{3} + \sqrt{7}) : \mathbb{Q}] = 4$ y $\{1, \sqrt{3} + \sqrt{7}, (\sqrt{3} + \sqrt{7})^2, (\sqrt{3} + \sqrt{7})^3\}$ es una base de $\mathbb{Q}(\sqrt{3} + \sqrt{7})$ como espacio vectorial sobre $\mathbb{Q}$. Por lo tanto, los elementos del campo $\mathbb{Q}(\sqrt{3} + \sqrt{7})$ son de la forma $a + b(\sqrt{3} + \sqrt{7}) + c(\sqrt{3} + \sqrt{7})^2 + d(\sqrt{3} + \sqrt{7})^3$ con $a, b, c, d \in \mathbb{Q}$.

Ejemplo. Demostrar que $[\mathbb{Q}(\sqrt{3},\sqrt{7}):\mathbb{Q}]=4$

Solución. Sabemos que $\mathbb{Q}(\sqrt{3},\sqrt{7})=(\mathbb{Q}(\sqrt{3}))(\sqrt{7})$, así tenemos

$$\begin{array}{c}\mathbb{Q}(\sqrt{3}))(\sqrt{7})\\ |\\ \mathbb{Q}(\sqrt{3})\\ |\\ \mathbb{Q}\end{array}$$

El polinomio irreducible de $\sqrt{3}$ sobre $\mathbb{Q}$ es $q(x)=x^2-3$, luego, $\mathbb{Q}(\sqrt{3})=\{a+b\sqrt{3}\mid a,b\in\mathbb{Q}\}$. Ahora mostremos que el polinomio irreducible de $\sqrt{7}$ sobre $\mathbb{Q}(\sqrt{3})$ es $p(x)=x^2-7$, para ello lo único que debemos mostrar es que $p(x)$ no tiene raíces en $\mathbb{Q}(\sqrt{3})$.

Supongamos que $\alpha=a+b\sqrt{3}$ es una raíz de $p(x)$. Entonces

$$p(\alpha)=(a+b\sqrt{3})^2-7=a^2+2ab\sqrt{3}+3b^2-7=0$$

Como $1,\sqrt{3}$ son linealmente independientes sobre $\mathbb{Q}$, entonces $a^2+3b^2-7=0$ y $2ab\sqrt{3}=0$. Ahora, si $a=0$ entonces $b^2=\frac{7}{3}$ lo que implica que $b=\frac{\sqrt{7}}{\sqrt{3}}\notin\mathbb{Q}$.
Si $b=0$ entonces $a^2=7$ lo que implica que $a=\sqrt{7}\notin\mathbb{Q}$.Por tanto, $p(x)$ no tiene raíces en $\mathbb{Q}(\sqrt{3})$. Así $p(x)$ es el polinomio irreducible de $\sqrt{7}$, con lo cual $[\mathbb{Q}(\sqrt{3}))(\sqrt{7}):\mathbb{Q}(\sqrt{3})]=2$. Luego, como $\{1,\sqrt{3}\}$ es una base de $\mathbb{Q}(\sqrt{3})$ como espacio vectorial sobre $\mathbb{Q}$, entonces $[\mathbb{Q}(\sqrt{3}):\mathbb{Q}]=2$, por el Teorema 3.1

$$\begin{aligned}[\mathbb{Q}(\sqrt{3},\sqrt{7}):\mathbb{Q}]&=[\mathbb{Q}(\sqrt{3}))(\sqrt{7}):\mathbb{Q}(\sqrt{3})][\mathbb{Q}(\sqrt{3}):\mathbb{Q}]\\&=2\cdot 2=4\end{aligned}$$

Además, $\{1,\sqrt{3},\sqrt{7},\sqrt{21}\}$ es una base de $\mathbb{Q}(\sqrt{3}))(\sqrt{7})$ como espacio vectorial sobre $\mathbb{Q}$.

Ejemplo. Demostrar que $\mathbb{Q}(\sqrt{3},\sqrt{7})=\mathbb{Q}(\sqrt{3}+\sqrt{7})$.

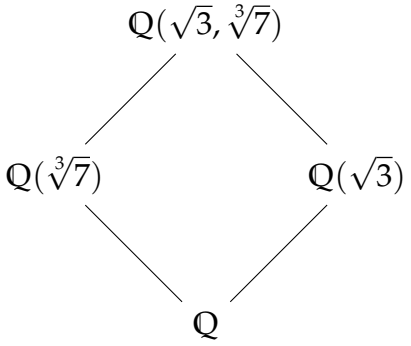
Solución. Vemos que $\sqrt{3}+\sqrt{7}\in\mathbb{Q}(\sqrt{3},\sqrt{7})$ lo que implica que $\mathbb{Q}(\sqrt{3}+\sqrt{7})$ es un subcampo de $\mathbb{Q}(\sqrt{3},\sqrt{7})$. Por los ejercicios anteriores se sabe que

$$[\mathbb{Q}(\sqrt{3}+\sqrt{7}):\mathbb{Q}]=4 \text{ y } [\mathbb{Q}(\sqrt{3},\sqrt{7}):\mathbb{Q}]=4,$$

entonces $[\mathbb{Q}(\sqrt{3},\sqrt{7}):\mathbb{Q}(\sqrt{3}+\sqrt{7})]=1$. Por tanto, $\mathbb{Q}(\sqrt{3},\sqrt{7})=\mathbb{Q}(\sqrt{3}+\sqrt{7})$.

Ejemplo. Demostrar que $\mathbb{Q}(\sqrt{3},\sqrt[3]{7})$ es una extensión finita de grado 6.

Solución. Se sabe que $\mathbb{Q}(\sqrt{3},\sqrt[3]{7})=\mathbb{Q}(\sqrt{3})(\sqrt[3]{7})=\mathbb{Q}(\sqrt[3]{7})(\sqrt{3})$, luego



Tenemos que el polinomio irreducible de $\sqrt{3}$ sobre $\mathbb{Q}$ es $q(x)=x^2-3$ y el polinomio irreducible de $\sqrt[3]{7}$ sobre $\mathbb{Q}$ es $q(x)=x^3-7$. Dado que $\sqrt{3}$ y $\sqrt[3]{7}$ son algebraicos sobre $\mathbb{Q}$, entonces por el Teorema 3.5, $\mathbb{Q}(\sqrt{3},\sqrt[3]{7})$ es un extensión finita de $\mathbb{Q}$. Utilizando el Teorema 3.1, obtenemos que 2 y 3 son divisores de $[\mathbb{Q}(\sqrt{3},\sqrt[3]{7}):\mathbb{Q}]$. Por lo tanto, $[\mathbb{Q}(\sqrt{3},\sqrt[3]{7}):\mathbb{Q}]\geq 6$. El polinomio $q(x)=x^3-7\in\mathbb{Q}(\sqrt{3})[x]$ se anula en $\sqrt[3]{7}$, luego el polinomio irreducible de $\sqrt[3]{7}$ es un divisor de $q(x)$. Por lo tanto, $[\mathbb{Q}(\sqrt{3}),\sqrt[3]{7}):\mathbb{Q}(\sqrt{3})]\leq 3$.

Utilizando nuevamente el Teorema 3.1, concluimos que

$$[\mathbb{Q}(\sqrt{3},\sqrt[3]{7}):\mathbb{Q}]=[\mathbb{Q}(\sqrt{3}),\sqrt[3]{7}):\mathbb{Q}(\sqrt{3})][\mathbb{Q}(\sqrt{3}):\mathbb{Q}]\geq 6.$$

Por lo tanto, $[\mathbb{Q}(\sqrt{3},\sqrt[3]{7}):\mathbb{Q}]=6$. Además obtenemos que $q(x)=x^3-7$ es el polinomio irreducible de $\sqrt[3]{7}$ sobre $\mathbb{Q}(\sqrt{3})$. Así, $\{1,\sqrt[3]{7},\sqrt[3]{49}\}$ es una base de $\mathbb{Q}(\sqrt{3},\sqrt[3]{7})$ sobre $\mathbb{Q}(\sqrt{3})$. Como $\{1,\sqrt{3}\}$ es una base de $\mathbb{Q}(\sqrt{3})$ sobre $\mathbb{Q}$, entonces obtenemos que $\{1,\sqrt[3]{7},\sqrt[3]{49},\sqrt{3},\sqrt{3}\sqrt[3]{7},\sqrt{3}\sqrt[3]{49}\}$ es una base $\mathbb{Q}(\sqrt{3},\sqrt[3]{7})$ sobre $\mathbb{Q}$.

Ejemplo. Demostrar que $\mathbb{Q}(\sqrt{3}+\sqrt[3]{7})=\mathbb{Q}(\sqrt{3},\sqrt[3]{7})$ y encontrar el polinomio irreducible de $\sqrt{3}+\sqrt[3]{7}$ sobre $\mathbb{Q}$.

Solución. Observamos que $\sqrt{3}+\sqrt[3]{7}$ es un elemento en el campo $\mathbb{Q}(\sqrt{3},\sqrt[3]{7})$. Luego, $\mathbb{Q}(\sqrt{3}+\sqrt[3]{7})$ es un subcampo de $\mathbb{Q}(\sqrt{3},\sqrt[3]{7})$. Como $\mathbb{Q}(\sqrt{3}+\sqrt[3]{7})$ es un subespacio vectorial de $\mathbb{Q}(\sqrt{3},\sqrt[3]{7})$ y $\mathbb{Q}(\sqrt{3},\sqrt[3]{7})$ es un subespacio vectorial de dimensión 6 sobre $\mathbf{Q}$, entonces $\mathbb{Q}(\sqrt{3}+\sqrt[3]{7})$ es un subespacio vectorial de dimensión finita sobre $\mathbb{Q}$. Luego tenemos

$$[\mathbb{Q}(\sqrt{3},\sqrt[3]{7}):\mathbb{Q}(\sqrt{3}+\sqrt[3]{7})][\mathbb{Q}(\sqrt{3}+\sqrt[3]{7}):\mathbb{Q}]=[\mathbb{Q}(\sqrt{3},\sqrt[3]{7}):\mathbb{Q}]=6.$$

Dado que $\sqrt{3}+\sqrt[3]{7}\notin\mathbb{Q}$, entonces $1<[\mathbb{Q}(\sqrt{3},\sqrt[3]{7}):\mathbb{Q}]\leq 6$.
Así $[\mathbb{Q}(\sqrt{3},\sqrt[3]{7}):\mathbb{Q}]=2,3$ ó 6. Si $[\mathbb{Q}(\sqrt{3},\sqrt[3]{7}):\mathbb{Q}]=2$ entonces, existe un polinomio mónico irreducible $p(x)=x^2+ax+b\in\mathbb{Q}$ tal que:

$$\begin{aligned}p(\sqrt{3}+\sqrt[3]{7}) &= (\sqrt{3}+\sqrt[3]{7})^2+a(\sqrt{3}+\sqrt[3]{7})+b\\ &= b+3+\sqrt[3]{49}+a\sqrt{3}+a\sqrt[3]{7}+2\sqrt{3}\sqrt[3]{7}=0.\end{aligned}$$

Por ejemplos anteriores sabemos que $1,\sqrt[3]{7},\sqrt[3]{49},\sqrt{3},\sqrt{3}\sqrt[3]{7},\sqrt{3}\sqrt[3]{49}$ son linealmente independientes sobre $\mathbb{Q}$. Luego, obtenemos que $1=0$, lo que es una contradicción. Si $[\mathbb{Q}(\sqrt{3}+\sqrt[3]{7}):\mathbb{Q}]=3$, entonces existe un polinomio mónico irreducible de $p(x)=x^3+ax^2+bx+c\in\mathbb{Q}$ tal que:

$$\begin{aligned}p(\sqrt{3}+\sqrt[3]{7}) &= (\sqrt{3}+\sqrt[3]{7})^3+a(\sqrt{3}+\sqrt[3]{7})^2+b(\sqrt{3}+\sqrt[3]{7})+c\\ &= 3\sqrt{3}+9\sqrt[3]{7}+3\sqrt[6]{64827}+7+3a+2\sqrt[6]{1323}a+\sqrt[3]{49}a+\\ &+\sqrt{3}b+\sqrt[3]{7}b+c\\ &= (3a+c+7)+(b+9)\sqrt[3]{7}+a\sqrt[3]{49}+(b+3)\sqrt{3}+\\ &+2a\sqrt{3}\sqrt[3]{7}+2\sqrt{3}\sqrt[3]{49}.\end{aligned}$$

Luego, obtenemos que $2=0$, una contradicción. Entonces, $[\mathbb{Q}(\sqrt{3}+\sqrt[3]{7}):\mathbb{Q}]\neq 3$, así tenemos que $[\mathbb{Q}(\sqrt{3}+\sqrt[3]{7}):\mathbb{Q}]=6$, luego $[\mathbb{Q}(\sqrt{3},\sqrt[3]{7}):\mathbb{Q}(\sqrt{3}+\sqrt[3]{7})]=6$, lo que implica que $\mathbb{Q}(\sqrt{3},\sqrt[3]{7})=\mathbb{Q}(\sqrt{3}+\sqrt[3]{7})$. Ahora nos queda por encontrar el polinomio irreducible de $\sqrt{3}+\sqrt[3]{7}$ sobre $\mathbb{Q}$.

Sea $\alpha = \sqrt{3} + \sqrt[3]{7}$ entonces

$$\begin{aligned}
\alpha - \sqrt{3} &= \sqrt[3]{7} \\
(\alpha - \sqrt{3})^3 &= (\sqrt[3]{7})^3 \\
\alpha^3 - 3\sqrt{3}\alpha^2 + 9\alpha - 3\sqrt{3} &= 7 \\
(\alpha^3 + 9\alpha - 7)^2 &= (3\sqrt{3}\alpha^2 + 3\sqrt{3}) \\
\alpha^6 + 18\alpha^4 - 14\alpha^3 + 81\alpha^2 - 126\alpha + 49 &= 27\alpha^4 + 54\alpha^2 + 27 \\
\alpha^6 - 9\alpha^4 - 14\alpha^3 + 27\alpha^2 - 126\alpha + 22 &= 0.
\end{aligned}$$

Así, $\sqrt{3} + \sqrt[3]{7}$ es una raíz de $p(x) = x^6 - 9x^4 - 14x^3 + 27x^2 - 126x + 22 = 0$.

Necesariamente, $q(x)$ debe ser irreducible sobre $\mathbb{Q}$. En efecto, si suponemos que $q(x)$ no lo es, entonces $[\mathbb{Q}(\sqrt{3} + \sqrt[3]{7}) : \mathbb{Q}] < 6$, lo que contradice lo demostrado anteriormente.

3.3 Raíces de Polinomios Irreducibles

Podemos afirmar que, si F es un subcampo de $\mathbb{C}$ y $p(x) \in F[x]$ es 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 $p(\alpha) = 0$. En efecto, por el Teorema Fundamental del Álgebra, sabemos que existe una raíz $\alpha \in \mathbb{C}$ de $p(x)$. Además, $E = F(\alpha)$ es una extensión finita de F de grado n. La afirmación anterior también es válida para un campo cualquiera F, no necesariamente un subcampo de $\mathbb{C}$, este resultado lo demuestra el siguiente teorema.

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. Puesto que $p(x) \in F[x]$ es un polinomio irreducible sobre F, por el Teorema 2.7 ($\Leftarrow$) $p(x)$ es maximal, entonces el anillo cociente $E = F[x]/\langle p(x)\rangle$ es un campo.

Demostraremos primero que E es una extensión de F. Para ello empezamos demostrando que la función $\sigma : F \to F[x]/\langle p(x)\rangle$ definida por $\sigma(a) = a + \langle p(x)\rangle$ es un monomorfismo.

- Mostremos que σ es un homomorfismo.
  Sean $a, b \in F$.

  1. Adición
  $$\begin{aligned}\sigma(a+b) &= a + b + \langle p(x)\rangle \\ &= (a + \langle p(x)\rangle) + (b + \langle p(x)\rangle) \\ &= \sigma(a) + \sigma(b).\end{aligned}$$

  2. Producto
  $$\begin{aligned}\sigma(ab) &= ab + \langle p(x)\rangle \\ &= (a + \langle p(x)\rangle)(b + \langle p(x)\rangle) \\ &= \sigma(a)\sigma(b).\end{aligned}$$

  Por tanto, σ es un homomorfismo.

- Mostremos que σ es inyectivo, es decir, debemos mostrar que si $\sigma(a) = \sigma(b)$ entonces $a = b$.
  $$\begin{aligned}\sigma(a) &= \sigma(b) \\ a + \langle p(x)\rangle &= b + \langle p(x)\rangle \\ a - b + \langle p(x)\rangle &= 0 + \langle p(x)\rangle.\end{aligned}$$
  De donde obtenemos que $a = b$.

Por tanto, concluimos que σ es un monomorfismo.

Ahora, podemos identificar un elemento cualquiera $a \in F$ con $a + \langle p(x)\rangle \in E$ y escribir $a = a + \langle p(x)\rangle$. Esto nos permite decir que E es una extensión de F.

A continuación mostraremos que E es una extensión finita de grado n sobre F. Del Lema 2.3 tenemos $E = \{a_0 + a_1x + \cdots + a_{n-1}x^{n-1} + \langle p(x)\rangle \mid a_0, \ldots, a_{n-1} \in F\}$. Donde los vectores $1 + \langle p(x)\rangle\, x + \langle p(x)\rangle, \ldots, x^{n-1} + \langle p(x)\rangle$ son generadores de E como espacio vectorial sobre F. Además, estos vectores son linealmente

independientes sobre F. Si suponemos que

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

con $a_0, a_1, \ldots, a_{n-1} \in F$, entonces

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

de donde $a_0+a_1x+\cdots+a_{n-1}x^{n-1} \in \langle p(x)\rangle$. Como $\deg(p)=n$, 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 $p(x)=b_o+b_1x+\cdots+b_nx^n \in F[x]$. Entonces $\alpha=x+\langle p(x)\rangle$ es una raíz de $p(x)$. En efecto:

$$\begin{aligned}
p(\alpha) &= b_o+b_1(x+\langle p(x)\rangle)+\cdots+b_n(x+\langle p(x)\rangle)^n \\
&= b_o+b_1(x+\langle p(x)\rangle)+\cdots+b_n(x^n+\langle p(x)\rangle) \\
&= b_o+b_1x+\cdots+b_nx^n+\langle p(x)\rangle \\
&= p(x)+\langle p(x)\rangle=0+\langle p(x)\rangle=0.
\end{aligned}$$

Por último, como $[F(\alpha):F]=n$, $[E:F]=n$ y $F(\alpha)$ es un subcampo de E, tenemos que $F(\alpha)=E$. □

Corolario 3.3
Sea F un campo y $f(x) \in F[x]$ un polinomio 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 que $f(x)$ es irreducible sobre F o $f(x)$ se puede escribir como el producto de polinomios irreducibles sobre F. Sea $p(x)$ un factor irreducible de $f(x)$. Por el teorema anterior 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 $[E:F] \leq \deg(f)$. □

Ejemplo. Sea $f(x)=x^4-7x^2+10 \in \mathbb{Q}[x]$. Construiremos una extensión E de $\mathbb{Q}$ donde $f(x)$ tenga una raíz. Notemos que $f(x)=(x^2-2)(x^2-5)$ no tiene raíces

en $\mathbb{Q}$. El polinomio $p(x) = x^2 - 2 \in \mathbb{Q}[x]$ es un factor de $f(x)$, irreducible sobre $\mathbb{Q}$. Por el Corolario 2.4, el anillo cociente $E = \mathbb{Q}[x]/\langle x^2 - 2\rangle$ es un campo. Además, E es una extensión finita de $\mathbb{Q}$, $[E : \mathbb{Q}] = \deg(x^2 - 2) = 2$ y $\alpha = x + \langle x^2 - 2\rangle \in E$ es una raís del polinomio $x^2 - 2 \in \mathbb{Q}[x]$, en efecto:

$$\begin{aligned} h(x) &= x^2 - 2 \\ h(\alpha) &= (x + \langle x^2 - 2\rangle)^2 - 2 \\ &= x^2 + \langle x^2 - 2\rangle - 2 \\ &= 0 + \langle x^2 - 2\rangle = 0. \end{aligned}$$

Además α es una raíz de $f(x)$

$$\begin{aligned} f(x) &= (x^2 - 2)(x^2 - 5) \\ f(\alpha) &= ((x + \langle x^2 - 2\rangle)^2 - 2)((x + \langle x^2 - 2\rangle)^2 - 5) \\ &= 0((x + \langle x^2 - 2\rangle)^2 - 5) = 0. \end{aligned}$$

La demostración del Teorema 3.8 nos entrega un método para construir extensiones de un campo F. En el siguiente ejemplo construiremos una extensión finita del campo $\mathbb{Z}/2 = \{\bar{0}, \bar{1}\}$ con 4 elementos. Para simplificar la notación escribiremos $\bar{a} = a$ para $\bar{a} \in \mathbb{Z}/2$.

Ejemplo. El polinomio $p(x) = x^2 + x + 1 \in \mathbb{Z}/2$ es irreducible sobre $\mathbb{Z}/2$ dado que $\deg(p) = 2$ y $p(x)$ no tiene raíces en $\mathbb{Z}/2$, puesto que $p(0) = 1$ y $p(1) = 1$. Por lo tanto, $\langle p(x)\rangle$ es un ideal maximal del anillo $\mathbb{Z}/2[x]$ y en consecuencia, el anillo cociente $E = \mathbb{Z}/2[x]/\langle p(x)\rangle$ es un campo. La función $\sigma : \mathbb{Z}/2 \to E$ definida por $\sigma(a) = a + \langle p(x)\rangle$, es un monomorfismo de anillos. Así podemos identificar $a \in \mathbb{Z}/2$ con $a + \langle p(x)\rangle \in E$ y escribir $a = a + \langle p(x)\rangle$.

Luego $E = \{a + bx + \langle p(x)\rangle \mid a, b \in \mathbb{Z}/2\}$, donde $a = \{0, 1\}$ y $b = \{0, 1\}$. Así, $E = \{0 + \langle p(x)\rangle, 1 + \langle p(x)\rangle, x + \langle p(x)\rangle, 1 + x + \langle p(x)\rangle\}$ De acuerdo a la demostración del teorema anterior, el elemento $\alpha = x + \langle p(x)\rangle$ es una raíz de $p(x)$ y, por lo tanto, $\alpha^2 + \alpha + 1 = 0$. Así, $\alpha^2 = -\alpha - 1 = \alpha + 1$. Luego, $E = 0, 1, \alpha, \alpha + 1$. De esta forma hemos construido un campo con 4 elementos con las siguientes tablas de adición y multiplicación:

$+$	0	1	α	$\alpha+1$
0	0	1	α	$\alpha+1$
1	1	0	$\alpha+1$	α
α	α	$\alpha+1$	0	1
$\alpha+1$	$\alpha+1$	α	1	0

$\cdot$	0	1	α	$\alpha+1$
0	0	0	0	0
1	0	1	α	$\alpha+1$
α	0	α	$\alpha+1$	1
$\alpha+1$	0	$\alpha+1$	1	α

Ejemplo. Utilizando los mismos argumentos del ejemplo anterior, el polinomio $p(x) = x^3 + x + 1 \in \mathbb{Z}/2[x]$ es irreducible sobre $\mathbb{Z}/2$, de donde el anillo cociente $E = \mathbb{Z}/2[x]/\langle p(x)\rangle$ es un campo. Así $E = \{a + bx + cx^2 + \langle p(x)\rangle \mid a, b, c \in \mathbb{Z}/2\}$ con $a = b = c = \{0, 1\}$.

Por tanto,

$E = \{0 + \langle p(x)\rangle, 1 + \langle p(x)\rangle, x + \langle p(x)\rangle, 1 + x + \langle p(x)\rangle, x^2 + \langle p(x)\rangle, 1 + x^2 + \langle p(x)\rangle, x + x^2 + \langle p(x)\rangle, 1 + x + x^2 + \langle p(x)\rangle\}$.

Como $\alpha = x + \langle p(x)\rangle$ es una raíz de $p(x)$, entonces $\alpha^3 + \alpha + 1 = 0$. Así, $\alpha^3 = -\alpha - 1 = \alpha + 1$. Luego, $E = \{0 + 1 + \alpha, \alpha + 1, \alpha^2, \alpha^2 + 1, \alpha^2 + \alpha, \alpha^2 + \alpha + 1\}$. De esta forma hemos construido un campo con 8 elementos con las siguientes tablas de adición y multiplicación:

$+$	0	1	α	$\alpha+1$	α^2	α^2+1	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$
0	0	1	α	$\alpha+1$	α^2	α^2+1	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$
1	1	0	$\alpha+1$	α	α^2+1	α^2	$\alpha^2+\alpha+1$	$\alpha^2+\alpha$
α	α	$\alpha+1$	0	1	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$	α^2	α^2+1
$\alpha+1$	$\alpha+1$	α	1	0	$\alpha^2+\alpha+1$	$\alpha^2+\alpha$	α^2+1	α^2
α^2	α^2	α^2+1	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$	0	1	α	$\alpha+1$
α^2+1	α^2+1	α^2	$\alpha^2+\alpha+1$	$\alpha^2+\alpha$	1	0	$\alpha+1$	α
$\alpha^2+\alpha$	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$	α^2	α^2+1	α	$\alpha+1$	0	1
$\alpha^2+\alpha+1$	$\alpha^2+\alpha+1$	$\alpha^2+\alpha$	α^2+1	α^2	$\alpha+1$	α	1	0

$\cdot$	0	1	α	$\alpha+1$	α^2	α^2+1	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$
0	0	0	0	0	0	0	0	0
1	0	1	α	$\alpha+1$	α^2	α^2+1	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$
α	0	α	α^2	$\alpha^2+\alpha$	$\alpha+1$	1	$\alpha^2+\alpha+1$	α^2+1
$\alpha+1$	0	$\alpha+1$	$\alpha^2+\alpha$	α^2+1	$\alpha^2+\alpha+1$	α^2	1	α
α^2	0	α^2	$\alpha+1$	$\alpha^2+\alpha+1$	$\alpha^2+\alpha$	α	α^2+1	1
α^2+1	0	α^2+1	1	α^2	α	$\alpha^2+\alpha+1$	$\alpha+1$	$\alpha^2+\alpha$
$\alpha^2+\alpha$	0	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$	1	α^2+1	$\alpha+1$	α	α^2
$\alpha^2+\alpha+1$	0	$\alpha^2+\alpha+1$	α^2+1	α	1	$\alpha^2+\alpha$	α^2	$\alpha+1$

3.4 Clausuras Algebraicas

En esta sección se demostrará que el conjunto

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

es una extensión algebraica de $\mathbb{Q}$ y algebraicamente cerrada. Este resultado nos permitirá demostrar que el recíproco del Teorema 3.2 no siempre es válido.

Teorema 3.9

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

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

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

Demostración. Sean $\alpha, \beta \in \overline{F}_E$. Como por hipótesis α, β son algebraicos sobre F, entonces por el Teorema 3.5 tenemos que $F(\alpha, \beta)$ es una extensión finita de F, luego por el Teorema 3.2, $F(\alpha, \beta)$ es una extensión algebraica de F, de donde $F(\alpha, \beta) \subset \bar{F}_E$. Así, $\alpha + \beta$, $-\alpha$, $\alpha\beta$ y α^{-1} con $\alpha \neq 0$ son elementos de $F(\alpha, \beta) \subset \bar{F}_E$. De esta manera, aplicando el Lema 1.3, tenemos que $\bar{F}_E$ es un subcampo de E. □

Observación. Se tiene que $\overline{F}_E = E$, si E es una extensión algebraica de un campo F, cuando E es una extesión finita de F.

Ejemplo. La clausura algebraica de $\mathbb{R}$ en $\mathbb{C}$ es $\mathbb{C}$. En efecto, $a + bi$ con $a, b \in \mathbb{R}$ es una raíz del polinomio $f(x) = x^2 - 2ax + a^2 + b^2 \in \mathbb{R}[x]$.

Teorema 3.10
La clausura algebraica de $\mathbb{Q}$ en $\mathbb{C}$ es un campo algebraicamente cerrado.

Demostración.
Debemos demostrar que el campo $\overline{\mathbb{Q}}_{\mathbb{C}} = \{\alpha \in \mathbb{C} \mid \alpha \text{ es algebraico sobre } \mathbb{Q}\}$ ea algebraicamente cerrado. Denotemos $\overline{\mathbb{Q}} = \overline{\mathbb{Q}}_{\mathbb{C}}$ y sea $f(x) = a_0 + a_1x + \cdots + a_nx^n \in \overline{\mathbb{Q}}[x]$ con $\deg(f) = n$ y $n \geq 1$. Por el Teorema Fundamental del Álgebra, existe un elemento $\alpha \in \mathbb{C}$ tal que $f(\alpha) = 0$. Ahora debemos probar que $\alpha \in \overline{\mathbb{Q}}$. Como $a_0, a_1, \ldots, a_n$ son algebraicos sobre $\mathbb{Q}$, entonces $\mathbb{Q}(a_0, \ldots, a_n)$ es una extensión finita sobre $\mathbb{Q}$, lo que implica que $\mathbb{Q}(a_0, \ldots, a_n)$ es una extensión algebraica sobre $\mathbb{Q}$.

Ahora $f(x) \in \mathbb{Q}(a_0, \ldots, a_n)[x]$ con $f(\alpha) = 0$, es decir, α es algebraico sobre $\mathbb{Q}(a_0, \ldots, a_n)$. Luego, $\mathbb{Q}(a_0, \ldots, a_n, \alpha)$ es una extensión finita de $\mathbb{Q}(a_0, \ldots, a_n)$ y, por lo tanto, $\mathbb{Q}(a_0, \ldots, a_n, \alpha)$ es una extensión algebraica sobre $\mathbb{Q}(a_0, \ldots, a_n)$. Del Teorema 3.7, concluimos que $\mathbb{Q}(a_0, \ldots, a_n, \alpha)$ es una extensión algebraica sobre $\mathbb{Q}$, lo que implica que α es algebraico sobre $\mathbb{Q}$. Así, hemos demostrado que $\alpha \in \overline{\mathbb{Q}}$. □

Observación. Vamos a mostrar que el recíproco del Teorema 3.2 no es válido. En efecto, $\overline{\mathbb{Q}} = \{\alpha \in \mathbb{C} \mid \alpha \text{ es algebraico sobre } \mathbb{Q}\}$ es un campo. Además, $\overline{\mathbb{Q}}$ no es una extensión finita del campo $\mathbb{Q}$. Si suponemos que $[\overline{\mathbb{Q}} : \mathbb{Q}] = n$, entonces $\sqrt[n+1]{2}$ es un elemento en $\overline{\mathbb{Q}}$ y $\sqrt[n+1]{2}$ es una raíz del polinomio $p(x) = x^{n+1} - 1 \in \mathbb{Q}[x]$ y luego, $\mathbb{Q}(\sqrt[n+1]{2}) \subset \overline{\mathbb{Q}}$. Por el criterio de Eisenstein, $p(x)$ es irrediciuble sobre $\mathbb{Q}$. Ahora, $\mathbb{Q}(\sqrt[n+1]{2})$ es una extensión de $\mathbb{Q}$ de grado $n+1$, lo que es una contradicción.

3.5 Derivada de un polinomio

En esta sección daremos una difinición algebraica de la derivada de un polinomio sin hacer uso del concepto de límite, también estudiaremos algunas definiciones que nos permitirá demostrar que si F es un subcampo de los números complejos y $p(x) \in F[x]$ es un polinomio irreducible sobre F de grado n, entonces $p(x)$ tiene n raíces distintas en $\mathbb{C}$.

Definición 3.11

Sea F un campo y $f(x) = a_0 + a_1x + \cdots + a_ix^i + \cdots + a_nx^n \in F[x]$. Entonces la *derivada* de $f(x)$, denotada por $f'(x)$, es el polinomio:

$$f'(x) = a_1 + \cdots + ia_ix^{i-1} + \cdots + na_nx^{n-1} \in F[x].$$

En un curso de cálculo se estudia que, si $f(x)$ es un polinomio con coeficientes reales tal que $f'(x) = 0$, entonces $f(x)$ es una constante. Este resultado no es necesariamente válido cuando consideramos un polinomio con coeficientes en un campo cualquiera. Por ejemplo, si p es un número primo y $f(x) = x^p \in \mathbb{Z}_p[x]$, entonces $f'(x) = px^{p-1}$ es el polinomio nulo, pero como vemos no lo obtuvimos de un polinomio que sea una constante.

Lema 3.2

Sea F un campo y $f(x), g(x) \in F[x]$ 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 $m\mathbb{Z}^+$, entonces $h'(x) = mf(x)^{m-1}f'(x)$.

Demostración.

Sean $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ y $g(x) = b_0 + b_1x + b_2x^2 + \cdots + b_mx^m$ con $n \geq m$.

$$h(x) = (a_0 + b_0) + (a_1 + b_1)x + (a_2 + b_2)x^2 + \cdots + (a_kb_m)x^m + \cdots + a_nx^n.$$

a) Por definición de la derivada de un polinomio tenemos que $f'(x) = a_1 + a_2x + \cdots + na_nx^{n-1}$ y $g'(x) = b_1 + 2b_2x + \cdots + mb_mx^{m-1}$. Por un lado, $h'(x) = (a_1 + b_1) + (a_2 + b_2)x + \cdots + m(a_kb_m)x^{m-1} + \cdots + na_nx^{n-1}$.

Por otro lado, tenemos que:

$$\begin{aligned} f'(x)+g'(x) &= (a_1+a_2x+\cdots+na_nx^{n-1})+(b_1+2b_2x+\cdots+mb_mx^{m-1}) \\ &= (a_1+b_1)+(a_2+b_2)x+\cdots+m(a_kb_m)x^{m-1}+\cdots+na_nx^{n-1} \end{aligned}$$

Con lo cual, tenemos que $h'(x) = f'(x) + g'(x)$.

b) Sea

$$\begin{aligned} h(x) &= \alpha(a_0+a_1x++a_2x^2+\cdots+a_nx^n) \\ &= \alpha a_0+\alpha a_1x+\alpha a_2x^2+\cdots+\alpha a_nx^n \end{aligned}$$

Derivando $h(x)$ tenemos:

$$\begin{aligned} h'(x) &= \alpha a_1+2\alpha a_2x+\cdots+n\alpha a_nx^{n-1} \\ &= \alpha(a_1x+2a_2x+\cdots+na_nx^{n-1}) \\ &= \alpha f'(x). \end{aligned}$$

c) Probaremos en un caso $f(x)= x^n$ y $g(x)= x^m$, donde m, n son enteros positivos. Entonces $h(x) = x^{n+m}$, derivándolo tenemos $h'(x)= (n+m)x^{n+m-1}$. También

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

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

d) Lo realizamos por inducción:

Para $m = 1$. Se tiene que $h(x) = f(x)$, luego por definición de la derivada de un polinomio tenemos qué $h'(x) = f'(x)$.

Suponemos que el resultado se cumple para $m = k$; es decir, suponemos que: si $h(x) = f^k(x)$, entonces $h'(x) = kf^{k-1}(x)f'(x)$.

Ahora probemos que se cumple para $m = k + 1$; es decir, probemos que: si $h(x) = f^{k+1}(x)$, entonces $h'(x) = (k+1)f^k(x)f'(x)$.

En efecto, si $h(x) = f^{k+1}(x)$, entonces $h(x) = f^k(x)f(x)$, derivando tenemos:

$$\begin{aligned} h'(x) &= kf^{k-1}(x)f'(x)f(x)+f^k(x)f'(x) \\ &= kf^k(x)f'(x)+f^k(x)f'(x) \\ &= (k+1)f^k(x)f'(x). \end{aligned}$$

Por tanto, para todo m entero positivo, se tiene que $h'(x) = mf(x)^{m-1}f'(x)$.

□

Teorema 3.11

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

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

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

Corolario 3.4

Sea F un subcampo de los números complejos y $p(x) \in F[x]$ un polinomio mónico irreducible sobre F. Sí $\deg(p) = n$, 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 debemos demostrar es que la multiplicidad de cada raíz de $p(x)$ en $\mathbb{C}$ es 1. Es claro que podemos suponer qué $n > 1$.

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 $m > 1$, de acuerdo al Teorema 3.11, $p'(\alpha) = 0$. Pero $p'(x) \in F[x]$ y $\deg(p') = n - 1 \geq 1$. Así, obtenemos que $p'(x) \in \langle p(x) \rangle$, de donde $\deg(p') \geq \deg(p)$, una contradicción. Por lo tanto, $m = 1$. □

3.6 Campos Finitos

Cuando p es un número primo, sabemos que $\mathbb{Z}_p$ es un campo finito con p elementos. En esta subsección, demostraremos que, si K es un campo finito, entonces K tiene p^n elementos donde p es un número primo y n es algún entero positivo. Recíprocamente, probaremos que, dado un núnmero primo p y un entero positivo n, existe un único campo (salvo isomorfismo) con p^n elementos.

Teorema 3.12
Sea F un campo finito con q elementos y K una extensión finita de F de grado n. Entonces K tiene q^n elementos.

Demostración. Sea $\{\alpha_1, \ldots, \alpha_n\}$ una base de K como espacio vectorial sobre F. Entonces, todo elemento en K tiene una única representación de la forma $c_1\alpha_1 + \cdots + c_n\alpha_n$, donde $c_1, \ldots, c_n$ son elementos en F. Como cada coeficiente $c_i \in F$ puede ser cualquiera de los q elementos de F, entonces el número total de dichas combinaciones lineales distintas de las α_i es q^n. Por tanto, K tiene q^n elementos. □

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. Si K es un campo finito, entonces del Teorema 1.9 (c), 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 3.12, obtenemos que K tiene p^n elementos. □

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. Como 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 $a^{p^n} = a$. □

Corolario 3.6

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

Demostración. De acuerdo al Teorema 2.3, $f(x)$ tiene a lo más p^n raíces en K y por el Lema 3.3, $a_1, \ldots, a_{p^n}$ son todas las raíces en K de $f(x)$. Como $x - a_1$ 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 $i \in \{2, \ldots, p^n\}$ 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 $i \in \{3, \ldots, p^n\}$ 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 $q_{p^n}(x) = 1$. □

Teorema 3.13

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

Demostración. Consideremos el campo de los enteros módulo p, $\mathbb{Z}_p$ 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 $\overline{\mathbb{Z}}_p$ de $\mathbb{Z}_p$.

Sea $K = \left\{\alpha \in \overline{\mathbb{Z}_p} / \alpha^{p^n} = \alpha\right\}$. Demostraremos a continuación que K es un campo con p^n elementos. Utilizaremos el Lema 1.3 para probar que K es un subcampo de $\overline{\mathbb{Z}}_p$. Claramente, 0 y 1 son elementos en K.

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

$$(\alpha - \beta)^{p^n} = \alpha^{p^n} + \sum_{k=1}^{p^n-1} \begin{pmatrix} p^n \\ k \end{pmatrix} \alpha^{p^n-k}(-\beta)^k + (-1)^{p^n}\beta^{p^n}$$

Como la característica de $\overline{\mathbb{Z}_p}$ es p y p es un divisor de $\begin{pmatrix} p^n \\ k \end{pmatrix}$ para todo entero k con $1 \leq k < p^n$, entonces

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

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, si p^n es par, entonces $p = 2$ y como $-1 \equiv 1$ (mód 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 $\left(\alpha^{-1}\right)^{p^n} = \left(\alpha^{p^n}\right)^{-1} = \alpha^{-1}$, lo cual demuestra que $\alpha^{-1} \in K$. De esta forma, hemos demostrado que K es un campo. Finalmente, como $f'(x) = p^n x^{p^n-1} - 1 = -1$, según el Teorema 3.11, las raíces de $f(x)$ son todas distintas y así, K tiene p^n elementos. □

Ejemplo. Construiremos un campo con 3^2 elementos. Nuestro punto de partida será considerar el campo $\mathbb{Z}/3 = \{0, 1, 2\}$. Del Teorema 3.12, debemos encontrar una extensión de $\mathbb{Z}/3$ de grado 2. Consideremos el polinomio $p(x) = x^2 + x + 2$ en $\mathbb{Z}/3[x]$. Como $\deg(p) = 2$ y $p(x)$ no tiene raíces en $\mathbb{Z}/3$, entonces $p(x)$ es irreducible sobre $\mathbb{Z}/3$. Existe una raíz β de $p(x)$ en la clausura algebraica de $\mathbb{Z}/3$ y así, $p(x)$ es el polinomio irreducible de β sobre $\mathbb{Z}/3$. Luego, $\mathbb{Z}/3(\beta)$ es una extensión de $\mathbb{Z}/3$ de grado 2 con 3^2 elementos. Por el Teorema 3.4, tenemos

$$\mathbb{Z}/3(\beta) = \{a + b\beta/a, b \in \mathbb{Z}/3\} = \{0, 1, 2, \beta, \beta + 1, \beta + 2, 2\beta, 2\beta + 1, 2\beta + 2\}.$$

Ejemplo. Encontraremos el polinomio irreducible de $\beta + 1 \in \mathbb{Z}/3(\beta)$ sobre $\mathbb{Z}/3$, donde $\mathbb{Z}/3(\beta)$ es el campo construido en el ejemplo anterior.

Dado que $\mathbb{Z}/3(\beta) = \mathbb{Z}/3(\beta+1)$ y $[\mathbb{Z}/3(\beta), \mathbb{Z}/3] = 2$, entonces el polinomio irreducible de $\beta+1$ sobre $\mathbb{Z}/3$ es de grado 2, el cual es de la forma $q(x) = x^2 + ax + b \in \mathbb{Z}/3[x]$. Deseamos encontrar los valores de $a, b \in \mathbb{Z}/3$ de modo que, $q(\beta+1) = 0$. Como $\beta^2 = -\beta - 2 = 2\beta + 1$, entonces,

$$q(\beta+1) = (\beta+1)^2 + a(\beta+1) + b = a + b + 2 + (a+1)\beta = 0.$$

de donde $a + b + 2 = 0$ y $a + 1 = 0$. Así, $a = b = 2$ y luego, $q(x) = x^2 + 2x + 2$.

Ejemplo. Demostraremos que el polinomio $p(x) = x^3 + 2x + 2 \in \mathbb{Z}/3(\beta)[x]$ es irreducible sobre $\mathbb{Z}/3(\beta)$. Notemos que $\beta^2 = 2\beta + 1$ y $\beta^3 = 2\beta^2 + \beta = 2\beta + 2$. Dado que $\deg(p) = 3$, solo es necesario probar que $p(x)$ no admite raíces en $\mathbb{Z}/3(\beta)$. Supongamos que $a + b\beta$ con $a, b \in \mathbb{Z}/3$ es una raíz de $p(x)$. Entonces

$$\begin{aligned} p(a+b\beta) &= (a+b\beta)^3 + 2(a+b\beta) + 2 = 2a + a^3 + 2 + 2b\beta + b^3\beta^3 \\ &= 2a + a^3 + 2 + 2b\beta + b^3(2\beta+2) = 2a + a^3 + 2b^3 + 2 + 2\left(b + b^3\right)\beta, \end{aligned}$$

de donde $2a + a^3 + 2b^3 + 2 = 0$ y $b + b^3 = 0$. El lector puede verificar que no existen a, $b \in \mathbb{Z}/3$ que verifiquen las relaciones anteriores. Por lo tanto, $p(x)$ es irreducible sobre $\mathbb{Z}/3(\beta)$.

4

Construcciones con Regla y Compás

Los tres problemas geométricos que trataremos en este capítulo, comparten un enunciado simple que cualquier persona ajena a las matemáticas podría entender. Sin embargo, abordar sus demostraciones requiere conocimientos matemáticos más avanzados. Es precisamente en estas demostraciones donde radica el principal interés de este capítulo. A través de este proceso, descubriremos la belleza y profundidad que subyace en estos enunciados aparentemente sencillos y mostraremos la importancia de las matemáticas avanzadas para su resolución.

4.1 Primeras Construcciones

Definición 4.1
Sea S un conjunto de dos o más puntos en el plano.

1. La recta del plano que pasa por dos puntos distintos de S la llamaremos *recta constructible* a partir de S.
2. La circunferencia del plano, cuyo centro es un punto en S y su radio es la distancia entre dos puntos de S, la llamaremos *circunferencia constructible* a partir de S.

Definición 4.2
Construir con regla y compás significa que, a partir de un conjunto S de puntos (por lo menos dos puntos en el plano), se pueden obtener otros puntos, utilizando solo las siguientes operaciones:

1. Intersecando dos rectas constructibles a partir de S. Intersecando una recta

con una circunferencia, ambas constructibles a partir de S.

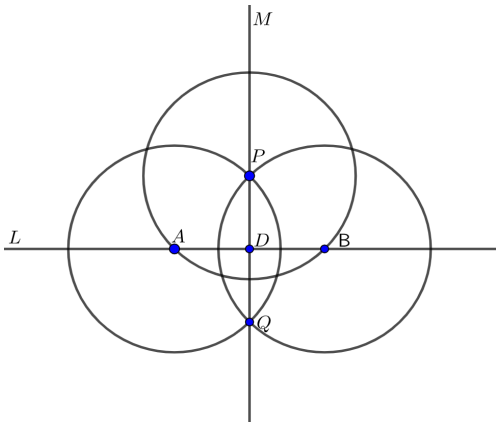
2. Intersecando dos circunferencias constructibles a partir de S.

Nota. Los nuevos puntos que se generan al realizar las operaciones se llaman *puntos constructibles* a partir de S.

Ejemplo. Sea L una recta del plano y P un punto del plano no contenido en L. Construir, solamente usando regla y compás, una recta que pase por un punto P y sea perpendicular a la recta L.

Solución. Consideremos un punto A cualquiera de la recta L, con el compás tracemos una circunferencia de centro P y radio el segmento PA, donde A es un punto de la intersección de L con la circunferencia. Sea B otro punto de intersección de L con la circunferencia. Utilizando el compás, tracemos dos circunferencias de radio AP, de centros A y B respectivamente. Entonces, P es uno de los puntos de intersección de ambas circunferencias. Sea Q el otro punto de intersección de ambas circunferencias. Ahora, con la regla, tracemos la recta M que pasa por los puntos P y Q. Sea D el punto de intersección de las rectas L y M. Donde M será la recta perpendicular buscada.

Figura 1: Recta perpendicular



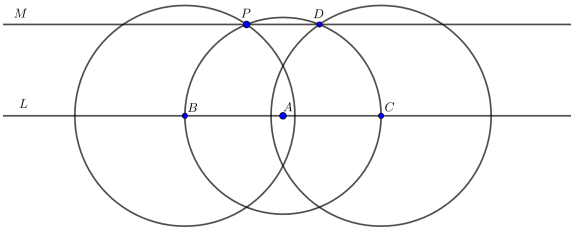
Fuente: Labra, A. & Suazo, A, 2011.

A contunuación demostraremos que los siguientes ejemplos son resolubles con regla y compas.

Ejemplo. Construir una recta que pase por un punto P dado en el plano y que sea paralela a una recta L dada en el plano.

Solución. Consideremos un punto A cualquiera en el plano. Con el compás trazamos una circunferencia de centro A y radio el segmento AP. Los puntos donde se intersecan la circunferencia y la recta L los llamamos B y C respectivamente. Con el compás trazamos una circunferencia de centro B y radio el segmento BP. Nuevamente con el compás trazamos una circunferencia de centro C y radio el segmento BP. La intersección de las circunferencias $\mathscr{C}(A, AP)$ y $\mathscr{C}(C, BP)$ lo llamamos D. Finalmente, con la regla trazamos la recta M que pasa por los puntos P y D, Donde M es la recta perpendicular buscada.

Figura 2: Recta paralela

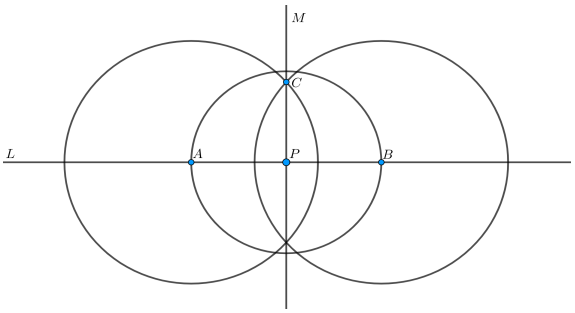


Fuente: Caguas, Wilmer, 2023.

Ejemplo. Dada una recta L y un punto P en ella, construir una recta en el plano que sea perpendicular a L y que pase por el punto P.

Solución. Con el compás trazamos una circunferencia de centro P y un radio r cualquiera. Los puntos de intersección de la circunferencia y la recta L los llamamos A y B respectivamente. Con el compás trazamos una circunferencia de centro A y radio r_1, el cual debe ser de longitud mayor al segmento AP. Nuevamente con el compás trazamos una circunferencia de centro B y radio r_1. El punto en el que se intersecan las dos circunferencias lo llamamos C. Finalmente, con la regla trazamos la recta que pasa por los puntos C y P, a esta recta la denotamos con M, la cual es la recta perpendicular que deseábamos construir.

Figura 3: Recta perpendicular dado un punto en L



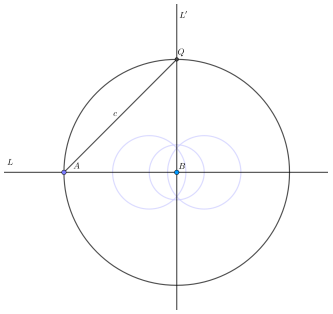
Fuente: Caguas, Wilmer, 2023.

4.2 Números y Campos Constructibles

Ejemplo. Sean A, B dos puntos en el plano, el segmento AB tiene longitud igual a 1, construir un segmento de longitud $\sqrt{2}$.

Solución. Empezamos trazando una recta L que pase por los puntos A y B. Trazamos una recta L' en el plano que sea perpendicular a L y que pase por B, esto lo realizamos utilizando los pasos del último ejemplo de la sección anterior. Con el compás trazamos la circunferencia en el plano de centro B y radio el segmento AB. Sea Q uno de los puntos en los que se intersecan la circunferencia con la recta L'. Por definición de la circunferencia los segmentos AB y BQ tienen longitud 1 y además son perpendiculares. Notemos que el segmento AQ es la hipotenusa de un tríangulo rectángulo. Denotemos por c la longitud del segmento AQ, luego por el teorema de Pitágoras tenemos que la hipotenusa del triángulo AQB es $c = \sqrt{1^2 + 1^2} = \sqrt{2}$.

Figura 4: Construcción de $\sqrt{2}$



Fuente: Caguas, Wilmer, 2023.

Así tenemos que $\sqrt{2}$ es un número que se puede construir con regla y compás, es decir $\sqrt{2}$, es un número constructible.

Definición 4.3
Un número real a se dice que es un *número constructible*, si podemos construir, usando solo regla y compás, un segmento rectilíneo de longitud $|a|$ es un número finito de pasos, a partir de un segmento de longitud unitaria.

Ejemplo. Todo número entero es constructible.

Teorema 4.1
El conjunto de números constructibles forman un subcampo W, del campo de los números reales.

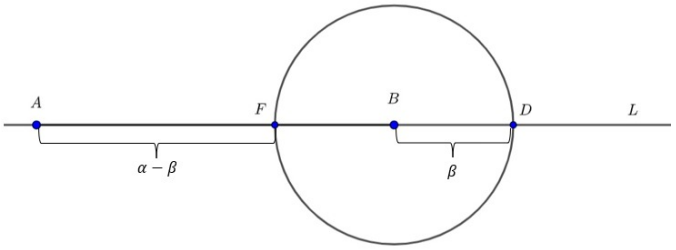
Demostración. Debemos mostrar que el conjunto de números constructibles W cumplen con las propiedades del Lema 1.3.

1. Se tiene que $0, 1 \in W$ por definición de números constructibles.

2. Si $\alpha \in W$, entonces $-\alpha \in W$. En efecto, como existe un segmento de longitud $|\alpha| = |-\alpha|$, entonces $-\alpha \in W$.

   Debemos probar que $\alpha - \beta \in W$. Como los inversos de números constructibles también son números constructibles, basta considerar α, β positivos y demostrar que: $\alpha - (-\beta) = \alpha + \beta$ y $\alpha - \beta$ son constructibles.

Figura 5: $\alpha - \beta$



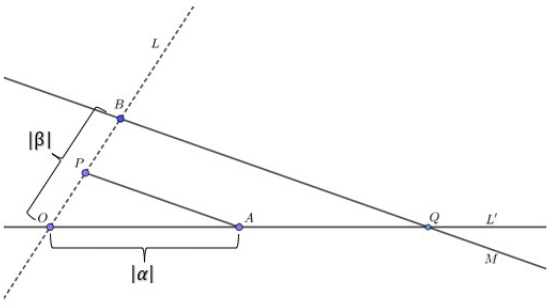
Fuente: Labra, A. & Suazo, A, 2011.

Sean $\alpha, \beta \in W$ reales positivos constructibles. Entonces existe un segmento AB de longitud $|AB| = \alpha$ y un segmento de longitud β. Sea L la recta que contiene al segmento AB. Con el compás tracemos una circunferencia de centro en B y radio un segmento de longitud β. Sean F, D los puntos de intersección de la circunferencia con la recta L, tal que B está entre F y D. el segmento AD tiene longitud $|AD| = \alpha + \beta$.

Nos queda por demostrar que $\alpha - \beta$ es constructible. Supongamos que $\alpha \neq \beta$, de donde $\alpha > \beta$ o $\alpha < \beta$. Si $\alpha > \beta$, entonces F está entre A y B. Así los segmentos FB y BD tienen longitud β. Con lo cual tenemos que el segmento AF tiene longitud $\alpha - \beta$, lo que implica que $\alpha - \beta \in W$, así, $\alpha - \beta$ es constructible. Ahora, sí $\alpha < \beta$, $\beta - \alpha$ es constructible, entonces su inverso $-(\beta - \alpha) \in W$, lo que implica que $\alpha - \beta$ es constructible.

3. Ahora demostraremos que W es cerrado respecto al producto.

Figura 6: Cerradura del producto

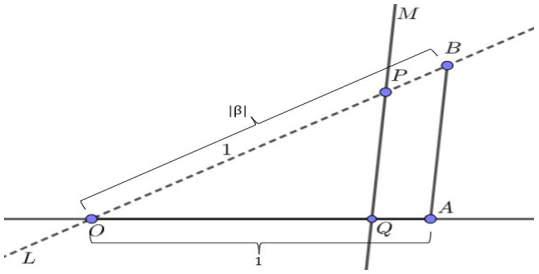


Fuente: Labra, A. & Suazo, A, 2011.

Sean α, β números constructibles, Sea OA un segmento de longitud $|OA| = |\alpha|$ y tracemos una recta L por O que no contenga al segmento OA. Sean P, B puntos en L tales que OP sea de longitud 1 y OB de longitud $|\beta|$. Sea M la recta paralela al segmento PA y que pasa por B. Sea Q el punto de intersección de M con la recta que contiene al segmento OA. Los triángulos OPA y OBQ son semejantes, en consecuencia, $\frac{|OP|}{|OA|} = \frac{|OB|}{|OQ}$. Así, $\frac{1}{|\alpha|} = \frac{|\beta|}{|OQ|}$, de donde $|\alpha\beta| = |OQ|$. Por lo tanto, el segmento OQ es de longitud $|\alpha\beta|$.

4. Nos falta mostrar que los inversos multiplicativos de elementos no nulos en W están en W. Sea β un número constructible no nulo. Sea OA un segmento de longitud $|OA| = 1$ y L una recta que pasa por O no contenida en el segmento OA. Sean B y P puntos de L tales que OB sea de longitud $|\beta|$ y OP de longitud 1. Consideremos la recta M que pasa por P y es paralela al segmento BA, sea Q el punto de intersección de la recta M con la recta que contiene al segmento OA. Los triángulos OQP y OAB son semejantes, puesto que tienen ángulos iguales. Luego, $\dfrac{|OQ|}{|1|} = \dfrac{1}{|\beta|}$. Por lo tanto, OQ es de longitud $\left|\dfrac{1}{\beta}\right|$.

Figura 7: Inverso multiplicativo



Fuente: Labra, A. & Suazo, A, 2011.

□

Observación. Si $\alpha, \beta \in W$ con $\beta \neq 0$, entonces $\alpha\dfrac{1}{\beta} = \dfrac{\alpha}{\beta} \in W$. Como los números enteros son constructibles obtenemos el siguiente corolario.

Corolario 4.1
Cada número racional es constructible.

Ejemplo. Tenemos que $\mathbb{Q}$ es un subcampo de W y como en un ejemplo anterior demostramos que $\sqrt{2} \in W$, entonces los elementos de la forma $a + b\sqrt{2}$ con $a, b \in \mathbb{Q}$ son constructibles. Así, la extensión $\mathbb{Q}(\sqrt{2})$ de $\mathbb{Q}$ es un subcampo de W.

A continuación introduciremos un sistema coordenado cartesiano rectangular en el plano, elegido de modo que el segmento unidad sea un número constructible con regla y compás. Así, tenemos representaciones algebraicas de puntos, rectas y circunferencias.

Ejemplo. Demostrar que$\sqrt{5}$ es un número constructible.

Solución. Consideremos $S = \mathbb{Q} \times \mathbb{Q}$, en las definiciones 4.1 y 4.2. Podemos trazar la circunferencia de centro en el punto $(0, 2)$ y radio, un segmento de longitud 3, lo cual es una operación permitida. Se sabe que la ecuación $x^2 + (y-2)^2 = 9$ representa algebraicamente a la circunferencia anterior. La ecuación de la recta que pasa por los puntos $(0, 0)$ y $(1, 0)$ es $y = 0$. Ahora calcularemos los puntos de intersección de la recta con la circunferencia. Reemplazando $y = 0$ en la ecuación de la circunferencia tenemos:

$$x^2 + (0-2)^2 = 9$$
$$x^2 = 5$$
$$x = \pm\sqrt{5}$$

Con lo cual $P = \left(-\sqrt{5}, 0\right)$ y $Q = \left(\sqrt{5}, 0\right)$ son los puntos de intersección que buscábamos. Así, P, Q son números constructibles a partir de $\mathbb{Q} \times \mathbb{Q}$. La distancia del segmento de extremos $(0, 0)$ y $\left(\sqrt{5}, 0\right)$ tiene longitud $\sqrt{5}$, lo que demuestra que $\sqrt{5}$ es un número constructible.

Sea K un subcampo cualquiera de R y consideremos el conjunto de todos los puntos (x, y) en el plano real euclidiano tales que $x, y \in K$. A dicho conjunto lo llamaremos el plano de K.

Si reemplazamos S por el plano de K, en la definición 4.1, las rectas constructibles y las circunferencias constructibles están en el plano real euclidiano y, por lo tanto, tienen representaciones algebraicas. Utilizando geometría analítica elemental y el hecho que K es un campo, es posible demostrar los siguientes resultados:

Ejemplo. Cualquier recta que pasa por dos puntos distintos del plano de K (esto es, cualquier recta constructible a partir del plano de K) tiene una ecuación de la forma $ax + by + c = 0$, donde $a, b, c \in K$ y a, b no son ambos ceros. Dichas rectas las llamaremos *rectas en* K.

Solución. Sean (m_1, n_1) y (m_2, n_2) dos puntos del plano K, con $m_1, m_2, n_1, n_2 \in K$ De la geometría analítica tenemos la fórmula para calcular la pendiente, la cual

es $p = \dfrac{x_2 - y_1}{x_2 - 1}$, reemplazando tenemos: $\dfrac{n_2 - n_1}{m_2 - m_1} = \dfrac{m}{n} \in K$. Pues $n_2 - n_1 \in K$ y $m_2 - m_1 \in K$, ya que la resta de elemento de K es también un elemento de K. Luego $\dfrac{m}{n} = t$ pues estamos multiplicando $m \in K$ con el inverso de $n \in K$, así $t \in K$.

Utilizamos la ecuación de punto y pendiente donde reemplazaremos los datos para determinar la ecuación buscada.

$$y - y_1 = p\,(x - x_1)$$
$$y - n_1 = t\,(x - m_1)$$
$$y - tx + tm_1 - n_1 = 0$$
$$tx - y + (n_1 - tm_1) = 0$$

Ahora, consideremos $a = t$, $b = -1$ y $c = (n_1 - tm_1)$ de donde obtenemos que $ax + by + c = 0$ con $a, b, c \in K$, pues $t \in K$, $-1 \in K$ y $n_1 - tm_1 \in K$, ya que sus elementos son también elementos de K.

Ejemplo. Cualquier circunferencia que tenga como centro un punto del plano de K y como radio la distancia entre dos puntos del plano de K (es decir, cualquier circunferencia constructible a partir del plano de K), tiene una ecuación de la forma $x^2 + y^2 + ax + by + c = 0$, donde $a, b, c \in K$. Dichas circunferencias las llamaremos *circunferencias en K*.

Solución. Sea (m, n) un punto del plano k, tal que (m, n) es el centro de una circunferencia y t como radio la distancia entre dos puntos del plano de K.

Por la geometría analítica podemos reemplazar los puntos en la ecuación de la circunferencia con centro fuera del origen. Así

$$(x - h)^2 + (y - k)^2 = r^2$$
$$(x - m)^2 + (y - n)^2 = t^2$$
$$x^2 - 2mx + m^2 + y^2 - 2ny + n^2 = t^2$$
$$x^2 + y^2 - 2mx - 2ny + m^2 + n^2 - t^2 = 0$$
$$x^2 + y^2 + ax + by + c = 0$$

donde $a, b, c \in K$ pues $a = -2m \in K$, $b = -2n \in K$ y $c = m^2 + n^2 + t^2 \in K$.

Ejemplo. Dos rectas distintas en K que se intersectan (en el plano real), se intersectan en un punto en el plano de K.

Solución. Sean $r : ax + by + c = 0$ y $t : a_1x + b_1y + c_1 = 0$ dos rectas en el plano de K, con $a, b, c, a_1, b_1, c_1, \in K$.

Calculamos el punto de intersección de las 2 rectas, y despejamos y de la recta t.

$$y = \frac{-a_1x - c_1}{b_1} \quad \text{con} b_1 \neq 0$$
$$y = -\frac{a_1}{b_1}x - \frac{c_1}{b_1}$$

Donde $-\frac{a_1}{b_1} \in K$, pues estamos multiplicando $a_1 \in K$ con el inverso multiplicativo de $b_1 \in K$. De manera análoga $-\frac{c_1}{b_1} \in K$.

Reemplazamos y en la recta r.

$$ax + b\left(-\frac{a_1}{b_1}x - \frac{c_1}{b_1}\right) + c = 0$$
$$ax - \frac{ba_1}{b_1}x - \frac{bc_1}{b_1} + c = 0$$
$$\frac{ab_1 - ba_1}{b_1}x - \frac{bc_1}{b_1} + c = 0$$
$$(ab_1 - ba_1)\, b_1^{-1}x - bc_1b_1^{-1} + c = 0$$

Donde $m = (ab_1 - ba_1)\, b_1^{-1}$ y $n = bc_1b_1^{-1} + c$ son elementos de K, pues estamos multiplicando, restando y sumando elementos de K. Así, $mx - n = 0$, donde $x = \frac{n}{m} = u \in K$.

Reemplazamos el valor de x en y:

$$\begin{aligned} y &= -\frac{a_1}{b_1}u - \frac{c_1}{b_1} \\ &= -\frac{a_1u}{b_1} - \frac{c_1}{b_1} \\ &= -\frac{a_1u + c_1}{b_1} \quad = v \in K \end{aligned}$$

Por tanto, (u, v) con $u, v \in K$ es el punto de intercesión en el plano de K.

Si una recta y una circunferencia en el plano de K se cruzan en el plano real, entonces sus puntos de intersección no son necesariamente puntos en el plano de K, este resultado lo veremos más adelante.

Definición 4.4

Diremos que K es un campo constructible, si K en un subcampo de W. Es decir, K es un subcampo de $\mathbb{R}$ y todo elemento en K es un nḿero constructible.

Teorema 4.2

Sea K un subcampo de $\mathbb{R}$. Si una recta en K y una circunferencia en K se intersectan en el plano real, entonces sus puntos de intersección están en el plano de K o el plano de $K(\sqrt{\gamma})$ donde γ es un real positivo en K y $K(\sqrt{\gamma})$ es una extensión de K de grado 2. Además, si K es un campo constructible, entonces $K(\sqrt{\gamma})$ también lo es.

Demostración. Supongamos que los puntos de intersección de la recta en K y la circunferencia en K no están en el plano de K. Por la geometría analítica se sabe que $Ax + By + C = 0$ y $x^2 + y^2 + Ax + By + C = 0$ son las ecuaciones generales de la recta y circunferencia respectivamente. Sean $a_1x + b_1y + c_1 = 0$ $yx^2 + y^2 + a_2x + b_2y + c_2 = 0$ las ecuaciones de la recta y la circunferencia en K que se intersectan en el plano real. Si suponemos que $b_1 = 0$ entonces:

$$
\begin{aligned}
&a_1x + b_1y + a_1 = 0 \\
&b_1y = -a_1x - c_1 \\
&y = -\frac{a_1}{b_1}x - \frac{c_1}{b_1} \\
&y = mx + n \qquad \text{con } m, n \in K
\end{aligned}
$$

Reemplazando y por $mx + n$ en la ecuación de la circunferencia obtenemos

$$
\begin{aligned}
&x^2 + (mx + n)^2 + a_2x + b_2(mx + n) + c_2 = 0 \\
&x^2 + m^2x^2 + 2mnx + n^2 + a_2x + b_2mx + b_2n + c_2 = 0 \\
&(1 + m^2)x^2 + (2mn + a_2 + b_2m)x + (n^2 + b_2n + c_2) = 0 \\
&x^2 + \frac{(2mn + a_2 + b_2m)x}{1 + m^2} + \frac{(n^2 + b_2n + c_2)}{1 + m^2} = 0 \\
&x^2 + bx + c = 0 \qquad \text{donde } b, c \in K
\end{aligned}
$$

Como existe la intersección entre la recta y la circunferencia al sacar los puntos de

interseción por medio de la fórmula general tenemos $x = \frac{-b\pm\sqrt{b^2-4ac}}{2a} = \frac{-b\pm\sqrt{b-4c}}{2}$ pues $a = 1$, donde $b^2 - 4c \geq 0$.

Si $b^2 - 4c = \gamma$ un número cuadrado en K, entonces los puntos de intersceción están en el plano de K, pero empezamos suponiendo que los puntos de intersección no están en K. En consecuencia, necesariamente $b^2 - 4c = \gamma$ es positivo y γ no es un cuadrado en K. Luego, el polinomio $f(x) = x^2 + bx + c$ es irreducible en $K[x]$ pues tiene raíces

$$x = \frac{-b \pm \sqrt{b^2 - 4c}}{2} = \frac{-b \pm \sqrt{\gamma}}{2}$$

Donde, $x_1 = \frac{1}{2}(-b + \sqrt{\gamma})$ y $x_2 = \frac{1}{2}(-b - \sqrt{\gamma})$. Así, $f(x)$ es al polinomio irreducible de x_1 sobre k y, por lo tanto, $k\left(\frac{1}{2}(-b + \sqrt{\gamma})\right) = K(\sqrt{\gamma})$, la cual es una extensión de k de grado 2.

Ahora, la intersección de la recta K y la circunferencia en K (en el plano real) son los puntos

$$P\left(\frac{1}{2}(-b + \sqrt{\gamma}), \frac{1}{2}m(-b + \sqrt{\gamma}) + n\right) \text{ y } Q\left(\frac{1}{2}(-b - \sqrt{\gamma}), \frac{1}{2}m(-b - \sqrt{8}) + n\right)$$

los cuales están en el plano $K(\sqrt{\gamma})$.

El segmento de extremos $(0,0)$ y $\left(\frac{1}{2}(-b + \sqrt{\gamma}), 0\right)$ tiene longitud $\left|\frac{1}{2}(-b + \sqrt{\gamma})\right|$. Si suponemos que K es un campo constructible, entonces $\frac{1}{2}(-b + \sqrt{\gamma})$ es un número constructible. El Teorema 4.1 implica que $\sqrt{\gamma}$ es constructible. Así, $K(\sqrt{\gamma}) = \{a + b\sqrt{\gamma} \mid a, b \in K\}$ es un campo constructible. □

Corolario 4.2

Sea K un subcampo de $\mathbb{R}$. Si dos circunferencias en K se intersecan en el plano real, entonces sus puntos de intersección están en el plano K o en el plano de $K(\sqrt{\gamma})$, donde γ es en real positivo en K y $K(\sqrt{\gamma})$ es una extensión de K de grado 2. Además, si K es un campo constructible, entonces $k(\sqrt{\gamma})$ lo es.

Demostración. Sean

$$x^2 + y^2 + a_1x + b_1y + c_1 = 0 \text{ y } x^2 + y^2 + a_2x + b_2y + c_2 = 0.$$

Las dos circunferencias que se intersecan en el plano K. Para poder determinar los puntos de intersección, por la geometría analítica realizamos:

$$x^2 + y^2 + a_1x + b_1y + c_1 = 0 - x^2 + y^2 + a_2x + b_2y + c_2 = 0$$
$$(a_1 - a_2)x + (b_1 - b_2)y + (c_1 - c_2) = 0$$

Obteniendo así la ecuación de una recta. Por tanto, el problema se reduce a la intersección en el plano real de una recta y una circunferencia, ambas en K. Por el teorema anterior se concluye el resultado. □

Corolario 4.3
Si α es un real positivo constructible, entonces $\sqrt{\alpha}$ es constructible.

Demostración. Como $\mathbb{Q}$ es un campo constructible y α es constructible, entonces $\mathbb{Q}(\alpha)$ es un subcampo de W. Podernos suponer que $\sqrt{\alpha} \notin \mathbb{Q}(\alpha)$. Ahora, $\left(0, \frac{1}{2}(\alpha - 1)\right)$ es un punto en el plano de $\mathbb{Q}(\alpha)$ y $\frac{1}{2}(\alpha + 1) > 0$ es un número positivo en $\mathbb{Q}(\alpha)$ Lo que implica que $x^2 + \left(y - \frac{1}{2}(\alpha - 1)\right)^2 = \left(\frac{1}{2}(\alpha + 1)\right)^2$ es una circunferencia en el plano de $\mathbb{Q}(\alpha)$. Calculemos los puntos de intersección de la circunferencia con la recta $y = 0$

$$x^2 + \left(-\frac{1}{2}(\alpha - 1)\right)^2 - \left(\frac{1}{2}(\alpha + 1)\right)^2 = 0$$
$$x^2 + \left(\frac{1}{4}\alpha^2 - \frac{1}{2}\alpha + \frac{1}{4}\right) - \left(\frac{1}{4}\alpha^2 + \frac{1}{2}\alpha + \frac{1}{4}\right) = 0$$
$$x^2 - \alpha = 0$$
$$x^2 = \alpha$$
$$x = \pm\sqrt{\alpha}$$

Donde $(\sqrt{\alpha}, 0)$ y $(-\sqrt{\alpha}, 0)$ son los puntos de interseción, los cuales están en el plano de $\mathbb{Q}(\alpha)(\sqrt{\alpha}) = Q(\sqrt{\alpha})$. Por el Teorema 4.2 concluimos que $\sqrt{\alpha}$ es un númeo constructible. □

Una conclusión inmediata que obtenemos a partir de este resultado es:

Corolario 4.4
Si K es un campo constructible y $\alpha \in K$ es un númeo positivo, entonces $K(\alpha)$ es un campo constructible.

Ejemplo. $\mathbb{Q}(\sqrt[4]{3})$ es un campo constructible.

Solución. Dado que $3 \in \mathbb{Q}$ es constructible, entonces por el corolario anterior tenemos que $\mathbb{Q}(\sqrt{3})$ es un campo constructible. Puesto que $\sqrt{3} \in \mathbb{Q}(\sqrt{3})$ obtenemos $\mathbb{Q}(\sqrt{3})(\sqrt{\sqrt{3}}) = \mathbb{Q}(\sqrt[4]{3})$.

Se puede observar que utilizando el criterio de Eisenstein, para $p = 3$ el polinomio $p(x) = x^4 - 3$ es irreducible en $\mathbb{Q}[x]$. Así, $[\mathbb{Q}(\sqrt[4]{3}) : \mathbb{Q}] = 4 = 2^2$.

Observación. El Teorema 4.2 y sus Corolarios naturalmente son válidos si reemplazamos el campo K por $\mathbb{Q}$. Así, podemos obtener campos constructibles a partir de $\mathbb{Q}$ como sigue: Si $\gamma_1 \in \mathbb{Q}^+$ y $\sqrt{\gamma_1} \notin \mathbb{Q}$, entonces $[\mathbb{Q}(\sqrt{\gamma_1}) : \mathbb{Q}] = 2$ y $\mathbb{Q}(\sqrt{\gamma_1})$ es un campo constructible. Ahora, si γ_2 es un número positivo en $\mathbb{Q}(\sqrt{\gamma_1})$ y $\sqrt{\gamma_2} \notin \mathbb{Q}(\sqrt{\gamma_1})$,entonces $[\mathbb{Q}(\sqrt{\gamma_1}, \sqrt{\gamma_2})) : \mathbb{Q}(\sqrt{\gamma_1})] = 2$ y $\mathbb{Q}(\sqrt{\gamma_1}, \sqrt{\gamma_2}))$ es un campo constructible.

Podemos continuar con este proceso y encontrar k reales positivos $\gamma_1, \ldots, \gamma_k$ tales que $\mathbb{Q}(\sqrt{\gamma_1}, \ldots, \sqrt{\gamma_k})$ es un campo constructible.

Lema 4.1
Sea F un campo constructible. Si $E \subset \mathbb{R}$ es una extensión de F de grado 2, entonces existe un real positivo $d \in F$ tal que $E = F(\sqrt{d})$. Por lo tanto, E es un campo constructible.

Demostración. Como $[E : F] = 2$, existe una base $\{1, \alpha\}$ de E como espacio vectorial sobre F. Por lo tanto, $E = F(1, \alpha) = F(\alpha)$. Nuevamente, dado que E es una extensión de F de grado 2, existe $q(x)=x^2 + bx + c \in F[x]$ el polinomio irreducible de α sobre F. Ahora, $\alpha = \frac{1}{2}\left(-b + \sqrt{b^2 - 4c}\right)$ ó $\alpha = \frac{1}{2}\left(-b - \sqrt{b^2 - 4c}\right)$.
Dado que α es un número real positivo constructible, implica que el discriminante

$b^2 - 4c$ es un real positivo y constructible. Así $d = \sqrt{b^2 - 4c}$, entonces por el Corolario 4.2, $E = F(\alpha) = F\left(\sqrt{d}\right)$ es un campo constructible. □

Teorema 4.3

Un número real $\alpha \notin \mathbb{Q}$ es un número constructible, si podemos encontrar una sucesión finita de campos $F_0 = \mathbb{Q}, F_1, \ldots, F_k$ tales que $\alpha \in F_k$, $F_0 \subset F_1 \subset \cdots \subset F_k \subset \mathbb{R}$ y $[F_i : F_{i-1}] = 2$ para todo $i \in \{1, \ldots, k\}$.

Demostración. Supongamos que $F_0 = \mathbb{Q}, F_1, \ldots, F_k$ son campos tales que $\alpha \in F_k$, $F_0 \subset F_1 \subset \cdots \subset F_k \subset \mathbb{R}$ y $[F_i : F_{i-1}] = 2$ para todo $i \in \{1, \ldots, k\}$. Como $\mathbb{Q}$ es un campo constructible, por el Lema 4.1, F_1 lo es. Utilizando nuevamente el Lema 4.1, F_2 es un campo constructible. Continuando con el mismo argumento, obtenemos que F_k es un campo constructible y, por lo tanto, $\alpha \in F_k$ es un número constructible. □

Corolario 4.5

Si α es un real constructible y $\alpha \notin \mathbb{Q}$, entonces α se encuentra en alguna extensión finita K de $\mathbb{Q}$, donde $[K : \mathbb{Q}] = 2^r$ para algún $r \geq 1$.

Demostración. Del Teorema 4.3, existe una sucesión finita de campos $F_0 = \mathbb{Q}$, $F_1, \ldots, F_k$ tales que $\alpha \in F_k, F_0 \subset F_1 \subset \cdots \subset F_k \subset \mathbb{R}$ y $[F_i : F_{i-1}] = 2$ para todo $i \in \{1, \ldots, k\}$. Dado que

$$[F_k : \mathbb{Q}] = [F_k : F_{k-1}] \cdot \cdots \cdot [F_2 : F_1]\,[F_1 : \mathbb{Q}]$$

y cada término del producto es 2, obtenemos que $[F_k : \mathbb{Q}] = 2^k$. □

Ejemplo. $\alpha = \sqrt[8]{2}$ es un número constructible.

Solución. Notemos que $\alpha^2 = \sqrt[4]{2}$ y $\alpha^4 = \sqrt{2}$. Por el criterio de Eisenstein, $p(x) = x^8 - 2$ es el polinomio irreducible de α sobre $\mathbb{Q}$. Así, $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 8$.

Claramente, $\mathbb{Q}(\alpha) = \mathbb{Q}\left(\alpha^4, \alpha^2, \alpha\right)$ y como $\alpha^4 \in \mathbb{Q}\left(\alpha^2\right)$, tenemos que

$$\begin{array}{c} \mathbb{Q}(\alpha) \\ | \\ \mathbb{Q}(\alpha^4) \\ | \\ \mathbb{Q}(\alpha^2) \\ | \\ \mathbb{Q} \end{array}$$

Luego, $\left[\mathbb{Q}\left(\alpha^4\right) : \mathbb{Q}\right] = 2$, pues $p(x)=x^2 - 2 \in \mathbb{Q}$ es el polinomio irreducible de $\alpha^4=\sqrt{2}$, el cual tiene grado 2. Por el criterio de Eisenstein, $q(x) = x^4 - 2$ es el polinomio irreducible de α^2 sobre $\mathbb{Q}$. Luego, $\left[\mathbb{Q}\left(\alpha^2\right) : \mathbb{Q}\right] = 4$ y necesariamente $\left[\mathbb{Q}\left(\alpha^2\right) : \mathbb{Q}\left(\alpha^4\right)\right] = 2$. Como $p(x) = x^8 - 2$ es el polinomio irreducible de α sobre $\mathbb{Q}$, entonces $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 8$ y, por lo tanto, $\left[\mathbb{Q}(\alpha) : \mathbb{Q}\left(\alpha^2\right)\right] = 2$. Concluimos que $\alpha = \sqrt[8]{2}$ es un número constructible.

Teorema 4.4

Si $\alpha \notin \mathbb{Q}$ es un real constructible, entonces $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ es una potencia de 2. En consecuencia, si $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ no es una potencia de 2, entonces α no es constructible.

Demostración. Si α es constructible, entonces de acuerdo al Corolario 4.5 existe una extensión finita K de $\mathbb{Q}$ tal que $\alpha \in K$ y $[K : \mathbb{Q}] = 2^r$ para algún $r \geq 1$. Pero $\mathbb{Q}(\alpha) \subset K$. Luego, $[K : \mathbb{Q}] = [K : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}] = 2^r$, de donde necesariamente $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ es una potencia de 2. □

4.3 Insolubilidad de los tres problemas geométricos clásicos

4.3.1 Duplicar un cubo

Dado un lado de un cubo, no siempre es posible construir con regla y compás el lado de un cubo cuyo volumen sea el doble del volumen del cubo original.

Consideremos un cubo de lado igual a 1. Así, su volumen es 1. Ahora, deseamos construir el lado de un cubo de modo que su volumen sea igual a 2. Luego, el lado de dicho volumen debe ser $\sqrt[3]{2}$. Por el criterio de Eisenstein $p(x) = x^3 - 2$ es el polinomio irreducible de $\sqrt[3]{2}$ sobre $\mathbb{Q}$, sabemos que la dimensión de la extensión $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}]$ es el grado del polinomio irreducible de $\sqrt[3]{2}$, entonces $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$. Por el Teorema 4.4, $\sqrt[3]{2}$ no es constructible, pues la dimensión de la extensión no es un múltiplo de 2. Por tanto, el problema de la diplicación del cubo no es posible.

4.3.2 Cuadratura de un círculo

Dado un círculo no siempre es posible construir con regla y compás un cuadrado que tenga la misma área del círculo dado.

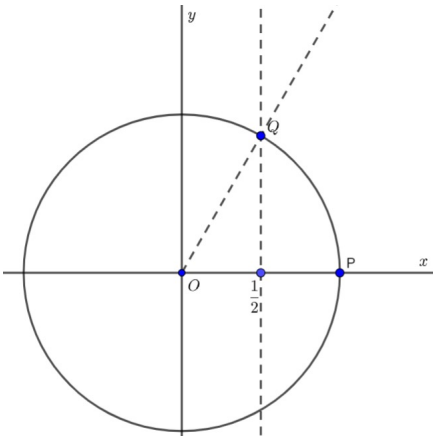
En efecto, consideremos un círculo de radio 1. Así, su área es π. Deseamos construir un cuadrado de lado $\sqrt{\pi}$, para poder obtener un cuadrado con la misma área del círculo dado. Supongamos que tenemos $[\mathbb{Q}(\sqrt{\pi}) : \mathbb{Q}] = 2$, lo que implica que existe un polinomio $p(x) \in \mathbb{Q}$ de grado dos tal que $p(\sqrt{\pi}) = 0$, pero si este hecho sucede, implica que $\sqrt{\pi}$ es algebraico. Por la teoría de números algebraicos se sabe que al multiplicar dos números algebraicos obtenemos un nuevo número algebraico, entonces $\sqrt{\pi} \cdot \sqrt{\pi} = \pi$ implica que π es algebraico, lo que es una contradiccion pues conocemos que π es tracendente. Entonces suponer que $\sqrt{\pi}$ es algebraico es erroneo. Por tanto, podemos concluir que $\sqrt{\pi}$ no es constructible. Con lo cual este problema es insoluble.

4.3.3 Trisecar un ángulo

Existen ángulos que no son posibles de trisecar con regla y compás. Demostraremos que es imposible trisecar un ángulo de $60°$.

Consideremos un sistema coordenado cartesiano rectangular en el plano y una circunferencia de ecuación $x^2 + y^2 = 1$. El punto $Q = \left(\frac{1}{2}, \frac{\sqrt{3}}{2}\right)$ que pertenece a la circunferencia es constructible, ya que sus coordenadas lo son.

Figura 8: Trisección del ángulo



Fuente: Labra, A. & Suazo, A, 2011.

Consideremos los puntos $P = (1,0)$ y $O = (0,0)$, con estos puntos formamos el triángulo POQ, este triángulo es equilátero, pues la longitud de los segmentos $OP = OQ = PO = 1$, luego el coseno del ángulo POQ es $\frac{1}{2}$ y de esto obtenemos que el ángulo POQ es $60°$. Para construir un ángulo de $20°$, necesitamos construir un segmento de longitud $\cos(20°)$.

De las identidades trigonométricas se conoce que $\cos(3\theta) = 4\cos^3(\theta) - 3\cos(\theta)$. Considerando $\theta = 20°$ y reemplazando en la identidad trigonométrica obtenemos $4\cos^3(20°) - 3\cos(20°) = \frac{1}{2}$, de donde $\alpha = \cos(20°)$ es una raíz del polinomio $p(x) = 8x^3 - 6x - 1$, el cuál se obtuvo al reemplazar α en $4\cos^3(\theta) - 3\cos(\theta)$ es decir $4\alpha^3 - 6\alpha = \frac{1}{2}$ y multiplicando por 2 se obtiene $8\alpha^3 - 6\alpha - 1 = 0$. Luego $p(x)$ es el polinomio irreducible de $\alpha = \cos(20°)$. Con lo cual $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$. Por el Teorema 4.4 concluimos que α no es constructible, pues 3 no es un múltiplo de 2, lo que implica que es imposible trisecar un ángulo de $60°$.

Bibliografía

[1] **FRALEIGH, J**. *A first course in Abstract Algebra* [en línea]. Seventh edition. Pearson new international edition, 2014. [Consulta: 14 de junio 2023]. Disponible en: https://www.mymathscloud.com/api/download/modules/University/Textbooks/algebra-abstract/5)A%20First%20Course%20in%20Abstract%20Algebra%20Fraleigh%207th%20edition.pdf?id=25323176

[2] **GALLIAN, J**. *Contemporany Abstract Algebra* [en línea]. Novena edición. USA: Cengage Learning, 2017. [Consulta: 24 de abril 2023]. Disponible en: https://books.google.com.ec/books?id=JMUaCgAAQBAJ&printsec=frontcover&dq=Contempora#v=onepage&q&f=false

[3] **HERSTEIN, I**. *Álgebra Moderna* [en línea]. Eitorial F trillas, S.A. México, 1970. [Consulta: 14 de junio 2023]. Disponible en: https://www.academia.edu/14931038/Algebra_Moderna_Herstein

[4] **JUDSON, T**. *Abstract Algebra Theory and Applications* [en línea]. Texas-USA: Orthogonal Publishing, 2012. [Consulta: 19 de ablir 2022]. Disponible en: http://debracollege.dspaces.org/bitstream/123456789/9/1/Thomas%20W.%20Judson.pdf

[5] **LABRA, A; SUAZO, A**. *Elementos de la teorá de cuerpos* [en línea]. Chile: Jc Sáez Editor, 2011. [Consulta: 17 de abril 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

[6] **STEWART, I**. *Galois Theory* [en línea]. Fourth Edition. CRC Press, 2015. [Consulta:18 de abril 2023]. Disponible en: https://eclass.uoa.gr/modules/document/file.php/MATH594/Stewart%20Galois%204th%20edition.pdf

espoch | Dirección de Bibliotecas y Recursos del Aprendizaje

UNIDAD DE PROCESOS TÉCNICOS Y ANÁLISIS BIBLIOGRÁFICO Y DOCUMENTAL

REVISIÓN DE NORMAS TÉCNICAS, RESUMEN Y BIBLIOGRAFÍA

Fecha de entrega: 19/ 12 / 2023

INFORMACIÓN DEL AUTOR/A (S)
Nombres – Apellidos: Wilmer Andres Caguas Chafla
INFORMACIÓN INSTITUCIONAL
Facultad: Ciencias
Carrera: Matemática
Título a optar: Matemático
f. Analista de Biblioteca responsable: Ing. Rafael Inty Salto Hidalgo

2059-DBRA-UPT-2023