Elementos de la Teoría de Cuerpos

ISBN: 978-956-306-069-0
Registro de Propiedad Intelectual: 200.530
Colección: Herramientas para la formación de profesores de matemáticas.
Diseño: Jessica Jure de la Cerda.
Diseño de Ilustraciones: Cristina Felmer Plominsky, Catalina Frávega Thomas.
Diagramación: Pedro Montealegre Barba, Francisco Santibáñez Palma.
Financiamiento: Proyecto Fondef D05I-10211.

Datos de contacto para la adquisición de los libros:
Para Chile:
1. En librerías para clientes directos.
2. Instituciones privadas directamente con:
   Juan Carlos Sáez C.
   Director Gerente
   Comunicaciones Noreste Ltda.
   J.C. Sáez Editor
   jcsaezc@vtr.net
   www.jcsaezeditor.blogspot.com
   Oficina: (56 2) 3260104 - (56 2) 3253148
3. Instituciones públicas o fiscales: www.chilecompra.cl

Desde el extranjero:
1. Liberalia Ediciones: www.liberalia.cl
2. Librería Antártica: www.antartica.cl
3. Argentina: Ediciones Manantial: www.emanantial.com.ar
4. Colombia: Editorial Siglo del Hombre
   Fono: (571) 3377700
5. España: Tarahumara, tarahumara@tarahumaralibros.com
   Fono: (34 91) 3656221
6. México: Alejandría Distribución Bibliográfica, alejandria@alejandrialibros.com.mx
   Fono: (52 5) 556161319 - (52 5) 6167509
7. Perú: Librería La Familia, Avenida República de Chile # 661
8. Uruguay: Dolmen Ediciones del Uruguay
   Fono: 00-598-2-7124857

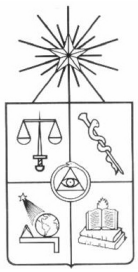
Elementos de la Teoría de Cuerpos — Alicia Labra y Avelino Suazo
Departamento de Matemáticas, Universidad de Chile, Universidad de la Serena
alimat@uchile.cl asuazo@userena.cl

ESTA PRIMERA EDICIÓN DE 2.000 EJEMPLARES
Se terminó de imprimir en febrero de 2011 en WORLDCOLOR CHILE S.A.

ELEMENTOS DE LA TEORÍA DE CUERPOS

Alicia Labra
Universidad de Chile

Avelino Suazo
Universidad de La Serena



Dirección del Proyecto Fondef D05I-10211
Herramientas para la Formación de Profesores de Matemática

Patricio Felmer, Director del Proyecto
Universidad de Chile.

Leonor Varas, Directora Adjunta del Proyecto
Universidad de Chile.

Salomé Martínez, Subdirectora de Monografías
Universidad de Chile.

Cristián Reyes, Subdirector de Estudio de Casos
Universidad de Chile.

Presentación de la Colección

La colección de monografías que presentamos es el resultado del generoso esfuerzo de los autores, quienes han dedicado su tiempo y conocimiento a la tarea de escribir un texto de matemática. Pero este esfuerzo y generosidad no se encuentra plenamente representado en esta labor, sino que también en la enorme capacidad de aprendizaje que debieron mostrar, para entender y comprender las motivaciones y necesidades de los lectores: Futuros profesores de matemática.

Los autores, encantados una y otra vez por la matemática, sus abstracciones y aplicaciones, enfrentaron la tarea de buscar la mejor manera de traspasar ese encanto a un futuro profesor de matemática. Éste también se encanta y vibra con la matemática, pero además se apasiona con la posibilidad de explicarla, enseñarla y entregarla a los jóvenes estudiantes secundarios. Si la tarea parecía fácil en un comienzo, esta segunda dimensión puso al autor, matemático de profesión, un tremendo desafío. Tuvo que salir de su oficina a escuchar a los estudiantes de pedagogía, a los profesores, a los formadores de profesores y a sus pares. Tuvo que recibir críticas, someterse a la opinión de otros y reescribir una y otra vez su texto. Capítulos enteros resultaban inadecuados, el orden de los contenidos y de los ejemplos era inapropiado, se hacía necesario escribir una nueva versión y otra más. Conversaron con otros autores, escucharon sus opiniones, sostuvieron reuniones con los editores. Escuchar a los estudiantes de pedagogía significó, en muchos casos, realizar eventos de acercamiento, desarrollar cursos en base a la monografía, o formar parte de cursos ya establecidos. Es así que estas monografías recogen la experiencia de los autores y del equipo del proyecto, y también de formadores de profesores y estudiantes de pedagogía. Ellas son el fruto de un esfuerzo consciente y deliberado de acercamiento, de apertura de caminos, de despliegue de puentes entre mundos, muchas veces, separados por falta de comunicación y cuya unión es vital para el progreso de nuestra educación.

La colección de monografías que presentamos comprende una porción importante de los temas que usualmente encontramos en los currículos de formación de profesores de matemática de enseñanza media, pero en ningún caso pretende ser exhaustiva. Del mismo modo, se incorporan temas que sugieren nuevas formas de abordar los contenidos, con énfasis en una matemática más pertinente para el futuro profesor, la que difiere en su enfoque de la matemática para un ingeniero o para un licenciado en matemática, por ejemplo. El formato de monografía, que aborda temas específicos

con extensión moderada, les da flexibilidad para que sean usadas de muy diversas maneras, ya sea como texto de un curso, material complementario, documento básico de un seminario, tema de memoria y también como lectura personal. Su utilidad ciertamente va más allá de las aulas universitarias, pues esta colección puede convertirse en la base de una biblioteca personal del futuro profesor o profesora, puede ser usada como material de consulta por profesores en ejercicio y como texto en cursos de especialización y post-títulos. Esta colección de monografías puede ser usada en concepciones curriculares muy distintas. Es, en suma, una herramienta nueva y valiosa, que a partir de ahora estará a disposición de estudiantes de pedagogía en matemática, formadores de profesores y profesores en ejercicio.

El momento en que esta colección de monografías fue concebida, hace cuatro años, no es casual. Nuestro interés por la creación de herramientas que contribuyan a la formación de profesores de matemática coincide con un acercamiento entre matemáticos y formadores de profesores que ha estado ocurriendo en Chile y en otros lugares del mundo. Nuestra motivación nace a partir de una creciente preocupación en todos los niveles de la sociedad, que ha ido abriendo paso a una demanda social y a un interés nacional por la calidad de la educación, expresada de muy diversas formas. Esta preocupación y nuestro interés encontró eco inmediato en un grupo de matemáticos, inicialmente de la Universidad de Chile, pero que muy rápidamente fue involucrando a matemáticos de la Pontificia Universidad Católica de Chile, de la Universidad de Concepción, de la Universidad Andrés Bello, de la Universidad Federico Santa María, de la Universidad Adolfo Ibáñez, de la Universidad de La Serena y también de la Universidad de la República de Uruguay y de la Universidad de Colorado de Estados Unidos.

La matemática ha adquirido un rol central en la sociedad actual, siendo un pilar fundamental que sustenta el desarrollo en sus diversas expresiones. Constituye el cimiento creciente de todas las disciplinas científicas, de sus aplicaciones en la tecnología y es clave en las habilidades básicas para la vida. Es así que la matemática actualmente se encuentra en el corazón del currículo escolar en el mundo y en particular en Chile. No es posible que un país que pretenda lograr un desarrollo que involucre a toda la sociedad, descuide el cultivo de la matemática o la formación de quienes tienen la misión de traspasar de generación en generación los conocimientos que la sociedad ha acumulado a lo largo de su historia.

Nuestro país vive cambios importantes en educación. Se ha llegado a la convicción que la formación de profesores es la base que nos permitirá generar los cambios cualitativos en calidad que nuestra sociedad ha impuesto. Conscientes de que la tarea formativa de los profesores de matemática y de las futuras generaciones de jóvenes es extremadamente compleja, debido a que confluyen un sinnúmero de factores y disciplinas, a través de esta colección de monografías, sus editores, autores y todos los que han participado del proyecto en cada una de sus etapas, contribuyen a esta tarea, poniendo a disposición una herramienta adicional que ahora debe tomar vida propia en los formadores, estudiantes, futuros profesores y jóvenes de nuestro país.

Patricio Felmer y Salomé Martínez
Editores

Agradecimientos

Agradecemos a todos quienes han hecho posible la realización de este proyecto Fondef: "Herramientas para la formación de Profesores de Matemáticas". A Cristián Cox, quien apoyó con decisión la idea original y contribuyó de manera crucial para obtener la participación del Ministerio de Educación como institución asociada. Agradecemos a Carlos Eugenio Beca por su apoyo durante toda la realización del proyecto. A Rafael Correa, Edgar Kausel y Juan Carlos Sáez, miembros del Comité Directivo. Agradecemos a Rafael Benguria, Servet Martínez y Fidel Oteiza, miembros del Comité Editorial de la colección, quienes realizaron valiosos aportes a los textos. A Guillermo Marshall, Decano de la Facultad de Matemáticas de la Pontificia Universidad Católica de Chile y José Sánchez, entonces Decano de la Facultad de Ciencias Físicas y Matemáticas de la Universidad de Concepción, quienes contribuyeron de manera decisiva a lograr la integridad de la colección de 15 monografías. A Jaime San Martín, director del Centro de Modelamiento Matemático por su apoyo durante toda la realización del proyecto. Agradecemos a Víctor Campos, Ejecutivo de Proyectos de Fondef, por su colaboración y ayuda en las distintas etapas del proyecto.

Agradecemos también a Bárbara Ossandón de la Universidad de Santiago, a Jorge Ávila de la Universidad Católica Silva Henríquez, a Víctor Díaz de la Universidad de Magallanes, a Patricio Canelo de la Universidad de Playa Ancha en San Felipe y a Osvaldo Venegas y Silvia Vidal de la Universidad Católica de Temuco, quienes hicieron posible las visitas que realizamos a las carreras de pedagogía en matemática. Agradecemos a todos los evaluadores, alumnos, académicos y profesores -cuyos nombres no incluimos por ser más de una centena- quienes entregaron sugerencias, críticas y comentarios a los autores, que ayudaron a enriquecer cada uno de los textos.

Agradecemos a Marcela Lizana por su impecable aporte en todas las labores administrativas del proyecto, a Aldo Muzio por su colaboración en la etapa de evaluación, y también a Anyel Alfaro por sus contribuciones en la etapa final del proyecto y en la difusión de los logros alcanzados.

Dirección del Proyecto

Índice General

Prefacio

El profesor de Matemáticas de Enseñanza Media, debe tener la capacidad de abstracción para construir y desarrollar argumentaciones lógicas, basadas en las teorías pertinentes con una identificación clara de hipótesis y conclusiones. Sin lugar a dudas, el estudio de la teoría de cuerpos debería contribuir fuertemente en el desarrollo de estas capacidades. Los cuerpos son objetos importantes de estudio en álgebra, puesto que proporcionan la generalización apropiada de dominios de números tales como los conjuntos de números racionales, de números reales y de números complejos. No trataremos el tema en su forma más general, pero incluiremos todos los resultados necesarios que nos permitan introducir las bellas ideas del matemático francés Evaristo Galois, las cuales se estudiarán en el último capítulo de esta monografía.

Suponemos que el lector conoce las propiedades más importantes de los números enteros y las estructuras algebraicas de Grupos, Anillos y Espacios Vectoriales.

El desarrollo teórico de esta monografía está acompañado de ejemplos y ejercicios, que pretenden contribuir a una mayor comprensión de la teoría. En los ejercicios, se incluyen algunas proposiciones que estimamos relevantes para que el lector realice sus demostraciones, puesto que dichos resultados serán utilizados en el desarrollo de este texto.

En los primeros cursos de álgebra se estudia que los conjuntos de números racionales, reales y complejos, que denotaremos por $\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{C}$ respectivamente, tienen la estructura algebraica de cuerpos. Veremos que éstos no son los únicos cuerpos que existen.

Comenzamos el primer capítulo con una revisión de algunas definiciones y resultados referentes a la estructura algebraica de anillo, que serán utilizados en el desarrollo de este texto. Recordaremos propiedades de algunas clases especiales de anillos, a saber, los dominios de integridad (o anillos enteros) y los cuerpos. Finalizamos este capítulo demostrando algunas propiedades de los cuerpos finitos. Dichos cuerpos se estudian nuevamente en el capítulo 3.

En el segundo capítulo se estudian los anillos de polinomios con coeficientes en un cuerpo. El lector podrá darse cuenta que los resultados estudiados en los primeros cursos universitarios, acerca de polinomios con coeficientes reales, se pueden generalizar

a polinomios con coeficientes en un cuerpo cualquiera. Se estudia cuándo un polinomio es irreducible sobre un cuerpo. Dichos polinomios tienen mucha importancia en esta teoría, dado que nos permiten crear nuevos cuerpos. En este capítulo también se muestran ejemplos de cuerpos finitos y se entregan técnicas para su construcción.

En el tercer capítulo se estudia la relación de un cuerpo F con otro cuerpo K, cuando F es un subconjunto de K (se dice que K es una extensión de F). El cuerpo K resulta ser un espacio vectorial sobre F y, en consecuencia, se dispone de la teoría del Álgebra Lineal para obtener resultados sobre las extensiones de cuerpos. En este capítulo se demuestra que todo polinomio no nulo con coeficientes en un cuerpo F, admite una raíz en una extensión K de F. Además, se demuestra que dados p un número primo y n un entero positivo, entonces existe un cuerpo finito con p^n elementos.

En el cuarto capítulo, se muestra cómo la teoría algebraica de cuerpos permite la resolución de problemas geométricos clásicos de construcciones con regla y compás, los que no pudieron ser resueltos por los matemáticos de la antigua Grecia.

En el quinto capítulo, se estudia parte de la Teoría de Galois y se demuestra el Teorema Fundamental de dicha teoría. En este capítulo, sólo se consideran cuerpos contenidos en los números complejos. Se estudia el grupo de Galois de un polinomio de grado 3 y la solubilidad por radicales de los polinomios de grados 3 y 4. Se demuestra que, si $\varphi(n)$ es una potencia de 2 y $n \geq 3$, entonces un polígono regular de n lados es constructible con regla y compás, donde $\varphi : \mathbb{Z}^+ \to \mathbb{Z}^+$ es la función φ de Euler.

Al final de cada capítulo se incluyen ejercicios que hemos llamado Ejercicios de Reforzamiento, cuya resolución por parte del lector debería contribuir a una mejor comprensión de los temas estudiados.

En el apéndice, se da una aplicación de los cuerpos finitos a los códigos lineales. Se transmiten mensajes codificados, el receptor del mensaje puede obtener información distorsionada y puede cometer errores al interpretar la señal transmitida. Se entrega una forma de corregir esos errores y leer el mensaje original.

Queremos expresar nuestro agradecimiento a Patricio Felmer y Salomé Martínez, quienes nos invitaron a participar del Proyecto: Herramientas para la Formación de Profesores de Matemáticas, Fondef D051-10211. Sus comentarios y sugerencias, al igual que las de los profesores: Jorge González Lorca, Irvin Roy Mentzel, Renato Lewin, Rolando Pomareda y de alumnos que revisaron esta monografía, fueron de gran valor al preparar la presente versión. Agradecemos también a los integrantes del Comité Revisor de las Monografías, Señores: Rafael Benguria, Servet Martínez y Fidel Oteiza.

Capítulo 1: Anillos y Cuerpos

1.1 Definiciones y Resultados Básicos

El lector recordará que los conjuntos de números enteros $\mathbb{Z}$ y de números racionales $\mathbb{Q}$, con las operaciones usuales de suma y producto, tienen la estructura algebraica de anillos conmutativos con elemento unidad. En el caso de los racionales $\mathbb{Q}$, todo elemento distinto de cero admite un inverso multiplicativo en $\mathbb{Q}$. Por tal razón, decimos que $\mathbb{Q}$ tiene la estructura algebraica de cuerpo o que simplemente $\mathbb{Q}$ es un cuerpo.

Como se estudió en el primer curso de Álgebra, la estructura algebraica[1] de Grupo tiene su origen en el conjunto de permutaciones de un conjunto sobre sí mismo y la estructura algebraica de Anillo surge de los números enteros. El concepto de anillo fue introducido por R. Dedekind, quien caracterizó los números reales como un cuerpo ordenado completo y realizó valiosos aportes a la teoría de números algebraicos. El primero en dar una definición abstracta de Anillo fue A. Fraenkel (conocido por sus trabajos en teoría axiomática de conjuntos) en 1914, mucho después que se conocieran numerosos ejemplos de anillos. Pero fue Emmy Noether (conocida por sus aportes en el desarrollo abstracto de la teoría de ideales en los cuerpos de números algebraicos y cuerpos de funciones) quien, en 1921, introdujo en su artículo "Ideal Theory of Rings", el concepto de anillo como se usa actualmente.

Amalie Emmy Noether (1882-1935), matemática alemana, es considerada por David Hilbert y Albert Einstein como la mujer más importante en la historia de las matemáticas. El destacado algebrista Irving Kaplansky llamaba a Emmy Noether la "madre del álgebra moderna". El también destacado matemático Saunders MacLane, afirmaba que el álgebra abstracta nace, como disciplina consciente, con el trabajo de E. Noether, "Ideal Theory in Rings", en 1921. Noether contribuyó a las siguientes áreas del álgebra: teoría de invariantes (1907-1919), álgebra conmutativa (1920-1929), álgebra no conmutativa y teoría de representaciones (1927-1933) y las aplicaciones del álgebra no conmutativa a los problemas de álgebra conmutativa (1932-1935).

Dado un anillo R, consideraremos un subconjunto U de R, verificando ciertas propiedades, que llamaremos ideal de R. Posteriormente, construiremos un conjunto de elementos de la forma $a + U$ con $a \in R$, que simbolizaremos por R/U, al que dotaremos de una suma y un producto que dará origen a un nuevo anillo, llamado el anillo cuociente de R por U. En el caso que R sea un anillo conmutativo con elemento unidad $1 \neq 0$, siempre será posible encontrar un ideal U tal que el anillo R/U sea un cuerpo. Esta forma de construir cuerpos nos permitirá la construcción

[1]Conjunto no vacío con operaciones definidas en él y que cumplen ciertas propiedades.

de algunos cuerpos finitos. La bien conocida construcción de los racionales $\mathbb{Q}$ a partir de los enteros $\mathbb{Z}$, la generalizaremos partiendo de un anillo D que verifica las mismas propiedades de $\mathbb{Z}$.

Iniciamos este primer capítulo recordando algunas definiciones y resultados estudiados en los cursos básicos de Álgebra. Nuestro propósito es incluir las herramientas matemáticas necesarias que serán utilizadas en el desarrollo de esta monografía. Además, incluimos las notaciones que usaremos a lo largo de este texto.

En este capítulo sólo demostraremos algunos resultados. Sugerimos realizar las demostraciones de aquellos resultados que sólo se enuncian.

Definición 1.1. *Sea R un conjunto no vacío, en el que están definidas dos operaciones denotadas por $+$ y $\cdot$. Diremos que $(R, +, \cdot)$ es un **anillo**, o simplemente que R es un anillo, si y solo si,*

1. $(R, +)$ *es un grupo Abeliano. Además, para todo* a, b, $c \in R$:
2. $a \cdot b \in R$,
3. $(a \cdot b) \cdot c = a \cdot (b \cdot c)$,
4. $a \cdot (b + c) = a \cdot b + a \cdot c \quad y \quad (b + c) \cdot a = b \cdot a + c \cdot a$.

Podemos observar que $(R, \cdot)$ es cerrado y asociativo. Ahora, si existe un elemento denotado por 1 en R tal que $a \cdot 1 = 1 \cdot a = a$ para todo $a \in R$, diremos que R es un **anillo unitario** o un **anillo con elemento unidad**. Si $a \cdot b = b \cdot a$ para todo a, $b \in R$, diremos que R es un **anillo conmutativo**.

Un elemento no nulo a de un anillo conmutativo R, se dice que es un **divisor del cero**, si existe un elemento no nulo $b \in R$ tal que $ab = 0$.

Un anillo conmutativo R con elemento unidad $1 \neq 0$ y sin divisores del cero, se dice que es un **dominio de integridad** o **anillo entero.**

Definición 1.2. *Si R es un anillo conmutativo con elemento unidad $1 \neq 0$ tal que todos los elementos no nulos de R admiten inversos multiplicativos en R, entonces diremos que R es un **cuerpo.***

Observación 1.1. *Sea F un cuerpo. De la definición de cuerpo concluimos que $(F, +)$ y $(F^*, \cdot)$ son grupos Abelianos, donde $F^* = F - \{0\}$.*

Definición 1.3. *Si S es un subconjunto de un anillo R y S es un anillo con las mismas operaciones de suma y producto de R, entonces se dice que S es un **subanillo** de R.*

Para demostrar que un subconjunto de un anillo R es un subanillo, podemos utilizar el siguiente Lema que dejamos como ejercicio.

Lema 1.1. *Un subconjunto S de un anillo R es un subanillo de R, si y solo si,*

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

Algunos ejemplos de anillos son los que siguen:

1. El conjunto de los números enteros $\mathbb{Z}$, con las operaciones usuales de suma y producto, es un dominio de integridad.
2. El conjunto $2\mathbb{Z} = \{2x \ / \ x \in \mathbb{Z}\}$, con las operaciones usuales de suma y producto, es un anillo conmutativo sin elemento unidad y sin divisores del cero.
3. El conjunto $\mathbb{Z}_n$ de los enteros módulo n, es un anillo conmutativo.
4. Sea $n \geq 2$. El conjunto $M_{n\times n}(\mathbb{Z})$ de las matrices $n \times n$, sobre los enteros $\mathbb{Z}$, con las operaciones usuales de suma y producto de matrices, es un anillo no conmutativo y con elemento unidad.
5. El conjunto $\mathbb{Z}[x]$ de todos los polinomios con coeficientes en $\mathbb{Z}$, con las operaciones usuales de suma y producto de polinomios, es un dominio de integridad.
6. El conjunto $\mathbb{Z}[i] = \{a + bi \ / \ a, b \in \mathbb{Z}\}$, 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.

A continuación, introduciremos la noción de ideal de un anillo la que fue creada por R. Dedekind en 1871. Los ideales generalizan el estudio de la divisibilidad en los números enteros. Existen versiones del Teorema Fundamental del Álgebra y el Teorema Chino del Resto en términos de ideales.

Definición 1.4. *Un subconjunto U de un anillo R, se dice que es un* ***ideal*** *de R, si:*

1. $0 \in U$,
2. *para todo* $a,\ b \in U : a - b \in U$,
3. *para todo* $u \in U$ *y* $r \in R : ur \in U$ *y* $ru \in U$.

Podemos observar que todo ideal de un anillo R es un subanillo de R, pero no todo subanillo de R es un ideal de R. En efecto, el conjunto $\mathbb{Z}[i] = \{a+bi \ / \ a, b \in \mathbb{Z}\}$, con las operaciones usuales de suma y producto de números complejos, es un subanillo de $\mathbb{C}$, pero $\mathbb{Z}[i]$ no es un ideal de $\mathbb{C}$.

El Teorema 1.1 y el Lema 1.2 son de fácil demostración y serán utilizados permanentemente en esta monografía.

Teorema 1.1. *Sea R un anillo conmutativo con elemento unidad y $a_1, \ldots, a_k$ elementos en R. Entonces el conjunto $U = \{a_1x_1 + \cdots + a_kx_k \ / \ x_1, \ldots, x_k \in R\}$ es un ideal de R. Se dice que U es el* ***ideal de*** *R* ***generado por los elementos*** *$a_1, \ldots, a_k$ y se denota $U = \langle a_1, \ldots, a_k \rangle$.*

En los cursos básicos de álgebra se demuestra el siguiente resultado: si U es un ideal del anillo de los enteros $\mathbb{Z}$, entonces existe un entero n tal que $U =< n >= n\mathbb{Z}$. Por tal razón, $\mathbb{Z}$ es un anillo de ideales principales.

Definición 1.5. *Sea R un anillo conmutativo con elemento unidad. Diremos que R es un* ***anillo de ideales principales****, si para cada ideal U de R existe un elemento $a \in R$ tal que $U = \langle a \rangle = \{ax \ / \ x \in R\}$.*

Lema 1.2. *Si U, V son ideales de un anillo R, entonces $U + V = \{u + v \ / \ u \in U, v \in V\}$ es un ideal de R.*

Ejercicios 1.1.

1. Si R es un anillo con elemento unidad 1 y U es un ideal de R tal que $1 \in U$, entonces $U = R$.
2. Si R es un cuerpo, entonces sus únicos ideales son los triviales, es decir, $\{0\}$ y R.
3. Demostrar que el anillo de los números enteros es un anillo de ideales principales (ver [13]).
4. Demostrar que $\mathbb{Q}[x]$ es un anillo de ideales principales.

Definición 1.6. *Si un subconjunto F de un cuerpo K, con las mismas operaciones de suma y producto de K, es un cuerpo, entonces diremos que F es un* ***subcuerpo*** *de K (denotado por $F \leq K$).*

Si un subconjunto F de un cuerpo K es un subanillo de K; para que F sea un cuerpo sólo es necesario que 1 sea un elemento en F y que todo elemento no nulo en F admita inverso multiplicativo en F. De esta forma obtenemos:

Lema 1.3. *Sea K un cuerpo y F un subconjunto de K. Entonces F es un subcuerpo de K, si y solo si,*

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

Ejemplo 1.1. *Demostraremos que el conjunto $\mathbb{Q}(i) = \{a + bi \ / \ a, b \in \mathbb{Q}\}$, donde i es el número complejo tal que $i^2 = -1$, es un cuerpo. Basta con demostrar que $\mathbb{Q}(i)$ es un subcuerpo de $\mathbb{C}$.*

1. $0 = 0 + 0i \in \mathbb{Q}(i)$.
2. *Sean $a + bi$, $c + di$ con a, b, c, $d \in \mathbb{Q}$. Entonces*
$$(a + bi) - (c + di) = (a - c) + (b - d)i \in \mathbb{Q}(i)$$
y
$$(a + bi)(c + di) = (ac - bd) + (ad + bc)i \in \mathbb{Q}(i).$$
3. $1 = 1 + 0i \in \mathbb{Q}(i)$.
4. *Sea $a + bi \neq 0$ con a, $b \in \mathbb{Q}$. Entonces $a \neq 0$ ó $b \neq 0$, de donde $a^2 + b^2 > 0$. El inverso multiplicativo de $a + bi$ es*
$$(a + bi)^{-1} = \frac{a}{a^2 + b^2} - \frac{b}{a^2 + b^2} i \in \mathbb{Q}(i).$$

Ejercicios 1.2.

1. Demostrar que el conjunto $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \ / \ a, b \in \mathbb{Q}\}$ es un subcuerpo de $\mathbb{R}$.

2. Demostrar que el conjunto $\mathbb{Q}(\sqrt{2}i) = \{a+b\sqrt{2}i \ / \ a, b \in \mathbb{Q}\}$ es un subcuerpo de $\mathbb{C}$.
3. Considerar el conjunto $K = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \ / \ a, \ b \in \mathbb{R} \right\}$ con las operaciones usuales de suma y producto de matrices.
   a) Demostrar que $\sigma : \mathbb{C} \to K$ definida por $\sigma(a+bi) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ para todo a, $b \in \mathbb{R}$, es un isomorfismo de anillos. En consecuencia, K es un cuerpo isomorfo a $\mathbb{C}$.
   b) Verificar que $\begin{pmatrix} -\frac{1}{2} & \frac{1}{2}\sqrt{3} \\ -\frac{1}{2}\sqrt{3} & -\frac{1}{2} \end{pmatrix} \in K$ es una solución de la ecuación $x^2 + x + \sigma(1) = \sigma(0)$.
   c) Sean c, d reales tales que $c^2 - 4d < 0$. Encontrar en K una solución de la ecuación $x^2 + \sigma(c)x + \sigma(d) = \sigma(0)$.

Consideremos a continuación un ideal U de un anillo R. Dado que $(U, +)$ es un subgrupo de $(R, +)$, podemos definir el conjunto $R/U = \{a + U \ / \ a \in R\}$ de todas las distintas clases laterales de U en R. De acuerdo a los resultados de la teoría de grupos, el conjunto R/U es un grupo bajo la adición donde

$$(a+U) + (b+U) = (a+b) + U$$

para todo a, $b \in R$. Para que R/U tenga la estructura de anillo, necesitamos definir un producto en R/U que esté bien definido y verifique las propiedades (3) y (4) de la definición 1.1. Dejamos como ejercicio para el lector, demostrar que el producto

$$(a+U)(b+U) = ab + U$$

está bien definido en R/U y que verifica las propiedades antes indicadas. El anillo R/U se dice que es el **anillo cuociente de** R **por** U.

Definición 1.7. *Sea R un anillo. Un ideal M de R con $M \neq R$ se dice que es un* ***ideal maximal*** *de R, si dado un ideal U de R tal que $M \subset U \subset R$, entonces $M = U$ ó $U = R$. Es decir, no existe un ideal U de R tal que $M \subsetneq U \neq R$.*

Ejemplo 1.2. *Demostraremos que el ideal $< 2 >= 2\mathbb{Z}$ de $\mathbb{Z}$ es un ideal maximal de $\mathbb{Z}$. Sea U un ideal de $\mathbb{Z}$ tal que $2\mathbb{Z} \subset U \subset \mathbb{Z}$. Como $\mathbb{Z}$ es un anillo de ideales principales y $U \neq \{0\}$ $(2 \in U)$, entonces existe $n \in \mathbb{Z}^+$ tal que $U = n\mathbb{Z}$. Dado que $2\mathbb{Z} \subset n\mathbb{Z}$, entonces existe $q \in \mathbb{Z}^+$ tal que $2 = nq$. Lo anterior implica que $n = 2$ ó $n = 1$. Si $n = 2$, entonces $2\mathbb{Z} = U$ y si $n = 1$, entonces $U = \mathbb{Z}$. Por lo tanto, $2\mathbb{Z}$ es un ideal maximal de $\mathbb{Z}$.*

Ejemplo 1.3. *El ideal $\langle 6 \rangle = 6\mathbb{Z}$ no es un ideal maximal de Z. En efecto, $\langle 2 \rangle = 2\mathbb{Z}$ es un ideal de $\mathbb{Z}$ y $6\mathbb{Z} \subsetneq 2\mathbb{Z} \neq \mathbb{Z}$.*

Ejercicios 1.3.

1. Sea p un número primo. Demostrar que $p\mathbb{Z}$ es un ideal maximal de $\mathbb{Z}$.

2. ¿Es el ideal $< x^2 - 1 >$ de $\mathbb{Q}[x]$ un ideal maximal de $\mathbb{Q}[x]$?
3. Demostrar que el ideal $< x^4 + 4 >$ de $\mathbb{Q}[x]$ no es un ideal maximal de $\mathbb{Q}[x]$.
4. ¿Cuántos ideales maximales tiene un cuerpo K?

El resultado que sigue, que permite la construcción de un cuerpo a partir de un anillo conmutativo con elemento unidad y de un ideal maximal del anillo, es fundamental en la Teoría de Cuerpos.

Teorema 1.2. *Sea R un anillo conmutativo con elemento unidad $1 \neq 0$ y M un ideal de R. Entonces M es un ideal maximal de R, si y solo si, R/M es un cuerpo.*

Demostración. Supongamos que M es un ideal maximal de R. Debemos demostrar que R/M es un anillo conmutativo con elemento unidad tal que todos los elementos no nulos en R/M admiten inversos multiplicativos en R/M.

Sabemos que R/M es un anillo conmutativo (dado que R también lo es) con elemento unidad $1 + M \neq 0 + M$. Probaremos a continuación que, si $a + M \in R/M$ con $a + M \neq 0 + M$ (es decir, $a \notin M$), entonces $a + M$ tiene un inverso multiplicativo en R/M. Ahora, $\langle a \rangle$ y M son ideales de R y por el Lema 1.2, $M + \langle a \rangle$ es un ideal de R. Como $a \notin M$ y $a = 0 + a \in M + \langle a \rangle$, entonces $M \subsetneqq M + \langle a \rangle$. Por hipótesis, M es un ideal maximal de R, en consecuencia, se debe tener que $M + \langle a \rangle = R$. Dado que $1 \in R$, existen $m \in M$ y $b \in R$ tales que $1 = m + ab$, lo que implica $ab - 1 = -m \in M$. Luego, $ab + M = 1 + M$. Por lo tanto, $(a + M)(b + M) = 1 + M$ y así, $(a + M)^{-1} = b + M$.

Supongamos que R/M es un cuerpo. Debemos probar que M es un ideal maximal de R. Sea U un ideal de R tal que $M \subsetneqq U \subset R$. Demostraremos que $U = R$. Utilizando la definición 1.4, obtenemos que $U/M = \{u + M \ / \ u \in U\}$ es un ideal de R/M. En efecto, $0 + M \in U/M$, además, si $u_1 + M$, $u_2 + M$ son elementos en U/M y $r + M \in R/M$, entonces

$$(u_1 + M) - (u_2 + M) = (u_1 - u_2) + M \in U/M$$

y

$$(r + M)(u_1 + M) = ru_1 + M \in U/M.$$

Como $M \subsetneqq U$, existe $u \in U$ tal que $u \notin M$. Luego, $u + M \in U/M$ y $u + M \neq 0 + M$, lo que demuestra $U/M \neq \{0 + M\}$. Por hipótesis, R/M es un cuerpo y por lo tanto, sus únicos ideales son $\{0 + M\}$ y R/M. Concluimos que, $U/M = R/M$. Consideremos $x \in R$, entonces existe $u \in U$ tal que $x + M = u + M$, de donde $x - u \in M \subset U$ y así, $x \in U$. Por lo tanto, $R = U$, lo que demuestra que M es un ideal maximal de R. □

Lema 1.4. *Si p es un número primo, entonces $\mathbb{Z}/p\mathbb{Z}$ es un cuerpo con p elementos.*

Demostración. Si p es un número primo, entonces $p\mathbb{Z}$ es un ideal maximal de $\mathbb{Z}$ (Ejercicios 1.3). Por el Teorema 1.2, $\mathbb{Z}/p\mathbb{Z}$ es un cuerpo.

Demostraremos a continuación que $\mathbb{Z}/p\mathbb{Z} = \{a + p\mathbb{Z} \ / \ 0 \leq a < p\}$. Si $b + p\mathbb{Z} \in \mathbb{Z}/p\mathbb{Z}$, entonces por el algoritmo de Euclides, existen enteros q, r tales que $b = pq + r$ con $0 \leq r < p$. Así, $b - r = pq \in p\mathbb{Z}$, de donde $b + p\mathbb{Z} = r + p\mathbb{Z}$ con $0 \leq r < p$.

Ahora demostraremos que $\mathbb{Z}/p\mathbb{Z}$ tiene p elementos. Supongamos que existen elementos $a+p\mathbb{Z}$, $c+p\mathbb{Z}$ en $\mathbb{Z}/p\mathbb{Z}$ tales que $a+p\mathbb{Z}=c+p\mathbb{Z}$ con $0\leq a<c<p$. Entonces $c-a\in p\mathbb{Z}$ y $0<c-a<p$, lo que es una contradicción. De esta forma hemos demostrado que $\mathbb{Z}/p\mathbb{Z}$ es un cuerpo con p elementos. □

Ejemplo 1.4. *Por el Lema 1.4, el anillo cuociente* $\mathbb{Z}/31\mathbb{Z}=\{a+31\mathbb{Z}\ /\ a\in\mathbb{Z}\}$ *es un cuerpo con* 31 *elementos. Como* $17+31\mathbb{Z}\neq 0+31\mathbb{Z}$, *entonces el elemento* $17+31\mathbb{Z}$ *debe tener un inverso multiplicativo en* $\mathbb{Z}/31\mathbb{Z}$. *Encontraremos dicho inverso.*

Deseamos encontrar un elemento de la forma $a+31\mathbb{Z}$ *con* $a\in\mathbb{Z}$ *tal que* $(a+31\mathbb{Z})(17+31\mathbb{Z})=1+31\mathbb{Z}$, *lo que es equivalente a encontrar enteros* a, q *tales que* $17a-1=31q$. *En consecuencia, el problema se resuelve encontrando una solución de la ecuación lineal Diofántica* $17x+31y=1$. *Utilizando el algoritmo de Euclides obtenemos que*

$$\begin{aligned}(1)\ &:\ 31=17\cdot 1+14\\(2)\ &:\ 17=14\cdot 1+3\\(3)\ &:\ 14=3\cdot 4+2\\(4)\ &:\ 3=2\cdot 1+1.\end{aligned}$$

De (4) *y* (3) *tenemos*

$$\begin{aligned}1 &= 3+2(-1)=3+(14+3(-4))(-1)\\ &= 3\cdot 5+14(-1).\end{aligned}$$

Luego, de (2) *y* (1) , *tenemos*

$$\begin{aligned}3\cdot 5+14(-1) &= (17+14(-1))5+14(-1)=17\cdot 5+14(-6)\\ &= 17\cdot 5+(31+17(-1))(-6)=17\cdot 11+31(-6).\end{aligned}$$

Por lo tanto, $17\cdot 11+31(-6)=1$ *y concluimos que* $(17+31\mathbb{Z})^{-1}=11+31\mathbb{Z}$.

Como es sabido, si $(G,\cdot)$ y $(H,*)$ son grupos, un homomorfismo de G en H se define como una función $\phi:G\to H$ tal que $\phi(a\cdot b)=\phi(a)*\phi(b)$ para todo $a,\,b\in G$. Es decir, ϕ es respetuosa de las operaciones de G y H. Una extensión natural de la definición anterior para el caso de anillos es la que sigue:

Definición 1.8. *Sean* A, B *anillos. Una función* $f:A\to B$ *es un* ***homomorfismo de anillos****, si y solo si,*

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

Podemos ver que la propiedad (1), de la definición anterior, nos dice que f es un homomorfismo del grupo $(A,+)$ en el grupo $(B,+)$. Por lo tanto, el núcleo de f (denotado por $Ker(f)$) es un subgrupo de $(A,+)$ y la imagen de f (denotada por $Im(f)$ o $f(A)$) es un subgrupo de $(B,+)$. Además, obtenemos el siguiente resultado: $f:A\to B$ es un homomorfismo inyectivo de anillos, si y solo si, $Ker(f)=\{0\}$.

$Ker(f)$ no sólo resulta ser un subgrupo de $(A, +)$, sino que es un ideal del anillo A. De acuerdo a la definición 1.4, sólo debemos probar la propiedad (3). Sea $a \in A$ y $r \in Ker(f)$. Entonces $f(ar) = f(a)f(r) = f(a)\cdot 0 = 0$ y $f(ra) = f(r)f(a) = 0 \cdot f(a) = 0$, lo que demuestra que ar y ra son elementos en $Ker(f)$.

Es fácil demostrar que $f(A) = \{f(a) \ / \ a \in A\}$ es un subanillo de B.

Definición 1.9. *Sean A, B anillos.*

a) *Si $f : A \to B$ es un homomorfismo biyectivo de anillos, diremos que $f : A \to B$ es un* ***isomorfismo de anillos****.*
b) *Si existe un isomorfismo de anillos $f : A \to B$, diremos que A y B son anillos isomorfos. Tal situación la denotaremos por $A \approx B$.*
c) *Si $f : A \to A$ es un isomorfismo de anillos, diremos que f es un* ***automorfismo de*** *A.*
d) *Si $f : A \to B$ es un homomorfismo inyectivo de anillos, diremos que f es un* ***monomorfismo de anillos****.*

Enunciaremos a continuación dos conocidos teoremas.

Teorema 1.3. Primer teorema de isomorfismo de anillos.
Sean A, B anillos. Si $f : A \to B$ es un homomorfismo de anillos, entonces los anillos A/K y $f(A)$ son isomorfos, donde $K = Ker(f)$.

Teorema 1.4. *Sean A, B, D anillos.*

a) *Si $\phi : A \to B$ es un isomorfismo de anillos, entonces $\phi^{-1} : B \to A$ también lo es.*
b) *Si $\phi : A \to B$ y $\sigma : B \to D$ son homomorfismo de anillos, entonces $\sigma \circ \phi : A \to D$ es un homomorfismo de anillos.*

Los dos Lemas que siguen permitirán demostrar el Corolario 1.1. La importancia de dicho resultado quedará de manifiesto en el capítulo 5.

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

Demostración. Sabemos que $\phi(0) = 0'$ y así, por hipótesis, $\phi(1) \neq 0'$. Como $\phi(1)\phi(1) = \phi(1 \cdot 1) = \phi(1)$, entonces $\phi(1)(\phi(1) - 1') = 0'$. Dado que D' no tiene divisores del cero y $\phi(1) \neq 0'$, entonces $\phi(1) = 1'$. □

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

Demostración. Del Lema 1.5, $\phi(1) = 1$. Sea $n \in \mathbb{Z}^+$ y supongamos como hipótesis de inducción que $\phi(n) = n$. Entonces $\phi(n + 1) = \phi(n) + \phi(1) = n + 1$. Por lo tanto, hemos probado que $\phi(m) = m$ para todo $m \in \mathbb{Z}^+$.

Ahora, para $n \in \mathbb{Z}^+$ tenemos $\phi(-n) = -\phi(n) = -n$. Dado que $\phi(0) = 0$, concluimos que $\phi(x) = x$ para todo $x \in \mathbb{Z}$. □

Corolario 1.1. *Sea K un subcuerpo de los números complejos y $\phi : \mathbb{Q} \to K$ un monomorfismo de anillos. Entonces $\phi(x) = x$ para todo $x \in \mathbb{Q}$.*

Demostración. Notemos primero que, si consideramos la restricción de ϕ a $\mathbb{Z}$, es decir, la función $\phi_{\mathbb{Z}} : \mathbb{Z} \to K$ definida por $\phi_{\mathbb{Z}}(n) = \phi(n)$ para todo $n \in \mathbb{Z}$, entonces $\phi_{\mathbb{Z}} : \mathbb{Z} \to K$ sigue siendo un monomorfismo de anillos. Por lo tanto, por el Lema 1.6, obtenemos que $\phi(x) = x$ para todo $x \in \mathbb{Z}$.

Como $\phi : \mathbb{Q} \to K$ es inyectiva, entonces para todo $x \in \mathbb{Q}^* = \mathbb{Q} - \{0\}$, debemos tener que $\phi(x) \in K^* = K - \{0\}$. Luego, $\phi : (\mathbb{Q}^*, \cdot) \to (K^*, \cdot)$ es un homomorfismo inyectivo de grupos. Sean a, $b \in \mathbb{Z}$ ambos no nulos. Entonces $\phi(\frac{a}{b}) = \phi(ab^{-1}) = \phi(a)\phi(b^{-1}) = \phi(a)\phi(b)^{-1} = ab^{-1} = \frac{a}{b}$. Por lo tanto, $\phi(x) = x$ para todo $x \in \mathbb{Q}$. □

Cuando se realiza la construcción de los números racionales $\mathbb{Q}$, a partir de los números enteros $\mathbb{Z}$, se define una función $h : \mathbb{Z} \to \mathbb{Q}$ por $h(n) = \frac{n}{1}$ para todo $n \in \mathbb{Z}$, la que resulta ser un monomorfismo de anillos. De esta forma, $\mathbb{Q}$ posee un subanillo $h(\mathbb{Z}) = \{h(n) \ / \ n \in \mathbb{Z}\}$ isomorfo a $\mathbb{Z}$. Podemos identificar el entero $n \in \mathbb{Z}$ con el racional $h(n) = \frac{n}{1}$ y, en este caso, escribir $n = \frac{n}{1}$. Por lo tanto, $\mathbb{Z} \subset \mathbb{Q}$.

Es natural pensar que los argumentos dados anteriormente, que nos permiten identificar enteros con racionales, se pueden generalizar en el siguiente sentido: si A, B son dominios de integridad y $h : A \to B$ es un monomorfismo de anillos, entonces A y $h(A)$ son dominios de integridad isomorfos, en consecuencia podemos pensar que A, manteniendo su estructura, vivirá en B como $h(A)$.

Demostraremos a continuación: si D es un dominio de integridad, entonces siempre existe un cuerpo K tal que $D \subset K$. El cuerpo K se construye en forma absolutamente análoga a la construcción de los números racionales a partir de los números enteros.

Teorema 1.5. *Si D es un dominio de integridad, entonces existe un cuerpo K tal que $D \subset K$.*

Demostración. Sea D un dominio de integridad. Construiremos un cuerpo K que contenga a D. El punto de partida es considerar el conjunto $M = \{(a, b) \ / \ a, b \in D \text{ y } b \neq 0\}$ en el que definimos la relación $\sim$ por: $(a, b) \sim (c, d)$, si y solo si, $ad = bc$. Esta relación resulta ser de equivalencia sobre M, luego existe la clase de equivalencia $[(a, b)] = \{(x, y) \in M \ / \ (x, y) \sim (a, b)\}$ para cualquier elemento $(a, b) \in M$.

Como es sabido, las distintas clases de equivalencia forman una partición del conjunto M. Sea K el conjunto de todas las clases de equivalencias $[(a, b)]$ con a, $b \in D$ y $b \neq 0$.

Para hacer de K un cuerpo, debemos introducir una suma y una multiplicación en K y probar que bajo estas operaciones K es un cuerpo. Definimos una suma y un producto en K como sigue

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

Dejamos como ejercicio para el lector demostrar que estas operaciones están bien definidas y que K es un cuerpo.

Denotando $[(a,b)] = \frac{a}{b}$, obtenemos que $K = \{\frac{a}{b} \ / \ a, b \in D \text{ y } b \neq 0\}$. Notemos que, si $\frac{a}{b}$, $\frac{c}{d} \in K$, entonces

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

y

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

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

Observación 1.2. *El cuerpo K, construido a partir del dominio de integridad D, se dice que es el* ***cuerpo de fracciones del dominio de integridad*** *D. Además, K resulta ser el cuerpo más pequeño que contiene a D en el siguiente sentido: si F es un cuerpo 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 cuerpo, entonces $b^{-1} \in F$. Así, $\frac{a}{b} = ab^{-1} \in F$, lo que demuestra $K \subset F$.*

Ejemplo 1.5. *De acuerdo a la observación 1.2, $\mathbb{Q}$ es el cuerpo de fracciones de $\mathbb{Z}$ y $\mathbb{Q}(x) = \{\frac{f(x)}{g(x)} \ / \ f(x), g(x) \in \mathbb{Q}[x] \text{ y } g(x) \neq 0\}$ es el cuerpo de fracciones del anillo de polinomios $\mathbb{Q}[x]$.*

Ejercicios 1.4.

1. Sea p un número primo, ¿cuál es el cuerpo de fracciones de $\mathbb{Z}/p\mathbb{Z}$?
2. Si D es un dominio de integridad y D es un conjunto finito, demostrar que D es un cuerpo.
3. $\mathbb{Q}(i) = \{a + bi \ / \ a, b \in \mathbb{Q}\}$ es el cuerpo de fracciones del dominio de integridad $\mathbb{Z}(i) = \{a + bi \ / \ a, b \in \mathbb{Z}\}$.
4. ¿Será verdadera la siguiente afirmación? Si K es un cuerpo, entonces existe un dominio de integridad $D \neq K$ tal que K es el cuerpo de fracciones de D.

Lema 1.7. *Si F es un subcuerpo de $\mathbb{C}$, entonces $\mathbb{Q} \subset F$.*

Demostración. Si F es un subcuerpo de $\mathbb{C}$, entonces 0 y 1 son elementos en F. Así, $1 + 1 \in F$ y por inducción $n \in F$ para todo $n \in \mathbb{Z}^+$. Ahora, para $n \in \mathbb{Z}^+$, $-n \in F$ y luego, $\mathbb{Z} \subset F$. De la observación 1.2, el cuerpo de fracciones de $\mathbb{Z}$ está contenido en F y por lo tanto, $\mathbb{Q} \subset F$. □

Definición 1.10. *Sea R un anillo con elemento unidad 1. Si $n \in \mathbb{Z}^+$, $n{\cdot}1$ denotará los n sumandos $1 + 1 + \cdots + 1 \in R$. Para $n \in \mathbb{Z}^-$, $n \cdot 1$ denotará los $(-n)$ sumandos $(-1)+(-1)+\cdots+(-1) = (-n)\cdot(-1)$ y $0_{\mathbb{Z}} \cdot 1 = 0$, donde $0_{\mathbb{Z}}$ es el cero en $\mathbb{Z}$. El menor entero positivo n (si es que existe) tal que $n \cdot 1 = 0$, se dice que es la* ***característica de*** *R. Si tal entero positivo n no existe, se dice que R es de* ***característica cero****.*

Ejemplo 1.6. *Los anillos* $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ *tienen característica cero y el anillo* $\mathbb{Z}_n$ *tiene característica* n.

Teorema 1.6. *Sea* K *un cuerpo.*

a) Si la característica de K *es* $n > 1$, *entonces* $n = p$ *es un número primo y* K *contiene un subcuerpo isomorfo a* $\mathbb{Z}/p\mathbb{Z}$.

b) Si la característica de K *es cero, entonces* K *contiene un subcuerpo isomorfo a* $\mathbb{Q}$ *y luego,* K *es infinito.*

c) Si K *es un conjunto finito, entonces* K *tiene característica* p *con* p *primo y luego,* K *contiene un subcuerpo isomorfo a* $\mathbb{Z}/p\mathbb{Z}$.

Demostración. Denotemos por 1_K el elemento unidad del cuerpo K. La función $\phi : \mathbb{Z} \to K$ definida por $\phi(m) = m \cdot 1_K$ para todo $m \in \mathbb{Z}$, es un homomorfismo de anillos (ver, [5]).

a) Supongamos que la característica de K es $n > 1$. Como $\phi(n) = n \cdot 1_K = 0$, entonces $Ker(\phi) \neq \{0\}$. Como $Ker(\phi)$ es un ideal de $\mathbb{Z}$ y $\mathbb{Z}$ es un anillo de ideales principales, existe $n_0 \in \mathbb{Z}^+$ tal que $Ker(\phi) = n_0\mathbb{Z}$. Dado que $\phi(n_0) = n_0 \cdot 1_K = 0$ y n es el menor entero positivo tal que $n \cdot 1_K = 0$, entonces tenemos que $n \leq n_0$. 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. Pero $\phi(\mathbb{Z})$ es un subanillo del cuerpo K y luego, no existen divisores del cero en $\phi(\mathbb{Z})$. Concluimos que necesariamente $n = p$ es un número primo.

b) Si la característica de K es cero, entonces $Ker(\phi) = \{0\}$. En efecto, si suponemos que $Ker(\phi) \neq \{0\}$, entonces existe $m \in \mathbb{Z}^+$ tal que $\phi(m) = 0$, lo que contradice nuestra hipótesis. Así, $\phi : \mathbb{Z} \to K$ es inyectiva y por lo tanto, existe un subanillo $\phi(\mathbb{Z})$ contenido en K, el que resulta ser isomorfo a $\mathbb{Z}$. Los cuerpos de fracciones de $\mathbb{Z}$ y de $\phi(\mathbb{Z})$ son isomorfos. De acuerdo a la observación 1.2, el cuerpo de fracciones de $\phi(\mathbb{Z})$ está contenido en el cuerpo K.

c) 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 $a \in K$, $m \cdot a = 0$ ($m \cdot a$ denota los m sumandos $a + a + \cdots + a$) y por lo tanto, $m \cdot 1_K = 0$. Existe un menor entero positivo p tal que $p \cdot 1_K = 0$ que es la característica de K. De (a), p es un número primo y K contiene un subcuerpo isomorfo a $\mathbb{Z}/p\mathbb{Z}$. □

1.2 Algunos Cuerpos Finitos

Un **cuerpo finito** es un cuerpo con un número finito de elementos. Es usual denotar por F_q a un cuerpo finito con q elementos. Los cuerpos finitos son totalmente conocidos y juegan un rol importante en teoría de los números, geometría algebraica, teoría de Galois.

Del Lema 1.4, tenemos que cuando p es un número primo, $\mathbb{Z}/p\mathbb{Z}$ es un cuerpo con p elementos. Para $n \geq 2$, el conjunto de clases de congruencia módulo n (denotado por $\mathbb{Z}_n$) es un anillo conmutativo con elemento unidad $\overline{1} \neq \overline{0}$. Si p es un número primo, entonces $\mathbb{Z}_p$ es un cuerpo. Para demostrar esta última afirmación, basta probar que

los elementos no nulos en $\mathbb{Z}_p$ admiten inversos multiplicativos en $\mathbb{Z}_p$. Si $\overline{a} \in \mathbb{Z}_p$ con $\overline{a} \neq \overline{0}$, entonces a, p son enteros primos relativos (resultado de fácil demostración). Luego, existen enteros u, v tales que $au + pv = 1$, de donde $au \equiv 1$ $(mód\ p)$. Por lo tanto, $\overline{au} = \overline{a} \cdot \overline{u} = \overline{1}$ y así, $(\overline{a})^{-1} = \overline{u} \in \mathbb{Z}_p$.

Otra forma de demostrar que $\mathbb{Z}_p$ es un cuerpo es considerando la función $\sigma : \mathbb{Z} \to \mathbb{Z}_p$ definida por $\sigma(a) = \overline{a}$ para todo $a \in \mathbb{Z}$. Claramente σ es un homomorfismo sobreyectivo de anillos. Si $a \in Ker(\sigma)$, entonces $\sigma(a) = \overline{a} = \overline{0}$, de donde $a \in p\mathbb{Z} = \{px \ / \ x \in \mathbb{Z}\}$. Así, $Ker(\sigma) \subset p\mathbb{Z}$. Dado que $p\mathbb{Z} \subset Ker(\sigma)$, obtenemos que $Ker(\sigma) = p\mathbb{Z}$. Sabemos que $p\mathbb{Z}$ es un ideal maximal de $\mathbb{Z}$ y luego, el anillo cuociente $\mathbb{Z}/p\mathbb{Z}$ es un cuerpo. Utilizando el Teorema 1.3, concluimos que los anillos $\mathbb{Z}/p\mathbb{Z}$ y $\mathbb{Z}_p$ son isomorfos. En consecuencia, $\mathbb{Z}_p$ es un cuerpo.

Observación 1.3. *Los cuerpos $\mathbb{Z}/p\mathbb{Z}$ y $\mathbb{Z}_p$ que se construyen en apariencia en forma diferente resultan ser iguales. En efecto, si $a \in \mathbb{Z}$, entonces*

$$\overline{a} = \{x \in \mathbb{Z}/x \equiv a(mod\, p)\} = \{a + pt/t \in \mathbb{Z}\} = a + p\mathbb{Z}.$$

Ejemplo 1.7. *Los primeros tres cuerpos con el menor número de elementos son $F_2 = \mathbb{Z}_2 = \{\overline{0}, \overline{1}\}$, $F_3 = \mathbb{Z}_3 = \{\overline{0}, \overline{1}, \overline{2}\}$ y $F_4 = \{0, 1, a, b\}$ con las operaciones de suma y producto definidas por*

$+$	0	1	a	b
0	0	1	a	b
1	1	0	b	a
a	a	b	0	1
b	b	a	1	0

y

$\cdot$	0	1	a	b
0	0	0	0	0
1	0	1	a	b
a	0	a	b	1
b	0	b	1	a

Con los resultados del capítulo 3, veremos que es posible construir este cuerpo finito con 4 elementos.

Después de los resultados del Teorema 1.6 es natural preguntarse, ¿será todo cuerpo de característica p un cuerpo finito? En el capítulo 2 se estudiará que cuando F es un cuerpo, entonces el anillo de polinomios $F[x]$ es un dominio de integridad. Luego, $\mathbb{Z}_2[x]$ es un dominio de integridad que contiene a $\mathbb{Z}_2$. Por el Teorema 1.5, el cuerpo de fracciones $\mathbb{Z}_2(x)$ contiene a $\mathbb{Z}_2[x]$ y claramente $\mathbb{Z}_2(x)$ es un cuerpo infinito de caraterística 2.

Con los resultados del capítulo 3, construiremos nuevos cuerpos finitos a partir de los cuerpos $\mathbb{Z}_p$.

El teorema que sigue, llamado Pequeño Teorema de Fermat, se debe a Pierre de Fermat, matemático francés (1601-1665), quien realizó importantes contribuciones para el desarrollo del cálculo moderno. Autor de la conjetura conocida como el "Último Teorema de Fermat": si n es un entero mayor que 2, entonces no existen enteros a, b y c distintos de cero tales $a^n + b^n = c^n$. Esta conjetura fue demostrada por Andrew Wiles en el año 1993.

Utilizando teoría de grupos y el hecho que $\mathbb{Z}_p$ es un cuerpo, cuando p es un número primo, demostraremos el Pequeño Teorema de Fermat.

Teorema 1.7. *Si p es un número primo y a un entero tal que $p \nmid a$, entonces $a^{p-1} \equiv 1$ (mód p).*

Demostración. Como $\mathbb{Z}_p$ es un cuerpo con p elementos, entonces $(\mathbb{Z}_p^*, \cdot)$ es un grupo con $p-1$ elementos, donde $\mathbb{Z}_p^* = \mathbb{Z}_p - \{\overline{0}\}$. Dado que $\overline{a} \in \mathbb{Z}_p$ y $p \nmid a$, entonces $\overline{a} \in \mathbb{Z}_p^*$. Luego, $\overline{a}^{p-1} = \overline{a^{p-1}} = \overline{1}$ y en consecuencia, $a^{p-1} \equiv 1$ (mód p). □

1.3 Ejercicios de Reforzamiento

1. Considerar el anillo $\mathbb{Z}_{12}$ de los enteros módulo 12.
   a) ¿Existen divisores del cero en $\mathbb{Z}_{12}$?
   b) ¿Qué elementos de $\mathbb{Z}_{12}$ admiten inversos multiplicativos en $\mathbb{Z}_{12}$?
2. Sea $n > 1$ y $\mathbb{Z}_n$ el anillo de los enteros módulo n.
   a) Si n no es un número primo, demostrar que $\mathbb{Z}_n$ tiene divisores del cero.
   b) Si $\overline{a} \in \mathbb{Z}_n$ y a es primo relativo con n, demostrar que $\overline{a}$ tiene inverso multiplicativo en $\mathbb{Z}_n$.
3. Determinar si las siguientes afirmaciones son verdaderas o falsas.
   a) El conjunto $\mathbb{Z}[\sqrt{5}] = \{a + b\sqrt{5} \ / \ a, b \in \mathbb{Z}\}$ es un dominio de integridad con las operaciones usuales de suma y producto de números reales.
   b) El conjunto $R = \{\alpha i \ / \ \alpha \in \mathbb{R}\}$ es un anillo con las operaciones usuales de suma y producto de números complejos.
4. Sea p un número primo y $R = \{\frac{m}{n} \ / \ m, n \in \mathbb{Z}, n \neq 0$ y n no es divisible por $p\}$. Demostrar que R es un anillo con la suma y producto usual de $\mathbb{Q}$.
5. Sea R un anillo con elemento unidad $1 \neq 0$. Consideremos el conjunto $\widetilde{R} = R$ con las operaciones $\oplus$ y $\odot$ definidas como sigue: $a \oplus b = a + b + 1$ y $a \odot b = ab + a + b$ para todo $a, b \in R$.
   a) Demostrar que $\widetilde{R}$ es un anillo con elemento unidad bajo las operaciones $\oplus$ y $\odot$.
   b) Demostrar que R y $\widetilde{R}$ son anillos isomorfos.
6. Sea D un dominio de integridad, ¿es todo subanillo S de D con $S \neq \{0\}$ un dominio de integridad?
7. Sea R un anillo y $C(R) = \{a \in R \ / \ ax = xa$ para todo $x \in R\}$. Demostrar que $C(R)$ es un subanillo de R.
8. Encontrar los elementos del subanillo $C(M_{2x2}(\mathbb{Z}))$ del anillo $M_{2x2}(\mathbb{Z})$. Se deben encontrar las matrices en $M_{2x2}(\mathbb{Z})$ que conmutan con toda matriz de $M_{2x2}(\mathbb{Z})$.
9. Sea R un anillo con elemento unidad $1 \neq 0$ y U el conjunto formado por las **unidades de** R (es decir, los elementos que admiten inversos multiplicativos en R). Demostrar que $(U, \cdot)$ es un grupo.
10. Sea $n \in Z^+$ y $\sigma : \mathbb{Z} \to \mathbb{Z}_n$ definida por $\sigma(a) = \overline{r}$, donde r es el resto de la división de a por n. Demostrar que $\sigma : \mathbb{Z} \to \mathbb{Z}_n$ es un homomorfismo sobreyectivo de anillos

y encontrar $Ker(\sigma)$, ¿qué concluye, utilizando el primer teorema de isomorfismo de anillos?

11. Sean R, S anillos. Si R tiene elemento unidad 1 y $\phi : R \to S$ es un homomorfismo sobreyectivo de anillos, demostrar que $\phi(1)$ es el elemento unidad de S.
12. Demostrar que los anillos $\mathbb{Z}$ y $2\mathbb{Z}$ no son isomorfos.
13. Demostrar que $2\mathbb{Z}$ y $3\mathbb{Z}$ no son anillos isomorfos. Recordar que cuando $\phi : 2\mathbb{Z} \to 3\mathbb{Z}$ es un isomorfismo de anillos, entonces $\phi : (2\mathbb{Z}, +) \to (3\mathbb{Z}, +)$ es un isomorfismo de grupos.
14. Demostrar que los números reales $\mathbb{R}$ y los números complejos $\mathbb{C}$ no son cuerpos isomorfos.
15. Entregar un ejemplo de un anillo R tal que $x^2 = x$ para todo $x \in R$. Demostrar que los anillos que verifican la identidad anterior son conmutativos.
16. Sea R un anillo conmutativo con elemento unidad $1 \neq 0$. Demostrar que R es un cuerpo, si y solo si, $\{0\}$ es un ideal maximal de R.
17. Resolver la ecuación $5x + 2 = 0$ en el anillo $\mathbb{Z}_{23}$.
18. Sea p un número primo, ¿qué elementos del cuerpo $\mathbb{Z}_p$ satisfacen la ecuación $x^2 = 1$?
19. Construir las tablas de adición y multiplicación del anillo cuociente $2\mathbb{Z}/8\mathbb{Z}$, ¿son $2\mathbb{Z}/8\mathbb{Z}$ y $\mathbb{Z}_4$ anillos isomorfos?
20. Sea R un anillo conmutativo y $a \in R$. Demostrar que el conjunto $J_a = \{x \in R \ / \ ax = 0\}$ es un ideal de R. Si $R = \mathbb{Z}_{12}$, encontrar $J_{\overline{8}}$.
21. Sea $n > 1$, $U \neq \{0\}$ un ideal del anillo $\mathbb{Z}_n$ y a el menor entero positivo tal que $\overline{a} \in U$. Demostrar que $U =< \overline{a} >$. Encontrar todos los ideales de $\mathbb{Z}_{18}$.

Capítulo 2: Anillos de Polinomios

En los primeros cursos de álgebra, se estudian polinomios con coeficientes racionales, reales o complejos. En esta sección estudiaremos polinomios con coeficientes en un cuerpo F cualquiera. Los resultados incluidos en este capítulo dejan de manifiesto la gran similitud existente entre la estructura algebraica del conjunto de polinomios con coeficientes en F y el conjunto $\mathbb{Z}$ de los números enteros.

Sea F un cuerpo. 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 indeterminada x. Denotaremos por $F[x]$ al conjunto formado por todos los polinomios con coeficientes en un cuerpo F y utilizaremos los símbolos $f(x)$, $g(x)$,..., etc., para denotar los elementos de $F[x]$.

Iniciaremos esta sección definiendo una suma y un producto de polinomios con coeficientes en un cuerpo F y generalizaremos algunos resultados acerca de polinomios ya estudiados por los alumnos en los primeros cursos universitarios.

Demostraremos que $F[x]$ es un dominio de integridad, que en $F[x]$ es válido el Algoritmo de Euclides (también llamado Algoritmo de la División para Polinomios) y que $F[x]$ es un anillo de ideales principales. Definiremos lo que se entiende por el máximo común divisor de dos polinomios no nulos en $F[x]$ y por polinomio irreducible sobre un cuerpo F. Demostraremos que: $p(x) \in F[x]$ es irreducible sobre F, si y solo si, el anillo cuociente $F[x]/\langle p(x)\rangle$ es un cuerpo. Este importante resultado nos permitirá construir nuevos cuerpos a partir de polinomios irreducibles sobre F. Incluiremos algunos conocidos criterios de irreducibilidad, como por ejemplo, el criterio de Schöneman-Eisenstein. Finalmente, demostraremos que todo polinomio en $F[x]$ de grado ≥ 1 admite una factorización en polinomios irreducibles sobre F.

2.1 La Estructura Algebraica 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* $F[x]$.

a) Diremos que $f(x) = g(x)$, *si y solo si,* $a_i = b_i$ *para todo* $i \geq 0$.
b) Definimos $(f+g)(x) = \sum_{i=0}^{n}(a_i + b_i)x^i$. *Entonces* $(f+g)(x)$ *es un elemento en* $F[x]$.

Definición 2.2. *Sean* $f(x) = \sum_{i=0}^{n} a_i x^i$ *y* $g(x) = \sum_{i=0}^{m} b_i x^i$ *elementos en* $F[x]$. *Definimos* $(f \cdot g)(x) = \sum_{i=0}^{n+m} c_i x^i$, *donde* $c_k = \sum_{i=0}^{k} a_i b_{k-i}$. *Entonces* $(f \cdot g)(x)$ *es un elemento en* $F[x]$.

Notemos que $(f+g)(x) = f(x)+g(x)$ y que $(f\cdot g)(x) = f(x)g(x)$. Para sumar los polinomios $f(x) = 1+x+2x^2 \in \mathbb{Q}[x]$ y $g(x) = 1+x \in \mathbb{Q}[x]$, consideramos $g(x)$ como $g(x) = 1+x+0x^2$ y sumamos de acuerdo a la definición. Así, $f(x)+g(x) = 2+2x+2x^2$.

Dejamos al lector la demostración del siguiente resultado:

Lema 2.1. *El conjunto $F[x]$ es un anillo conmutativo con elemento unidad bajo las operaciones de suma y producto de polinomios, definidas anteriormente.*

Definición 2.3. *Si $f(x) = \sum_{i=0}^{n} a_i x^i$ es un elemento en $F[x]$ y $a_n \neq 0$, entonces diremos que el **grado** de $f(x)$ es n. Denotaremos $n = gr(f)$ ó $n = gr(f(x))$. No definiremos el grado del polinomio cero.*

Podemos observar que para un polinomio $f(x) \in F[x]$ se tiene la equivalencia:

$$f(x) \neq 0 \Leftrightarrow gr(f(x)) \geq 0$$

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

Teorema 2.1. *Si $f(x)$, $g(x)$ son elementos distintos de cero en $F[x]$, entonces:*

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

Demostración. Sean $f(x) = \sum_{i=0}^{n} a_i x^i$ y $g(x) = \sum_{i=0}^{m} b_i x^i$ en $F[x]$ con $a_n \neq 0$ y $b_m \neq 0$. De la definición de producto obtenemos que $f(x)g(x) = c_0 + c_1 x + \cdots + c_{n+m}x^{n+m}$, donde $c_{n+m} = a_n b_m \neq 0$. Por lo tanto, $gr(f(x)g(x)) = n+m = gr(f(x))+gr(g(x))$. □

Corolario 2.1. *El anillo $F[x]$ no tiene divisores de cero. Por lo tanto, $F[x]$ es un dominio de integridad.*

Demostración. Debemos demostrar que, si $f(x)$, $g(x)$ son elementos en $F[x]$ tales que $f(x) \neq 0$ y $g(x) \neq 0$, entonces $f(x)g(x) \neq 0$. De $gr(f(x)g(x)) = gr(f(x))+gr(g(x)) \geq 0$, obtenemos que $gr(f(x)g(x)) \geq 0$ y así, $f(x)g(x) \neq 0$. □

Como $F[x]$ es un dominio de integridad, de acuerdo a la observación 1.2, existe el cuerpo de fracciones de $F[x]$ que es usual denotar por $F(x)$. Por lo tanto,

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

Los siguientes ejercicios son de fácil demostración.

Ejercicios 2.1.

1. Sean $f(x)$, $g(x)$, $h(x)$ en $F[x]$. Si $f(x)g(x) = f(x)h(x)$ y $f(x) \neq 0$, entonces $g(x) = h(x)$.
2. Supongamos que $f(x) \in F[x]$ admite un inverso multiplicativo en $F[x]$. Demostrar que $f(x)$ es un polinomio de grado cero.

2.2 Algoritmo de Euclides

El Algoritmo de Euclides para números enteros nos afirma 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 importante resultado también es válido en el anillo de polinomios $F[x]$.

Euclides fue un matemático griego que vivió aproximadamente 300 años a.C., conocido como el "Padre de la Geometría". "Los Elementos" es una de sus obras científicas más conocidas, compuesta por 13 volúmenes, recopila gran parte del saber matemático de su época. En esta obra se incluye la construcción de lo que hoy se conoce como Geometría Euclideana.

Teorema 2.2. Algoritmo de Euclides o Algoritmo de la División.
Dados dos polinomios $f(x)$ y $g(x)$ en $F[x]$ con $g(x) \neq 0$, entonces existen únicos polinomios $q(x)$ y $r(x)$ en $F[x]$ tales que $f(x) = g(x)q(x) + r(x)$, donde $r(x) = 0$ ó $gr(r) < gr(g)$. El polinomio $r(x)$ se llama resto y $q(x)$ cuociente de la división de $f(x)$ por $g(x)$.

Demostración. La demostración se realizará por inducción sobre el grado de $f(x)$. Notemos primero que, si $f(x) = 0$ ó $gr(f) < gr(g)$ no hay nada que probar, en tal caso, basta considerar $q(x) = 0$ y $r(x) = f(x)$. Podemos suponer que

$$f(x) = a_0 + a_1x + \cdots + a_nx^n, \quad g(x) = b_0 + b_1x + \cdots + b_mx^m$$

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

Supongamos, como hipótesis de inducción, que el Teorema es válido para todos los polinomios de grados menores que n. El polinomio $f_1(x) = f(x) - (a_nb_m^{-1})x^{n-m}g(x)$ tiene grado menor que n, por la hipótesis de inducción, existen polinomios $q_1(x)$ y $r(x)$ en $F[x]$ tales que $f_1(x) = g(x)q_1(x) + r(x)$, donde $r(x) = 0$ ó $gr(r) < gr(g)$. Así,

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

de donde

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

Ahora, si consideramos $q(x) = a_nb_m^{-1}x^{n-m} - q_1(x)$, obtenemos que $f(x) = g(x)q(x) + r(x)$, donde $r(x) = 0$ ó $gr(r) < gr(g)$, lo que demuestra la existencia de los polinomios $q(x)$ y $r(x)$ en $F[x]$.

Para demostrar la unicidad de los polinomios $q(x)$ y $r(x)$ en $F[x]$, supongamos que $f(x) = g(x)q(x) + r(x) = g(x)q_0(x) + r_0(x)$ con $q_0(x)$ y $r_0(x)$ en $F[x]$, ($r(x) = 0$ ó $gr(r) < gr(g)$) y ($r_0(x) = 0$ ó $gr(r_0) < gr(g)$). Entonces

$$r(x) - r_0(x) = (q_0(x) - q(x))g(x).$$

Si suponemos que $r(x) - r_0(x) \neq 0$, entonces

$$gr(r(x) - r_0(x)) = gr((q_0(x) - q(x)) + gr(g(x)) \geq gr(g(x)).$$

Por otro lado, concluimos que $gr(r(x) - r_0(x)) < gr(g(x))$, lo que es una contradicción. Por lo tanto, $r(x) = r_0(x)$ y claramente de $(q_0(x) - q(x))g(x) = 0$ obtenemos que $q(x) = q_0(x)$. □

Ejemplo 2.1. *Sean* $f(x) = x^4 - 3x^3 + 2x^2 + 4x - 1$ *y* $g(x) = x^2 - 2x + 3$ *en* $Z_5[x]$. *Encontraremos el cuociente* $q(x)$ *y el resto* $r(x)$ *de la división de* $f(x)$ *por* $g(x)$.

$$\begin{array}{rcl} x^4 - 3x^3 + 2x^2 + 4x - 1 & : & x^2 - 2x + 3 \quad = \quad x^2 - x - 3 \\ \underline{x^4 - 2x^3 + 3x^2} & & \\ \quad -x^3 - \ x^2 + 4x - 1 & & \\ \quad \underline{-x^3 + 2x^2 - 3x} & & \\ \quad\quad -3x^2 + 2x - 1 & & \\ \quad\quad \underline{-3x^2 + \ x - 4} & & \\ \quad\quad\quad\quad x + 3 & & \end{array}$$

Por lo tanto, el cuociente es $q(x) = x^2 - x - 3$ y el resto es $r(x) = x + 3$. Notemos que efectivamente

$$\begin{aligned} (x^2 - 2x + 3)(x^2 - x - 3) + x + 3 &= x^4 - 3x^3 + 2x^2 + 4x - 6 \\ &= x^4 - 3x^3 + 2x^2 + 4x - 1. \end{aligned}$$

Ejemplo 2.2. *Sean* $f(x) = x^4 - 3x^3 + x^2 + 4$ *y* $g(x) = x - 2$ *en* $Z_7[x]$. *Encontraremos el cuociente* $q(x)$ *y el resto* $r(x)$ *de la división de* $f(x)$ *por* $g(x)$.

$$\begin{array}{rcl} x^4 - 3x^3 + x^2 + 4 & : & x - 2 \quad = \quad x^3 - x^2 - x - 2 \\ \underline{x^4 - 2x^3} & & \\ \quad -x^3 + x^2 + 4 & & \\ \quad \underline{-x^3 + 2x^2} & & \\ \quad\quad -x^2 + 4 & & \\ \quad\quad \underline{-x^2 + 2x} & & \\ \quad\quad\quad -2x + 4 & & \\ \quad\quad\quad \underline{-2x + 4} & & \\ \quad\quad\quad\quad 0 & & \end{array}$$

Por lo tanto, el cuociente es $q(x) = x^3 - x^2 - x - 2$ y el resto es $r(x) = 0$. Es decir, $x - 2$ y $x^3 - x^2 - x - 2$ son factores de $f(x)$.

Definición 2.4. *Sea* $f(x)$ *un polinomio con coeficientes en* F *y* $\alpha \in F$. *Diremos que* α *es una* ***raíz*** *(o un* ***cero****) de* $f(x)$, *si* $f(\alpha) = 0$.

Un resultado inmediato del algoritmo de Euclides es el que sigue:

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

Demostración. Supongamos que α es una raíz de $f(x)$. Por el algoritmo de Euclides, existen polinomios $q(x)$ y $r(x)$ tales que $f(x) = (x - \alpha)q(x) + r(x)$, donde $r(x) = 0$ ó $gr(r) < gr(x - \alpha) = 1$. Así, $r(x) = 0$ ó $gr(r) = 0$, de donde $r(x) = a_0 \in F$. Dado que α es una raíz de $f(x)$, obtenemos que $0 = f(\alpha) = (\alpha - \alpha)q(\alpha) + r(\alpha) = r(\alpha)$. Por lo tanto, $a_0 = 0$ y $f(x) = (x - \alpha)q(x)$. El recíproco es inmediato. □

Definición 2.5. *Un cuerpo F es* ***algebraicamente cerrado****, si todo polinomio no constante (es decir, todo polinomio de grado ≥ 1) en $F[x]$ tiene a lo menos una raíz en F.*

Corolario 2.3. *Sea F un cuerpo algebraicamente cerrado. Si $f(x) \in F[x]$ y $gr(f) = n \geq 1$, entonces existen elementos d, α_1, $\alpha_2, \ldots, \alpha_n$ en F tales que*

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

Demostración. La demostración se realizará por inducción sobre el grado de $f(x)$. Si $gr(f) = 1$, entonces $f(x) = ax+b$ con $a, b \in F$ y $a \neq 0$. Luego, $f(x) = a(x-(-a^{-1}b))$. Supongamos, como hipótesis de inducción, que el Corolario es verdadero para todos los polinomios no constantes de grado menor que n y sea $gr(f) = n > 1$. Como F es algebraicamente cerrado existe $\alpha_n \in F$ raíz de $f(x)$. Por el Corolario 2.2, existe $q(x) \in F[x]$ tal que $f(x) = (x-\alpha_n)q(x)$. Dado que $gr(q) = n-1$, entonces por la hipótesis de inducción, existen elementos d, α_1, $\alpha_2, ..., \alpha_{n-1}$ en F tales que

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

Por lo tanto,

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

□

Teorema 2.3. *Un polinomio $f(x) \in F[x]$ de grado $n \geq 1$ tiene a lo más n raíces en F.*

Demostración. Probaremos este resultado por inducción sobre el grado de $f(x)$. Si $gr(f) = 1$, es decir $f(x) = ax + b$ con a, b en F y $a \neq 0$, entonces $-a^{-1}b \in F$ es la única raíz de $f(x)$. Supongamos, como hipótesis de inducción, que el teorema es verdadero para todos los polinomios no constantes de grado menor que n y sea $gr(f) = n > 1$. Si $f(x)$ tiene una raíz $\alpha \in F$, entonces por el Corolario 2.2, existe un polinomio $q(x) \in F[x]$ tal que $f(x) = (x-\alpha)q(x)$, donde $gr(q) = n-1$. Cualquier raíz $\beta \in F$ de $f(x)$ distinta de α es una raíz de $q(x)$. En efecto, $f(\beta) = (\beta-\alpha)q(\beta) = 0$ implica $q(\beta) = 0$. De nuestra hipótesis de inducción, $q(x)$ tiene a lo más $n-1$ raíces. Dado que las raíces de $f(x)$ son α y las raíces de $q(x)$, concluimos que $f(x)$ tiene a lo más n raíces en F. □

Definición 2.6. *Sea $f(x)$ un polinomio con coeficientes en F y $\alpha \in F$. Diremos que α como raíz de $f(x)$ tiene* ***multiplicidad*** *$m \geq 1$, si existe $q(x) \in F[x]$ tal que $f(x) = (x-\alpha)^m q(x)$ con $q(\alpha) \neq 0$.*

La primera demostración conocida del teorema que sigue, llamado "Teorema Fundamental del Álgebra", fue dada por Gauss en 1799. Posteriormente, en 1849, Gauss dio a conocer una nueva versión de su demostración original.

Johann Carl Friedrich Gauss (1777-1855), fue un matemático, físico y astrónomo alemán. En 1801 publicó el libro "Disquisitiones Arithmeticae" en gran parte dedicado a la teoría de números, dándole a esta rama de las matemáticas una estructura sistematizada.

En esta monografía sólo enunciaremos el teorema que sigue, debido a que su demostración requiere herramientas matemáticas más avanzadas de las que disponemos.

Teorema 2.4. Teorema Fundamental del Álgebra.
Si $f(x)$ es un polinomio no constante con coeficientes en el cuerpo de los complejos $\mathbb{C}$, entonces $f(x)$ tiene a lo menos una raíz en $\mathbb{C}$. En consecuencia, $\mathbb{C}$ es un cuerpo algebraicamente cerrado y el Corolario 2.3 es válido si reemplazamos F por $\mathbb{C}$.

2.3 Máximo Común Divisor

Teorema 2.5. *$F[x]$ es 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. Si $J = \{0\}$, entonces $J = \langle 0 \rangle$. Supongamos que $J \neq \{0\}$. Elijamos un polinomio no nulo $g(x) \in J$ con la siguiente propiedad: si $h(x) \in J$ y $h(x) \neq 0$, entonces $gr(g) \leq gr(h)$. Demostraremos que $J = \langle g(x) \rangle$. Sea $f(x) \in J$. Por el algoritmo de Euclides, existen $q(x)$, $r(x)$ en $F[x]$ tales que $f(x) = g(x)q(x) + r(x)$, donde $r(x) = 0$ ó $gr(r) < gr(g)$. Como J es un ideal de $F[x]$, entonces $r(x) = f(x) - g(x)q(x)$ es un elemento en J. Por la elección de $g(x)$ y dado que $r(x) = 0$ ó $gr(r) < gr(g)$, obtenemos que $r(x) = 0$. Así, $f(x) = g(x)q(x)$ y por lo tanto, $J = \langle g(x) \rangle$. □

Observación 2.1. *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 $gr(g_1) = gr(g_2) + gr(q)$, entonces $gr(g_1) \geq gr(g_2)$. Por el mismo argumento, obtenemos que $gr(g_2) \geq gr(g_1)$. Por lo tanto, $gr(g_1) = gr(g_2)$ y así, $q(x) = a \in F$ 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. Es claro que este generador es único.*

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

Definición 2.8. *Sean $f_1(x)$, $f_2(x)$ en $F[x]$ 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. $g(x) \mid f_1(x)$ *y* $g(x) \mid f_2(x)$,
2. $h(x) \in F[x]$ *y* $h(x) \mid f_1(x)$ *y* $h(x) \mid f_2(x)$, *entonces* $h(x) \mid g(x)$.

Podemos observar que necesariamente $g(x) \neq 0$, pues $f_1(x)f_2(x) \neq 0$.

Teorema 2.6. *Sean* $f_1(x)$, $f_2(x)$ *en* $F[x]$ *con* $f_1(x)f_2(x) \neq 0$. *Entonces existe un máximo común divisor* $g(x) \in F[x]$ *de* $f_1(x)$ *y* $f_2(x)$. *Además, existen polinomios* $q(x)$, $t(x)$ *en* $F[x]$ *tales que* $g(x) = f_1(x)q(x) + f_2(x)t(x)$.

Demostración. Como $F[x]$ es un anillo de ideales principales, entonces existe un generador $g(x) \in F[x]$ del ideal $\langle f_1(x), f_2(x)\rangle$ de $F[x]$. Demostraremos que $g(x)$ es un máximo común divisor de $f_1(x)$ y $f_2(x)$.

Claramente $g(x) \neq 0$. Como $\langle g(x)\rangle = \langle f_1(x), f_2(x)\rangle$, entonces $f_1(x) \in \langle g(x)\rangle$ y $f_2(x) \in \langle g(x)\rangle$, de donde existen $q(x)$ y $t(x)$ en $F[x]$ tales que $f_1(x) = g(x)q(x)$ y $f_2(x) = g(x)t(x)$. Por lo tanto, $g(x) \mid f_1(x)$ y $g(x) \mid f_2(x)$, lo que demuestra (1) de la definición 2.8. Dado que $g(x) \in \langle f_1(x), f_2(x)\rangle$, existen $q(x)$ y $t(x)$ en $F[x]$ tales que $g(x) = f_1(x)q(x) + f_2(x)t(x)$.

Para demostrar (2) de la definición 2.8, consideremos $h(x) \in F[x]$ tal que $h(x) \mid f_1(x)$ y $h(x) \mid f_2(x)$. Existen $q_0(x)$, $t_0(x)$ en $F[x]$ tales que $f_1(x) = h(x)q_0(x)$ y $f_2(x) = h(x)t_0(x)$. Ahora,

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

de donde

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

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

Observación 2.2. *Si en la demostración del teorema anterior* $g(x) = a_0 + a_1x + \cdots + a_nx^n$ *con* $a_n \neq 0$, *entonces* $a_n^{-1}g(x)$ *es también generador de* J *y en consecuencia, el polinomio mónico* $a_n^{-1}g(x)$, *que es único, también es un máximo común divisor de* $f_1(x)$ *y* $f_2(x)$. *Diremos que un máximo común divisor mónico es* ***el máximo común divisor de*** $f_1(x)$, $f_2(x)$ *y lo denotaremos por* $(f_1(x), f_2(x))$.

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

Como es sabido, utilizando sucesivamente el algoritmo de Euclides, es posible calcular el máximo común divisor de dos enteros no nulos. En forma absolutamente similar, es posible obtener un máximo común divisor para dos polinomios no nulos en $F[x]$. La demostración del algoritmo que sigue se deja como ejercicio para el lector.

Lema 2.2. *Sean* $f(x)$, $g(x)$ *en* $F[x]$ *ambos no nulos. Utilizando el algoritmo de Euclides sucesivamente tenemos que*

$f(x) = g(x)q_1(x) + r_1(x)$, *donde* $r_1(x) = 0$ *ó* $gr(r_1) < gr(g)$,
$g(x) = r_1(x)q_2(x) + r_2(x)$, *donde* $r_2(x) = 0$ *ó* $gr(r_2) < gr(r_1)$,

$r_1(x) = r_2(x)q_3(x) + r_3(x)$, *donde* $r_3(x) = 0$ *ó* $gr(r_3) < gr(r_2)$,

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

$r_{n-1}(x) = r_n(x)q_{n+1}(x) + r_{n+1}(x)$, *donde* $r_{n+1}(x) = 0$ *ó* $gr(r_{n+1}) < gr(r_n)$.

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

Ejemplo 2.3. *Calcularemos el máximo común divisor de los polinomios*

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

sobre el cuerpo de los números racionales. Utilizando el algoritmo del Lema 2.2, tenemos que

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

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

Por lo tanto, $15x^2 + 15x + 30$ *es un máximo común divisor de* $f(x)$ *y* $g(x)$. *Es claro que* $x^2 + x + 2$ *es el máximo común divisor de* $f(x)$ *y* $g(x)$.

Ejemplo 2.4. *Calcularemos el máximo común divisor* $d(x)$ *de los polinomios*

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

sobre el cuerpo $\mathbb{Z}_{11}$ *de los enteros módulo 11. Encontraremos polinomios* $u(x)$, $v(x)$ *en* $\mathbb{Z}_{11}[x]$ *tales que* $f(x)u(x) + g(x)v(x) = d(x)$. *Por el algoritmo del Lema 2.2, tenemos que*

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

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

$4x^2 + 7x - 4 = (2x - 8)(2x + 6)$.

Así, $2x - 8$ *es un máximo común divisor de* $f(x)$ *y* $g(x)$. *Dado que* $6(2x - 8) = x - 4$, *concluimos que* $x - 4$ *es el máximo común divisor de* $f(x)$ *y* $g(x)$. *Ahora,*

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

Así,

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

Multiplicando esta última expresión por $6 \in \mathbb{Z}_{11}$, *obtenemos que*

$$f(x)(4x + 4) + g(x)(-4x^3 + x^2 + 6x - 4) = x - 4.$$

Ejercicios 2.2.

1. Sean $f(x) = x^3 - 6x^2 + x + 4$ y $g(x) = x^5 - 6x + 1$ polinomios con coeficientes en el cuerpo de los racionales $\mathbb{Q}$. Encontrar polinomios $u(x)$, $v(x)$ en $\mathbb{Q}[x]$ tales que $f(x)u(x) + g(x)v(x) = d(x)$, donde $d(x)$ es el máximo común divisor de $f(x)$ y $g(x)$.
2. Sean $f(x) = x^2 + 1$ y $g(x) = x^6 + x^3 + x + 1$ polinomios con coeficientes en el cuerpo de los reales $\mathbb{R}$. Encontrar un generador para el ideal $\langle f(x), g(x)\rangle$ de $\mathbb{R}[x]$.
3. Supongamos que $f(x)$, $g(x)$ en $\mathbb{Q}[x]$ son primos relativos en $\mathbb{Q}[x]$. Demostrar que son primos relativos en $\mathbb{R}[x]$.

2.4 Polinomios Irreducibles

Como veremos más adelante, los polinomios irreducibles juegan un rol importante en la Teoría de Cuerpos. Nos interesa conocer aquellos polinomios $f(x) \in F[x]$ con $gr(f) = n \geq 1$, que no se pueden escribir como el producto de dos polinomios en $F[x]$ de grados menores que n. Estudiaremos algunos criterios para determinar dichos polinomios.

Definición 2.9. *Sea $f(x) \in F[x]$ con $gr(f) \geq 1$. Diremos que $f(x)$ es **irreducible sobre** F o **irreducible en** $F[x]$, si no existen polinomios $g(x)$, $h(x)$ en $F[x]$ tales que $f(x) = g(x)h(x)$ con $gr(g) < gr(f)$ y $gr(h) < gr(f)$. Si existen tales polinomios se dice que $f(x)$ es **reducible** sobre F o **reducible** en $F[x]$.*

Ejemplo 2.5. *Consideremos el polinomio $f(x) = x^2 + 2 \in \mathbb{R}[x]$, donde $\mathbb{R}$ es el cuerpo de los números reales. Supongamos que $f(x)$ se puede escribir como el producto de dos polinomios $g(x)$ y $h(x)$ en $\mathbb{R}[x]$ con $gr(g) < 2$ y $gr(h) < 2$. Necesariamente $g(x) = ax + b$ y $h(x) = cx + d$ con a, b, c, $d \in \mathbb{R}$, $a \neq 0$ y $c \neq 0$. Luego,*

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

Por la igualdad de polinomios obtenemos que $ac = 1$. Sean $\frac{b}{a} = \alpha$ y $\frac{d}{c} = \beta$. Así, tenemos que $x^2 + 2 = (x + \alpha)(x + \beta) = x^2 + (\alpha + \beta)x + \alpha\beta$, de donde $\alpha + \beta = 0$ y $\alpha\beta = 2$. Luego, $\alpha^2 = -2$ con $\alpha \in \mathbb{R}$, lo que es una contradicción. En consecuencia, $f(x) = x^2 + 2$ es irreducible sobre $\mathbb{R}$ o irreducible en $\mathbb{R}[x]$.

Observemos que la irreducibilidad de un polinomio depende del cuerpo. Como se demostró en el ejemplo anterior, el polinomio $f(x) = x^2 + 2$ es irreducible sobre el cuerpo de los reales, sin embargo, $f(x) = x^2 + 2$ es reducible sobre el cuerpo de los números complejos $\mathbb{C}$. En efecto, $x^2 + 2 = (x + \sqrt{2}i)(x - \sqrt{2}i)$.

Observación 2.3. *Los polinomios con coeficientes en $\mathbb{C}$ y de grados ≥ 2 son reducibles sobre $\mathbb{C}$. La afirmación anterior es una conclusión inmediata del Teorema Fundamental del Álgebra, como se demuestra a continuación. Si $f(x) \in \mathbb{C}[x]$ y $gr(f) = n \geq 2$, entonces por el teorema antes mencionado, existe una raíz $\alpha \in \mathbb{C}$ de $f(x)$. Así, existe un polinomio $q(x) \in \mathbb{C}[x]$ tal que $f(x) = (x - \alpha)q(x)$. Ahora, $gr(x - \alpha) < n$ y $gr(q) = n - 1 < n$, lo que demuestra que $f(x)$ es reducible sobre $\mathbb{C}$.*

Lema 2.3. *Sea $h(x) \in F[x]$ un polinomio de grado 2 (o de grado 3). Entonces, $h(x)$ es reducible en $F[x]$, si y solo si, $h(x)$ tiene una raíz en F.*

Demostración. Sea $h(x)$ reducible en $F[x]$. Existen un polinomio de la forma $ax + b \in F[x]$ con $a \neq 0$ y un polinomio $q(x) \in F[x]$ de grado 1 (o grado 2) tal que $h(x) = (ax + b)q(x)$. Ahora, $\alpha = -\frac{b}{a} \in F$ es una raíz de $h(x)$.

Recíprocamente, si suponemos que $\alpha \in F$ es una raíz de $h(x)$, entonces por el Corolario 2.2, existe un polinomio $q(x)$ en $F[x]$ tal que $h(x) = (x - \alpha)q(x)$ con $gr(q) = 1$ (o $gr(q) = 2$). Por lo tanto, $h(x)$ es reducible en $F[x]$. □

Ejemplo 2.6. *El polinomio $g(x) = x^3 + 4x^2 + 4x + 1 \in \mathbb{Z}_5[x]$ es reducible sobre $\mathbb{Z}_5$. En efecto, $g(1) = 1 + 4 + 4 + 1 = 0$ y luego, existe un polinomio $q(x) \in \mathbb{Z}_5[x]$ con $gr(q) = 2$ tal que $g(x) = (x - 1)q(x)$.*

Ejemplo 2.7. *El polinomio $p(x) = x^3 + 3x + 2 \in \mathbb{Z}_5[x]$ es irreducible sobre $\mathbb{Z}_5$. En efecto, $p(0) = 2$, $p(1) = 1$, $p(2) = 1$, $p(3) = 2$ y $p(4) = 3$. Es decir, $p(x)$ no tiene raíces en $\mathbb{Z}_5$. De acuerdo al Lema 2.3, la afirmación es verdadera.*

Ejemplo 2.8. *El polinomio $f(x) = x^4 + 2x^2 + 1 \in \mathbb{R}[x]$ no tiene raíces en $\mathbb{R}$, sin embargo es reducible en $\mathbb{R}[x]$, dado que $f(x) = (x^2+1)(x^2+1)$. Por lo tanto, el Lema 2.3 no es válido para polinomios de grados ≥ 4.*

Ejemplo 2.9. *Sea $f(x) \in \mathbb{R}[x]$ mónico irreducible y $gr(f) = 2$. Demostraremos que $f(x)$ se puede escribir en la forma $f(x) = (x - a)^2 + b^2$ con $a, b \in \mathbb{R}$ y $b \neq 0$. Recíprocamente, probaremos que tal polinomio es irreducible sobre $\mathbb{R}$. Supongamos que $f(x) \in \mathbb{R}[x]$ es mónico irreducible y $gr(f) = 2$. Entonces $f(x) = x^2 + cx + d \in \mathbb{R}[x]$. Ahora*

$$\begin{aligned} f(x) &= x^2 + cx + d = (x + \frac{1}{2}c)^2 + d - \frac{1}{4}c^2 \\ &= (x + \frac{1}{2}c)^2 + \frac{1}{4}(4d - c^2). \end{aligned}$$

Del Lema 2.3, $f(x)$ no puede tener raíces en $\mathbb{R}$. En consecuencia, necesariamente $4d - c^2 > 0$. Definiendo $a = -\frac{1}{2}c$ y $b = \frac{1}{2}\sqrt{4d - c^2}$, obtenemos lo deseado.

Inversamente, si $f(x) = (x - a)^2 + b^2$ con $a, b \in \mathbb{R}$ y $b \neq 0$, entonces $f(\alpha) > 0$ para todo $\alpha \in \mathbb{R}$ y luego, $f(x)$ no tiene raíces en $\mathbb{R}$. Del Lema 2.3, concluimos que $f(x)$ es irreducible sobre $\mathbb{R}$.

Ejemplo 2.10. *Sea $f(x) = x^4 + 1 \in \mathbb{Z}_5[x]$. Determinaremos si $f(x)$ es reducible o irreducible sobre $\mathbb{Z}_5$. Dado que $f(0) = 1$, $f(1) = 2$, $f(2) = 2$, $f(3) = 2$ y $f(4) = 2$, entonces no existen polinomios $g(x)$, $h(x)$ en $\mathbb{Z}_5[x]$ tales que $f(x) = g(x)h(x)$ con $gr(g) = 1$ y $gr(h) = 3$. Supongamos que*

$$f(x) = (x^2 + ax + b)(x^2 + cx + d)$$

con a, b, c, d en $\mathbb{Z}_5$. Entonces

$$x^4 + 1 = x^4 + (a + c)x^3 + (b + d + ac)x^2 + (ad + bc)x + bd,$$

de donde $a + c = 0$, $b + d + ac = 0$, $ad + bc = 0$ *y* $bd = 1$. *Como* $a = -c$, *entonces* $bc - cd = c(b - d) = 0$. *Luego,* $c = 0$ *o* $b = d$. *Si* $c = 0$, *entonces* $b + d = 0$ *y* $bd = 1$. *Vemos que* $b = 2$ *y* $d = 3$ *verifican las relaciones anteriores. Por lo tanto,* $f(x) = (x^2 + 2)(x^2 + 3)$ *y así,* $f(x)$ *es reducible sobre* $\mathbb{Z}_5$.

Ejercicios 2.3.

1. Todo polinomio en $F[x]$ de grado 1 es irreducible sobre F.
2. Encontrar todos los polinomios irreducibles de grados 2 ó 3 en $\mathbb{Z}_2[x]$ y $\mathbb{Z}_3[x]$.
3. ¿Es $f(x) = 2x^3 + x^2 + 2x + 2 \in \mathbb{Z}_5[x]$ un polinomio irreducible sobre $\mathbb{Z}_5$?
4. Si $\alpha \in F$ con $\alpha \neq 0$ es una raíz de $f(x) = a_0 + a_1x + \cdots + a_nx^n \in F[x]$, demostrar que α^{-1} es una raíz de $g(x) = a_n + a_{n-1}x + \cdots + a_0x^n$.
5. Sean $f(x)$, $g(x)$ en $F[x]$ no nulos tales que $f(x) \mid g(x)$ y $g(x) \mid f(x)$. Demostrar que $f(x) = ag(x)$ con $a \in F$ no nulo.

Teorema 2.7. *Sea* $p(x) \in F[x]$ *con* $gr(p) \geq 1$. *Entonces* $\langle p(x) \rangle$ *es un ideal maximal de* $F[x]$, *si y solo si,* $p(x)$ *es irreducible sobre* F.

Demostración. Notemos que el teorema es equivalente a demostrar que: $\langle p(x) \rangle$ no es ideal maximal de $F[x]$, si y solo si, $p(x)$ es reducible sobre F.

Supongamos que el ideal $\langle p(x) \rangle$ no es ideal maximal de $F[x]$. Entonces existe un ideal U de $F[x]$ tal que $\langle p(x) \rangle \subset U$ con $\langle p(x) \rangle \neq U$ y $U \neq F[x]$. Como $F[x]$ es un dominio de ideales principales, existe un $g(x) \in F[x]$ tal que $U = \langle g(x) \rangle$. Ahora $\langle p(x) \rangle \subset \langle g(x) \rangle$, de donde $p(x) = g(x)h(x)$ con $h(x) \in F[x]$. Notemos que, si $g(x)$ es constante, entonces $U = F[x]$, una contradicción. Ahora, si $h(x)$ es constante, entonces $\langle p(x) \rangle = U$, una contradicción. Por lo tanto, necesariamente $gr(g) \geq 1$ y $gr(h) \geq 1$. Concluimos que $p(x) = g(x)h(x)$ con $gr(g) < gr(p)$ y $gr(h) < gr(p)$, es decir, $p(x)$ es reducible sobre F.

Recíprocamente, supongamos que $p(x)$ es reducible sobre F. Existen polinomios $g(x)$, $h(x)$ en $F[x]$ tales que $p(x) = g(x)h(x)$ con $gr(g) < gr(p)$ y $gr(h) < gr(p)$. Notemos que $gr(g) > 0$ y $gr(h) > 0$, de lo contrario $gr(g) = gr(p)$ ó $gr(h) = gr(p)$. Claramente $\langle p(x) \rangle \subset \langle g(x) \rangle$ *y* $\langle g(x) \rangle \neq F[x]$, esto último, dado que $1 \notin \langle g(x) \rangle$. Ahora $g(x) \notin \langle p(x) \rangle$. En efecto, si suponemos que $g(x) \in \langle p(x) \rangle$, entonces $g(x) = p(x)q(x)$ con $q(x) \in F[x]$. Así, $p(x) = g(x)h(x) = p(x)q(x)h(x)$, lo cual implica que $q(x)h(x) = 1$, dado que $p(x) \neq 0$ y $F[x]$ no tiene divisores cero. De $q(x)h(x) = 1$, concluimos que $gr(q) = gr(h) = 0$, lo que es una contradicción. Por lo tanto, $g(x) \notin \langle p(x) \rangle$ y así, $\langle p(x) \rangle \neq \langle g(x) \rangle$. Hemos demostrado que $\langle p(x) \rangle$ no es ideal maximal de $F[x]$. □

Un importante resultado es el que se obtiene de los Teoremas 1.2 y 2.7, que nos permitirá la construcción de nuevos cuerpos a partir de polinomios irreducibles.

Corolario 2.4. *Sea* $p(x) \in F[x]$ *con* $gr(p) \geq 1$. *Entonces* $p(x)$ *es irreducible sobre* F, *si y solo si,* $F[x] / \langle p(x) \rangle$ *es un cuerpo.*

Las demostraciones de los siguientes resultados quedan como ejercicios.

Ejercicios 2.4.

1. Sea $f(x) \in \mathbb{R}[x]$. Si $z \in \mathbb{C}$ es una raíz de $f(x)$, entonces el conjugado de z también es raíz de $f(x)$.
2. Sea $f(x) \in \mathbb{R}[x]$ no nulo. Si $a + bi \in \mathbb{C}$ con a, $b \in \mathbb{R}$ y $b \neq 0$ es una raíz de $f(x)$, entonces $x^2 - 2ax + a^2 + b^2$ es un factor de $f(x)$.
3. Si $f(x) \in \mathbb{R}[x]$ tiene grado impar, entonces $f(x)$ tiene al menos una raíz real.
4. Si $f(x) \in \mathbb{R}[x]$ y $\text{gr}(f(x)) \geq 3$, entonces $f(x)$ es reducible sobre $\mathbb{R}$.
5. Sea $f(x) = a_0 + a_1x + \cdots + a_nx^n$ con a_0, a_1, ..., a_n números enteros y $a_0a_n \neq 0$. Si $\frac{a}{b}$ con $a, b \in \mathbb{Z}$ y $(a, b) = 1$ es una raíz de $f(x)$, entonces a es un divisor de a_0 y b es un divisor de a_n.
6. Sea F un cuerpo, $f(x) \in F[x]$ con $gr(f) \geq 1$ y $a \in F$ no nulo. Demostrar que: $f(x)$ es irreducible sobre F, si y solo si, $af(x)$ es irreducible sobre F.

Si $p(x)$ es un polinomio irreducible sobre un cuerpo F, entonces por el Corolario 2.4, $F[x]/\langle p(x)\rangle$ es un cuerpo. Demostraremos a continuación que, dado un elemento $f(x) + \langle p(x)\rangle$ en $F[x]/\langle p(x)\rangle$, siempre existe un polinomio $g(x) \in F[x]$ tal que $f(x) + \langle p(x)\rangle = g(x) + \langle p(x)\rangle$, donde $g(x) = 0$ ó $gr(g) < gr(p)$.

Lema 2.4. *Sea F cuerpo, $p(x) \in F[x]$ irreducible sobre F y $gr(p) = n$. Entonces*

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

Demostración Sea $f(x) + \langle p(x)\rangle$ un elemento en $F[x]/\langle p(x)\rangle$. Por el algoritmo de Euclides, existen $q(x)$, $r(x)$ en $F[x]$ tales que $f(x) = p(x)q(x) + r(x)$, donde $r(x) = 0$ ó $gr(r) < gr(p)$. 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 $gr(r) < n$, 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,

$$f(x) + \langle p(x)\rangle = a_0 + a_1x + \cdots + a_{n-1}x^{n-1} + \langle p(x)\rangle . \qquad \square$$

Ejemplo 2.11. *Sea $p(x) = x^3 - 2 \in \mathbb{Q}[x]$. Demostraremos que el anillo cuociente $\mathbb{Q}[x]/\langle p(x)\rangle$ es un cuerpo y encontraremos el inverso multiplicativo del elemento $2 + 3x - 5x^2 + \langle p(x)\rangle \in \mathbb{Q}[x]/\langle p(x)\rangle$.*

Para demostrar que el anillo cuociente $\mathbb{Q}[x]/\langle p(x)\rangle$ es un cuerpo, por el Corolario 2.4, basta probar que $p(x) = x^3 - 2$ es irreducible sobre $\mathbb{Q}$. Las posibles raíces en $\mathbb{Q}$ de $p(x) = x^3 - 2$ son ± 1, ± 2. Como ninguno de estos enteros es una raíz de $p(x)$, concluimos (Lema 2.3) que $p(x)$ es irreducible sobre $\mathbb{Q}$.

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

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

lo que es equivalente a

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

es decir,

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

Dividiendo el polinomio

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

por x^3-2 *obtenemos que el cuociente de la división es*

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

y el resto es

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

Deseamos que $r(x)=0$. *Luego, se obtiene el sistema de ecuaciones*

$$-5a+3b+2c=0,\ 3a+2b-10c=0 \text{ y } 2a-10b+6c=1,$$

de donde $a=-\frac{17}{129}$, $b=-\frac{22}{129}$ *y* $c=-\frac{19}{258}$. *Por lo tanto,*

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

Ejemplo 2.12. *Sea* $p(x)=x^3+x^2+x+2\in\mathbb{Z}_7[x]$. *Demostraremos que el anillo cuociente* $\mathbb{Z}_7[x]\diagup\langle p(x)\rangle$ *es un cuerpo con* 7^3 *elementos y encontraremos el inverso multiplicativo del elemento* $2+3x+5x^2+(p(x))\in\mathbb{Z}_7[x]\diagup\langle p(x)\rangle$.

De $p(0)=2$, $p(1)=5$, $p(2)=2$, $p(3)=6$, $p(4)=2$, $p(5)=3$ *y* $p(6)=1$, *obtenemos que* $p(x)$ *no tiene raíces en el cuerpo* $\mathbb{Z}_7$ *y por lo tanto,* $p(x)=x^3+x^2+x+2$ *es irreducible sobre* $\mathbb{Z}_7$. *Por el Corolario 2.4,* $\mathbb{Z}_7[x]\diagup\langle p(x)\rangle$ *es un cuerpo y del Lema 2.4,*

$$\mathbb{Z}_7[x]\diagup\langle p(x)\rangle=\{a+bx+cx^2+\langle p(x)\rangle\,/a,b,c\in\mathbb{Z}_7\}$$

tiene 7^3 *elementos. Encontraremos*

$$(2+3x+5x^2+\langle p(x)\rangle)^{-1}\in\mathbb{Z}_7[x]\diagup\langle p(x)\rangle\,.$$

Deseamos encontrar elementos a, b, $c\in\mathbb{Z}_7$ *tales que*

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

equivalente a

(1) $2a+(3a+2b)x+(5a+3b+2c)x^2+(5b+3c)x^3+5cx^4+\langle p(x)\rangle=1+\langle p(x)\rangle\,.$

Aún cuando podemos encontrar los elementos a, b, $c\in\mathbb{Z}_7$, *utilizando los mismos argumentos empleados en la resolución del ejemplo anterior, desarrollaremos este problema de una forma diferente, para lo cual denotaremos un elemento cualquiera* $f(x)+\langle p(x)\rangle\in\mathbb{Z}_7[x]\diagup\langle p(x)\rangle$ *por* $\overline{f(x)}$. *Así, podemos escribir* (1) *de la forma*

$$\overline{2a+(3a+2b)x+(5a+3b+2c)x^2+(5b+3c)x^3+5cx^4}=\overline{1},$$

lo que es equivalente a

(2) $$\overline{2a}+\overline{(3a+2b)}\overline{x}+\overline{(5a+3b+2c)x^2}+\overline{(5b+3c)x^3}+\overline{5c}\overline{x^4}-\overline{1}=\overline{0}.$$

Dado que $x^3+\langle p(x)\rangle = -x^2-x-2+\langle p(x)\rangle$ *, es decir,* $\overline{x^3} = \overline{-x^2-x-2} = -\overline{x^2}-\overline{x}-\overline{2}$, *obtenemos que*

$$\overline{x^4} = \overline{x}\overline{x^3} = \overline{x}(-\overline{x^2}-\overline{x}-\overline{2}) = -\overline{x^3}-\overline{x^2}-\overline{2x} = -(-\overline{x^2}-\overline{x}-\overline{2})-\overline{x^2}-\overline{2x} = -\overline{x}+\overline{2}.$$

Reemplazando $\overline{x^3}$ *por* $-\overline{x^2}-\overline{x}-\overline{1}$ *y* $\overline{x^4}$ *por* $\overline{1}$ *en* (2) *, obtenemos*

$$\begin{aligned}\overline{0} &= \overline{2a}+\overline{(3a+2b)}\overline{x}+\overline{(5a+3b+2c)x^2}+\overline{(5b+3c)}(-\overline{x^2}-\overline{x}-\overline{2})+\overline{5c}(-\overline{x}+\overline{2})-\overline{1}\\ &= \overline{2a+(3a+2b)x+(5a+3b+2c)x^2+(5b+3c)(-x^2-x-2)+5c(2-x)-1}\\ &= \overline{(2a-3b+4c-1)+(3a-3b-c)x+(5a-2b-c)x^2}.\end{aligned}$$

Así,

$$(2a-3b+4c-1)+(3a-3b-c)x+(5a-2b-c)x^2+\langle p(x)\rangle = 0+\langle p(x)\rangle$$

es equivalente a

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

Luego,

$$\begin{aligned}2a-3b+4c-1 &= 0\\ 3a-3b-c &= 0\\ 5a-2b-c &= 0.\end{aligned}$$

Resolviendo este sistema en el cuerpo $\mathbb{Z}_7$*, obtenemos* $a=4$*,* $b=-1$ *y* $c=1$*. Por lo tanto,* $(2+3x+5x^2+\langle p(x)\rangle)^{-1} = 4-x+x^2+\langle p(x)\rangle \in \mathbb{Z}_7[x]/\langle p(x)\rangle$.

En general, no es fácil determinar si un polinomio $f(x)\in\mathbb{Q}[x]$ con $gr(f)\geq 4$ es irreducible o reducible en $\mathbb{Q}[x]$. Existen conocidos resultados que son buenas herramientas para intentar resolver este problema. Estos resultados son los Teoremas 2.8, 2.9 y el Corolario 2.5, que se enuncian a continuación (ver demostraciones en [5] , [6]), debiéndose el primero de ellos a Gauss.

Teorema 2.8. *Si un polinomio mónico* $f(x)$ *con coeficientes enteros se factoriza como el producto de dos polinomios no constantes con coeficientes racionales, entonces se factoriza como el producto de dos polinomios mónicos con coeficientes enteros.*

Ejemplo 2.13. *Determinaremos si el polinomio* $f(x)=x^4+4\in\mathbb{Q}[x]$ *es reducible o irreducible sobre* $\mathbb{Q}$*. Claramente* $f(x)$ *no tiene raíces racionales, en consecuencia no se puede factorizar como el producto de un polinomio de grado* 1 *y un polinomio de grado 3 sobre* $\mathbb{Q}$*. Si* $f(x)$ *admite una factorización como el producto de dos polinomios de grado* 2 *sobre* $\mathbb{Q}$*, entonces por el Teorema 2.8, existen polinomios mónicos* $u(x)$*,* $v(x)$ *con coeficientes enteros tales que* $f(x)=u(x)v(x)$*. Por lo tanto,* $x^4+4=(x^2+ax+b)(x^2+cx+d)$ *con* a*,* b*,* c*,* d *enteros. Así,* $a+c=0$*,* $b+d+ac=0$*,* $ad+bc=0$ *y* $bd=4$*. Por lo tanto,* $a(d-b)=0$*. Si* $a=0$*, obtenemos* $b^2=-4$*, lo que es una contradicción. Luego,* $a\neq 0$*, de donde* $b^2=4$*. Así,* $b=2$ *ó* $b=-2$*. Si* $b=2$*, entonces* $d=2$ *y* $a^2=4$*. Como* $x^4+4=(x^2+2x+2)(x^2-2x+2)$*, entonces* $f(x)$ *es reducible sobre* $\mathbb{Q}$*.*

El siguiente teorema fue publicado por Schöneman en 1846 e independientemente por Eisenstein en 1850. Ferdinand Eisenstein (1823-1852) fue un matemático alemán que realizó importantes contribuciones en la teoría de formas cuadráticas y funciones elípticas.

Teorema 2.9. El criterio de Schöneman-Eisenstein.
Sea $f(x) = a_0 + a_1x + \cdots + a_nx^n$ *un polinomio no constante con coeficientes enteros. Supongamos que para algún número primo* p *se tiene que* $p \nmid a_n$, p *es un divisor de* $a_0, a_1, \ldots, a_{n-1}$ *y* $p^2 \nmid a_0$. *Entonces* $f(x)$ *es irreducible sobre los racionales.*

Corolario 2.5. *El polinomio* $\phi_p(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$ *es irreducible sobre* $\mathbb{Q}$ *para todo número primo* p.

Ejemplo 2.14. *Sea* $f(x) = \frac{2}{9}x^5 + \frac{5}{3}x^4 + x^3 + \frac{1}{3} \in \mathbb{Q}[x]$. *Notemos que,* $f(x)$ *es irreductible sobre* $\mathbb{Q}$, *si y solo si,* $9f(x) = 2x^5 + 15x^4 + 9x^3 + 3$ *es irreducible sobre* $\mathbb{Q}$. *Eligiendo* $p = 3$ *y utilizando el criterio de Schöneman-Eisenstein, vemos que* $f(x)$ *es irreducible sobre* Q.

Ejercicios 2.5.

1. Si p es un número primo y $n \geq 1$, demuestre que el polinomio $x^n - p$ es irreducible sobre los racionales.
2. Determine cuáles de los siguientes polinomios son irreducibles sobre los números racionales.
   a) $x^4 + 2$
   b) $x^4 - 2$
   c) $x^4 - x + 1$.
3. ¿Qué polinomios satisfacen el criterio de Schöneman-Eisenstein de irreducibilidad sobre $\mathbb{Q}$?
   a) $8x^3 + 6x^2 - 9x + 24$
   b) $4x^{10} - 9x^3 + 24x - 18$
   c) $2x^{10} - 25x^3 + 10x^2 - 30$.

   Los resultados que siguen, que se dejan como ejercicios, serán utilizados en la demostración del teorema de factorización única. Para realizar las demostraciones, sugerimos revisar las propiedades de los números enteros.
4. Si $p(x)$, $q(x)$ en $F[x]$ son irreducibles sobre F y $p(x) \mid q(x)$, entonces $q(x) = ap(x)$ con $a \in F$ no nulo.
5. Sean $f(x)$, $g(x)$, $h(x)$ en $F[x]$ no nulos. Si $f(x) \mid g(x)h(x)$ y $(f(x), g(x)) = 1$, entonces $f(x) \mid h(x)$.
6. Sea $g(x) \in F[x]$ no nulo. Si $p(x) \in F[x]$ es irreducible sobre F y $p(x) \nmid g(x)$, entonces $(p(x), g(x)) = 1$.
7. Sean $f_1(x), \ldots, f_n(x)$ en $F[x]$ todos no nulos. Si $p(x) \in F[x]$ es irreducible sobre F y $p(x) \mid f_1(x)f_2(x)\cdots f_n(x)$, entonces $p(x) \mid f_i(x)$ para algún entero $i \in \{1, 2, \ldots, n\}$.

Teorema 2.10. Teorema de la Factorización única.
Sea $f(x) \in F[x]$ *y* $gr(f) \geq 1$.

a) Existen polinomios $p_1(x), ..., p_n(x)$ *en* $F[x]$ *irreducibles sobre* F *tales que* $f(x) = p_1(x) \cdots p_n(x)$.

b) Si $f(x) = p_1(x) \cdots p_n(x) = q_1(x) \cdots q_m(x)$, *donde* $p_1(x), \ldots, p_n(x)$, $q_1(x), ...,$ $q_m(x)$ *en* $F[x]$ *son irreducibles sobre* F, *entonces* $n = m$, *y después, haciendo una posible permutación de* $q_1(x), \ldots, q_m(x)$, *se tiene que* $q_i(x) = a_i p(x)$ *con* $a_i \in F$ *para todo* $i \in \{1, \ldots, n\}$.

Demostración. Probaremos (a) por inducción sobre el grado de f. Si $gr(f) = 1$, entonces claramente $f(x)$ es irreducible sobre F. Sea $gr(f) = k \geq 2$ y supongamos como hipótesis de inducción, que cualquier polinomio no constante en $F[x]$ de grado $< k$, admite una factorización en polinomios irreducibles de $F[x]$. Si $f(x)$ es irreducible sobre F, entonces no hay nada que demostrar. Si suponemos que $f(x)$ no es irreducible sobre F, existen polinomios $g(x)$, $h(x)$ en $F[x]$ tales que $f(x) = g(x)h(x)$ con $gr(g) < gr(f)$ y $gr(h) < gr(f)$. Por la hipótesis de inducción, podemos escribir $g(x)$ y $h(x)$ como un producto de polinomios irreducibles en $F[x]$ y por lo tanto, $f(x) = g(x)h(x)$ es un producto de irreducibles en $F[x]$.

Ahora demostraremos (b). Supongamos que

$$f(x) = p_1(x)p_2(x) \cdots p_n(x) = q_1(x)q_2(x) \cdots q_m(x),$$

donde $p_1(x), \ldots, p_n(x)$, $q_1(x), \ldots, q_m(x)$ en $F[x]$ son irreducibles sobre F y $n \leq m$. Claramente $p_1(x) \mid q_1(x)q_2(x) \cdots q_m(x)$ y como $p_1(x)$ es irreducible sobre F, entonces $p_1(x) \mid q_j(x)$ para algún $j \in \{1, \ldots, m\}$. Después de volver a numerar los $q_i(x)$ podemos suponer que $p_1(x) \mid q_1(x)$ y así, $q_1(x) = a_1 p_1(x)$ con $a_1 \in F$. Ahora tenemos que $p_1(x)p_2(x) \cdots p_n(x) = a_1 p_1(x)q_2(x) \cdots q_m(x)$, de donde $p_2(x) \cdots p_n(x) = a_1 q_2(x) \cdots q_m(x)$. Repitiendo nuestro argumento inductivamente, concluimos que existen $a_i \in F$ tales que $q_i(x) = a_i p_i(x)$ para todo $i \in \{1, \ldots, n\}$.

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

2.5 Ejercicios de Reforzamiento

1. Encontrar todas las raíces en $\mathbb{C}$ de cada uno de los siguientes polinomios. Escribir dichas raíces en la forma $a + bi$ con a, $b \in \mathbb{R}$. *a)* $x^2 + x + 1$ *b)* $x^3 - 2$ *c)* $x^4 + 2x^2 + 1$ *d)* $x^6 - 1$ *e)* $x^3 - i$
2. Sea $f(x) = x^9 + ax^6 + bx + 3 - \sqrt{3} \in \mathbb{R}[x]$. Encontrar los reales a y b, sabiendo que $\frac{1}{2}\sqrt{3} - \frac{1}{2}i$ es una raíz de $f(x)$.
3. Expresar cada polinomio como un producto de polinomios irreducibles sobre $\mathbb{Q}$. *a)* $x^3 + 3x^2 - 8$ *b)* $2x^3 + x^2 - 2x - 1$ *c)* $x^4 - 22x^2 + 1$ *d)* $x^3 + \frac{1}{3}x^2 + \frac{1}{3}x - \frac{2}{3}$
4. Expresar cada polinomio como un producto de polinomios irreducibles sobre $\mathbb{Z}_5$. *a)* $x^4 + 4$ *b)* $x^4 + x^3 + x^2 + x + 1$ *c)* $2x^3 + x^2 + 2x + 2$ *d)* $x^3 + 3$
5. Sea $f(x) = x^4 + 2x^3 + 4x^2 + 3x + 2 \in \mathbb{Z}_5[x]$, ¿son válidas las siguientes afirmaciones?

a) El polinomio $f(x)$ no tiene raíces en $\mathbb{Z}_5$, sin embargo, es reducible sobre $\mathbb{Z}_5$.
b) El anillo cuociente $\mathbb{Z}_5[x]/\langle f(x)\rangle$ tiene divisores del cero.

6. Determinar cuáles de los siguientes anillos cuocientes son cuerpos.
   a) $\mathbb{Q}[x]/\langle x^2-5x+6\rangle$ *b*) $\mathbb{Q}[x]/\langle x^3+x+1\rangle$ *c*) $\mathbb{Z}_5[x]/\langle x^4+4\rangle$
   d) $\mathbb{Z}_5[x]/\langle x^4+4\rangle$ *e*) $\mathbb{Z}_7[x]/\langle x^3+x^2+x+1\rangle$
7. Sea $p(x)=x^3+x+1\in\mathbb{Q}[x]$. Demostrar que el anillo $\mathbb{Q}[x]/\langle p(x)\rangle$ es un cuerpo y encontrar el inverso multiplicativo de $x^2+2x-1+\langle p(x)\rangle\in\mathbb{Q}[x]/\langle p(x)\rangle$.
8. Sea $p(x)=x^2+x+1\in\mathbb{Z}_5[x]$. Demostrar que el anillo $\mathbb{Z}_5[x]/\langle p(x)\rangle$ es un cuerpo y encontrar el inverso multiplicativo de $x+1+\langle p(x)\rangle\in\mathbb{Z}_5[x]/\langle p(x)\rangle$.
9. ¿Es el polinomio $p(x)=x^4+2x+2\in\mathbb{Q}[x]$ irreducible sobre $\mathbb{Q}$?
10. Sea $p(x)=x^3+2x+1\in\mathbb{Z}_3[x]$. Demostrar que el anillo $\mathbb{Z}_3[x]/\langle p(x)\rangle$ es un cuerpo con 27 elementos.
11. Sea $\sigma:\mathbb{R}[x]\to\mathbb{C}$ definida por $\sigma(f(x))=f(i)$ para todo $f(x)\in\mathbb{R}[x]$, donde $i^2=-1$. Demostrar que $\sigma:\mathbb{R}[x]\to\mathbb{C}$ es un homomorfismo sobreyectivo de anillos y que $Ker(\sigma)=\langle x^2+1\rangle$. Concluir que $\mathbb{R}[x]/\langle x^2+1\rangle$ y $\mathbb{C}$ son cuerpos isomorfos.
12. Sean $f(x)=x^3+2x^2+x+2$ y $g(x)=x^2+2x$ polinomios en $\mathbb{Q}[x]$, ¿es $p(x)=\frac{1}{2}(x+2)$ un generador del ideal $\langle f(x),\ g(x)\rangle$ de $\mathbb{Q}[x]$?
13. Sean $f(x)=x^2+1$ y $g(x)=x^3+1$ polinomios en $\mathbb{Z}_7[x]$. Encontrar un generador del ideal $\langle f(x),\ g(x)\rangle$ de $\mathbb{Z}_7[x]$.

Capítulo 3: Extensiones de Cuerpos

La evolución de la teoría de cuerpos abarca un período de 100 años, empezando a comienzos del siglo 19. En este período, también se desarrollan la mayoría de las teorías algebraicas, tales como: teoría de grupos, teoría de anillos y álgebra lineal. La teoría de cuerpos y las tres teorías antes mencionadas, están estrechamente ligadas. En efecto, ya en los capítulos anteriores estudiamos que:

1. A partir de un dominio de integridad era posible construir el cuerpo de fracciones del dominio de integridad. En particular, $\mathbb{Q}$ es el cuerpo de fracciones del dominio de integridad $\mathbb{Z}$ y $\mathbb{Q}(x)$ es el cuerpo de fracciones del anillo de polinomios $\mathbb{Q}[x]$.

2. Si R es un anillo conmutativo con elemento unidad $1 \neq 0$ y M es un ideal maximal de R, entonces el anillo cuociente R/M es un cuerpo. En particular, $\mathbb{Z}/p\mathbb{Z}$ es un cuerpo, cuando p es un primo y $\mathbb{Q}[x]/\langle x^2+1\rangle$ es un cuerpo.

La teoría abstracta de cuerpos ha surgido como una consecuencia de tres grandes teorías como lo son: la teoría de Galois (que estudiaremos en el capítulo 5), la teoría algebraica de los números y la geometría algebraica.

La teoría de cuerpos que desarrollaremos en este capítulo nos permitirá, en los capítulos posteriores, abordar temas tales como: decidir si un problema geométrico dado se puede resolver utilizando solamente regla y compás, estudiar parte de la teoría de Galois y la solubilidad por radicales de polinomios con coeficientes en un cuerpo.

En el ejemplo 1.1, demostramos que $\mathbb{Q}(i) = \{a+bi \ / \ a, b \in \mathbb{Q}\}$ es un cuerpo. Claramente $\mathbb{Q}(i)$ contiene a $\mathbb{Q}$. Notemos que podemos ver a $\mathbb{Q}(i)$ como espacio vectorial sobre $\mathbb{Q}$. Además, $\{1, i\}$ es una base de $\mathbb{Q}(i)$ sobre $\mathbb{Q}$. En efecto, si $a \cdot 1 + b \cdot i = 0$ con $a, b \in \mathbb{Q}$, entonces $a = b = 0$. Es decir, los vectores 1, i son linealmente independientes sobre $\mathbb{Q}$. Como, $\{ \ a \cdot 1 + b \cdot i \ / \ a, b \in \mathbb{Q}\} = \mathbb{Q}(i)$, entonces los vectores 1, i son generadores de $\mathbb{Q}(i)$ como espacio vectorial sobre $\mathbb{Q}$. Concluimos que, $\mathbb{Q}(i)$ es un espacio vectorial de dimensión 2 sobre $\mathbb{Q}$.

Lo que se da en el ejemplo anterior no es mera casualidad, dado que si F es un subcuerpo de un cuerpo K (es decir, $F \leq K$), 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.

En este capítulo desarrollaremos la teoría necesaria que nos permitirá, por ejemplo:

1. Demostrar que el conjunto $\mathbb{Q}(\sqrt[3]{2}) = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} \ / \ a, b, c \in \mathbb{Q}\}$ es un cuerpo que contiene a $\mathbb{Q}$ y que $\mathbb{Q}(\sqrt[3]{2})$ es un espacio vectorial de dimensión 3 sobre $\mathbb{Q}$.

2. Demostrar que, dada una raíz $\alpha \in \mathbb{C}$ de un polinomio $p(x) \in \mathbb{Q}[x]$ irreducible sobre $\mathbb{Q}$ y de grado n, entonces el conjunto

$$\{a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} \ / \ a_0, \ldots, a_{n-1} \in \mathbb{Q}\}$$

es un cuerpo que contiene a $\mathbb{Q}$ y es un espacio vectorial de dimensión n sobre $\mathbb{Q}$.

3. Construir cuerpos F, E tales que $\mathbb{Q} \leq F \leq E \leq \mathbb{R}$ tales que F es un espacio vectorial de dimensión finita sobre $\mathbb{Q}$ y E es un espacio vectorial de dimensión finita sobre F.

4. Construir infinitos cuerpos intermedios entre $\mathbb{Q}$ y $\mathbb{R}$.

5. Demostrar que no existe un cuerpo K tal que $\mathbb{Q} \subset K \subset \mathbb{Q}(\sqrt[3]{2})$ con $\mathbb{Q} \neq K$ y $K \neq \mathbb{Q}(\sqrt[3]{2})$.

6. Demostrar que $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \ / \ a, b, c, d \in \mathbb{Q}\}$ es un cuerpo que contiene a $\mathbb{Q}$ y $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ es un espacio vectorial de dimensión 4 sobre $\mathbb{Q}$.

7. Demostrar que, si p es un número primo y n un entero positivo, entonces existe un cuerpo finito con p^n elementos.

3.1 Extensiones Finitas y Algebraicas

Definición 3.1. *Diremos que K es una* ***extensión de un cuerpo*** *F, si K es un cuerpo y F es un subcuerpo de K.*

Definición 3.2. *Sea K una extensión de un cuerpo F. Diremos que la dimensión de K, como espacio vectorial sobre F, es el* ***grado de*** *K* ***sobre*** *F, que denotaremos por $[K : F]$. Además, cuando $[K : F]$ sea finito diremos que K es una* ***extensión finita*** *de F.*

Ejemplo 3.1. *$\mathbb{Q}(i)$ es una extensión finita de $\mathbb{Q}$ y $[\mathbb{Q}(i) : \mathbb{Q}] = 2$.*

Ejercicios 3.1.

1. Demostrar que $\mathbb{C} = \{a+bi \ / \ a, b \in \mathbb{R}\}$ es una extensión finita de $\mathbb{R}$ y que $[\mathbb{C} : \mathbb{R}] = 2$.
2. Demostrar que $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \ / \ a, b \in \mathbb{Q}\}$ es una extensión finita de $\mathbb{Q}$ y que $[\mathbb{Q}(\sqrt{2} : \mathbb{Q}] = 2$.
3. Demostrar que $\mathbb{R}$ no es una extensión finita de $\mathbb{Q}$. Sugerencia: suponer lo contrario y establecer una contradicción con cardinalidades.

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

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

Teorema 3.1. *Sean E una extensión de un cuerpo K y K una extensión de un cuerpo F.*

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

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

Demostración.

a) Sean $\{\alpha_1, ..., \alpha_n\}$ una base de K sobre F y $\{\beta_1, \ldots, \beta_m\}$ una base de E sobre K. Demostraremos que $\{\alpha_i\beta_j \ / \ i \in \{1, \ldots, n\} \text{ y } j \in \{1, ..., m\}\}$ es una base para E como espacio vectorial sobre F.

i) Demostraremos que los mn vectores: $\alpha_1\beta_1$, $\alpha_1\beta_2, \ldots, \alpha_1\beta_m$, $\alpha_2\beta_1$, $\alpha_2\beta_2, \ldots,$ $\alpha_2\beta_m$, $\ldots\ldots, \alpha_n\beta_1$, $\alpha_n\beta_2, \ldots, \alpha_n\beta_m$ son linealmente independientes sobre F.

Sea $\sum k_{ij}\alpha_i\beta_j = 0$, donde $k_{ij} \in F$. Entonces $(k_{11}\alpha_1\beta_1 + k_{12}\alpha_1\beta_2 + \cdots + k_{1m}\alpha_1\beta_m) + (k_{21}\alpha_2\beta_1 + k_{22}\alpha_2\beta_2 + \cdots + k_{2m}\alpha_2\beta_m) + \cdots + (k_{n1}\alpha_n\beta_1 + k_{n2}\alpha_n\beta_2 + \cdots + k_{nm}\alpha_n\beta_m) = 0$, lo cual implica que $(k_{11}\alpha_1 + k_{21}\alpha_2 + \cdots + k_{n1}\alpha_n)\beta_1 + (k_{12}\alpha_1 + k_{22}\alpha_2 + \cdots + k_{n2}\alpha_n)\beta_2 + \cdots + (k_{1m}\alpha_1 + k_{2m}\alpha_2 + \cdots + k_{nm}\alpha_n)\beta_m = (\sum_{i=1}^{n} k_{i1}\alpha_i)\beta_1 + (\sum_{i=1}^{n} k_{i2}\alpha_i)\beta_2 + \cdots + (\sum_{i=1}^{n} k_{im}\alpha_i)\beta_m = 0$.

Sabemos que los vectores $\beta_1, \beta_2, \ldots, \beta_m$ son linealmente independientes sobre K. Luego, para $j \in \{1, \ldots, m\}$ el coeficiente de β_j es cero, es decir, $\sum_{i=1}^{n} k_{ij}\alpha_i = 0$. Pero $\alpha_1, \alpha_2, \ldots, \alpha_n$ son linealmente independientes sobre F, luego $k_{1j} = k_{2j} = \cdots = k_{nj} = 0$. Concluimos que $k_{ij} = 0$ para todo $i \in \{1, \ldots, n\}$ y $j \in \{1, \ldots, m\}$.

ii) Demostraremos que los mn vectores $\alpha_i\beta_j$ con $i \in \{1, \ldots, n\}$ y $j \in \{1, \ldots, m\}$ son generadores del espacio vectorial E sobre F. Tomemos un elemento $\beta \in E$. Debemos probar que β se puede escribir como una combinación lineal de los mn vectores $\alpha_i\beta_j$ con coeficientes en F. Ahora, como $\{\beta_1, \ldots, \beta_m\}$ es una base de E sobre K, existen elementos $k_1, ..., k_m$ en K tales que $\beta = k_1\beta_1 + k_2\beta_2 + \cdots + k_m\beta_m$.

Pero cada k_j es un elemento en K y $\{\alpha_1, \ldots, \alpha_n\}$ una base de K sobre F. Por lo tanto, para cada k_j existen elementos $t_{1j}, t_{2j}, \ldots, t_{nj}$ en F tales que $k_j = t_{1j}\alpha_1 + t_{2j}\alpha_2 + \cdots + t_{nj}\alpha_n$.

Finalmente, $\beta = k_1\beta_1 + k_2\beta_2 + \cdots + k_m\beta_m = (t_{11}\alpha_1 + t_{21}\alpha_2 + \cdots + t_{n1}\alpha_n)\beta_1 + (t_{12}\alpha_1 + t_{22}\alpha_2 + \cdots + t_{n2}\alpha_n)\beta_2 + \cdots + (t_{1m}\alpha_1 + t_{2m}\alpha_2 + \cdots + t_{nm}\alpha_n)\beta_m = \sum t_{ij}\alpha_i\beta_j$, lo que demuestra lo deseado.

b) Por hipótesis, $[E : F]$ es finito y K es un subespacio vectorial de E. Luego, $[K : F]$ es finito. Sólo nos falta demostrar que $[E : K]$ es finito.

Supongamos que $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ es una base de E como espacio vectorial sobre F. Para cualquier elemento $\alpha \in E$, existen $b_1, b_2, ..., b_n \in F$ tales que $\alpha = b_1\alpha_1 + b_2\alpha_2 + \cdots + b_n\alpha_n$. Pero F es un subconjunto de K, luego $\alpha = b_1\alpha_1 + b_2\alpha_2 + \cdots + b_n\alpha_n$ con $b_1, b_2, \ldots, b_n \in K$.

Por lo tanto, los vectores $\alpha_1,\ \alpha_2, \ldots, \alpha_n$ son generadores de E como espacio vectorial sobre K. Así, $[E : K] \leq n$, es decir, $[E : K]$ es finito. $\square$

Con la teoría que desarrollaremos en esta sección, será posible demostrar que los conjuntos $F = \{a + b\sqrt{5} \ / \ a,\ b \in \mathbb{Q}\}$ y $K = \{a + b\sqrt{7} \ / \ a,\ b \in F\}$ son cuerpos tales que $\mathbb{Q} \leq F \leq K$. Además, $\{1,\ \sqrt{5}\}$ resulta ser una base de F como espacio vectorial sobre $\mathbb{Q}$ y $\{1,\ \sqrt{7}\}$ es una base de K como espacio vectorial sobre F. De acuerdo a la demostración de la parte (a) del Teorema 3.1, $\{1,\ \sqrt{5},\ \sqrt{7},\ \sqrt{35}\}$ es una base del K como espacio vectorial sobre $\mathbb{Q}$ y así,

$$K = \{a + b\sqrt{5} + c\sqrt{7} + d\sqrt{35} \ / \ a,\ b,\ c,\ d \in \mathbb{Q}\}.$$

El siguiente resultado es una generalización del Teorema 3.1 (a).

Corolario 3.1. *Si $F_1,\ F_2, \ldots,\ F_r$ son cuerpos tales que cada cuerpo F_{i+1} es una extensión finita de F_i, entonces F_r es una extensión finita de F_1 y además,*

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

Consideremos el real $\alpha = \sqrt{5} + \sqrt{7}$. Nos interesa encontrar un polinomio no nulo $f(x) \in \mathbb{Q}[x]$ (si es que existe) tal que $f(\alpha) = 0$. Como $\alpha^2 = (\sqrt{5} + \sqrt{7})^2 = 2\sqrt{35} + 12$, entonces $(\alpha^2 - 12)^2 = (2\sqrt{35})^2$, de donde $\alpha^4 - 24\alpha^2 + 4 = 0$. Por lo tanto, $\sqrt{5} + \sqrt{7}$ es una raíz del polinomio $f(x) = x^4 - 24x^2 + 4 \in \mathbb{Q}[x]$. Es decir, $\sqrt{5} + \sqrt{7}$ es un **número algebraico**[1].

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

Definición 3.3. *Sea K una extensión de un cuerpo 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.*

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

Ejemplo 3.2. $\sqrt{2} \in \mathbb{R}$ *es algebraico sobre* $\mathbb{Q}$, *dado que* $\sqrt{2}$ *es una raíz del polinomio* $f(x) = x^2 - 2 \in \mathbb{Q}[x]$.

Ejemplo 3.3. $\sqrt[4]{2} \in \mathbb{R}$ *es algebraico sobre el cuerpo* $F = \{a + b\sqrt{2} \ / \ a,\ b \in \mathbb{Q}\}$, *dado que* $\sqrt[4]{2}$ *es una raíz de* $f(x) = x^2 - \sqrt{2} \in F[x]$.

Ejemplo 3.4. $i \in \mathbb{C}$ *es algebraico sobre* $\mathbb{Q}$, *dado que* i *es una raíz del polinomio* $f(x) = x^2 + 1 \in \mathbb{Q}[x]$.

Ejemplo 3.5. *Si F es un cuerpo, entonces $\alpha \in F$ es algebraico sobre F. En efecto,* $f(x) = x - \alpha \in F[x]$ *y* $f(\alpha) = 0$.

[1]Un número complejo que es raíz de un polinomio no nulo con coeficientes racionales se llama un número algebraico.

Ejemplo 3.6. *Demostraremos que* $\mathbb{Q}(i) = \{a + bi \ / \ a, b \in \mathbb{Q}\}$ *es una extensión algebraica de* $\mathbb{Q}$. *Es claro que* $\mathbb{Q}(i)$ *es una extensión de* $\mathbb{Q}$. *Debemos demostrar que todo elemento de* $\mathbb{Q}(i)$ *es algebraico sobre* $\mathbb{Q}$. *Sea* $\beta = a + bi$ *con* a, $b \in \mathbb{Q}$. *Como* $\beta - a = bi$, *entonces* $(\beta - a)^2 = (bi)^2$, *de donde obtenemos que* $\beta^2 - 2a\beta + a^2 + b^2 = 0$. *Por lo tanto,* $\beta = a + bi$ *es una raíz del polinomio* $f(x) = x^2 - 2ax + a^2 + b^2 \in \mathbb{Q}[x]$, *lo que demuestra que* $\mathbb{Q}(i)$ *es una extensión algebraica de* $\mathbb{Q}$.

Observación 3.1. *Ya sabemos 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 transcendente 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 de geometría que sólo permiten utilizar regla y compás. Dichos problemas serán abordados en el capítulo 4 de esta monografía.*

Ejercicios 3.2.

1. ¿Es $\sqrt{2} + \sqrt{7} \in \mathbb{R}$ algebraico sobre $\mathbb{Q}$?
2. Demostrar que $\sqrt{2} + \sqrt{3} + \sqrt{5} \in \mathbb{R}$ es algebraico sobre $\mathbb{Q}$.
3. Demostrar que el elemento $a + b\sqrt{2}i \in \mathbb{C}$ con $a, b \in \mathbb{Q}$ es algebraico sobre $\mathbb{Q}$.
4. Demostrar que $\mathbb{C} = \{a + bi \ / \ a, b \in \mathbb{R}\}$ es una extensión algebraica de $\mathbb{R}$.
5. Considerar la extensión $F_4 = \{0, 1, a, b\}$ del cuerpo $F = \{0, 1\}$, dada en el Ejemplo 1.7, ¿es F_4 una extensión algebraica de F?
6. Sea K un cuerpo infinito. Demostrar que no existe un polinomio no nulo $f(x) \in K[x]$ tal que $f(\alpha) = 0$ para todo $\alpha \in K$.

Teorema 3.2. *Si* K *es una extensión finita de un cuerpo* F, *entonces* K *es una extensión algebraica de* F.

Demostración. Sea $[K : F] = n$ y α un elemento cualquiera en K. Se demostrará 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 los $n+1$ vectores α, $\alpha^2, \ldots, \alpha^n, \alpha^{n+1}$ 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 de $f(x) = a_1x + a_2x^2 + \cdots + a_nx^n + a_{n+1}x^{n+1} \in F[x]$ y por lo tanto, α es algebraico sobre F. □

Observación 3.2. *El recíproco del teorema anterior no es necesariamente válido. El conjunto* $\overline{\mathbb{Q}} = \{\alpha \in \mathbb{C} \ / \ \alpha$ *es algebraico sobre* $\mathbb{Q}\}$ *es un cuerpo, como se concluye del Teorema 3.9, dicho cuerpo es una extensión algebraica de* $\mathbb{Q}$, *sin embargo,* $\overline{\mathbb{Q}}$ *es*

un espacio vectorial de dimensión infinita sobre $\mathbb{Q}$*, resultado que se demuestra en la Observación 3.5.*

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

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

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

Demostración.

a) Es fácil demostrar que el conjunto $J = \{f(x) \in F[x] \ / \ f(\alpha) = 0\}$ es un ideal del anillo $F[x]$. Como $\alpha \in K$ es algebraico sobre F, entonces existe un polinomio no nulo $f(x) \in F[x]$ tal que $f(\alpha) = 0$. Así, $f(x) \in J$ y $J \neq \{0\}$.

Por el Teorema 2.5, sabemos que $F[x]$ es un dominio de ideales principales y por lo tanto, existe un polinomio $q(x) \in F[x]$ que genera el ideal J. Es decir, $J = \langle q(x) \rangle = \{q(x)r(x) \ / \ r(x) \in F[x]\}$. Notemos que $q(x)$ no puede ser un polinomio constante, dado que $q(\alpha) = 0$. Así, necesariamente $gr(q) \geq 1$.

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

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

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, $h(x) = b_0 \in F$ con $b_0 \neq 0$ y $r(x) = b_0^{-1}$. Por lo tanto, $q(x) = g(x)b_0$, de donde

$$gr(q(x)) = gr(g(x)b_0) = gr(g(x)) + gr(b_0) = gr(g(x)) + 0 = gr(g(x)),$$

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

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

b) Sea $t(x) \in F[x]$ un polinomio irreducible mónico tal que $t(\alpha) = 0$. Entonces $t(x) \in J = \langle p(x) \rangle$ y así, $t(x) = p(x)r(x)$ con $r(x) \in F[x]$. Si $gr(r) \geq 1$, entonces, dado que $gr(p) = n \geq 1$, se obtiene que $t(x)$ es reducible, una contradicción. Por lo tanto, $gr(r) = 0$ y así, $r(x) = c \in F$. Como $t(x) = cp(x)$, entonces $gr(t) = gr(p) = n$. Los coeficientes de x^n de los polinomios $t(x)$ y $cp(x)$ son 1 y c, respectivamente, pero estos polinomios son iguales, en consecuencia $c = 1$, de donde $t(x) = p(x)$. De este modo, concluimos que $p(x) \in F[x]$ es único. □

Definición 3.4. *Sea* K *una extensión de un cuerpo* 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* $gr(p)$ *es el* ***grado de*** α ***sobre*** F*.*

Ejemplo 3.7. *Encontraremos el polinomio irreducible de* $\sqrt{2}+\sqrt{5}$ *sobre* $\mathbb{Q}$. *Sea* $\alpha = \sqrt{2}+\sqrt{5}$. *Entonces* $\alpha^2 = (\sqrt{2}+\sqrt{5})^2 = 7+2\sqrt{10}$ *y así,* $\alpha^2 - 7 = 2\sqrt{10}$. *Ahora,* $(\alpha^2-7)^2 = (2\sqrt{10})^2$ *implica que* $\alpha^4 - 14\alpha^2 + 9 = 0$. *Por lo tanto,* $\sqrt{2}+\sqrt{5}$ *es un raíz del polinomio* $p(x) = x^4 - 14x^2 + 9 \in \mathbb{Q}[x]$ *y de esta forma,* $\sqrt{2}+\sqrt{5}$ *es algebraico sobre* $\mathbb{Q}$.

Demostraremos a continuación que $p(x) = x^4 - 14x^2 + 9$ *es irreducible sobre* $\mathbb{Q}$. *Notemos que* $p(x)$ *no tiene raíces en* $\mathbb{Q}$. *En efecto,* $p(1) = p(-1) = -4$, $p(3) = p(-3) = -36$ *y* $p(9) = p(-9) = 5436$. *Luego,* $p(x)$ *no se puede factorizar como el producto de un polinomio de grado* 1 *y un polinomio de grado* 3 *sobre* $\mathbb{Q}$.

Si suponemos que $p(x)$ *se puede factorizar como el producto de dos polinomios de grado* 2 *sobre* $\mathbb{Q}$, *por el Teorema 2.8, existen polinomios mónicos con coeficientes enteros* $u(x) = x^2 + ax + b$ *y* $v(x) = x^2 + cx + d$ *tales que* $p(x) = u(x)v(x)$. *Luego,*

$$\begin{aligned} x^4 - 14x^2 + 9 &= (x^2+ax+b)(x^2+cx+d) \\ &= x^4 + (a+c)x^3 + (b+d+ac)x^2 + (ad+bc)x + bd, \end{aligned}$$

de donde $a+c=0$, $b+d+ac=-14$, $ad+bc=0$ *y* $bd=9$. *Por lo tanto,* $0 = ad+bc = ad+b(-a) = a(d-b)$.

Si $a=0$, *entonces* $b+d+14=0$ *y* $bd=9$. *Ahora,* $0 = b(b+d+14) = b^2+bd+14b = b^2+14b+9 = (b+7)^2 - 40$, *de donde* $(b+7)^2 = 40$ *con* $b \in \mathbb{Z}$, *lo que es una contradicción.*

Si $d=b$, *entonces* $b^2 = 9$. *Así,* $b=3$ *ó* $b=-3$. *Si* $b=d=3$, *entonces* $ac=-20$ *y* $a+c=0$. *Luego,* $0 = a(a+c) = a^2+ac = a^2-20$, *de donde* $a^2 = 20$ *con* $a \in \mathbb{Z}$, *una contradicción. Si* $b=d=-3$ *se obtiene que* $a^2 = 8$ *con* $a \in \mathbb{Z}$, *una contradicción.*

De esta forma hemos demostrado que el polinomio irreducible de $\sqrt{2}+\sqrt{5}$ *sobre* $\mathbb{Q}$ *es* $p(x) = x^4 - 14x^2 + 9$.

Ejemplo 3.8. *Sea* $\beta = a+bi$ *con* $a, b \in \mathbb{R}$ *y* $b \neq 0$. *Encontraremos el polinomio irreducible de* β *sobre* $\mathbb{R}$. *Como* $\beta = a+bi$, *entonces* $(\beta-a)^2 = (bi)^2$ *y así,* $\beta^2 - 2a\beta + a^2 + b^2 = 0$. *Por lo tanto,* β *es una raíz del polinomio* $p(x) = x^2 - 2ax + a^2 + b^2 \in \mathbb{R}[x]$. *Notemos que* $p(x) = (x-a)^2 + b^2$. *Como* $b \neq 0$, *entonces* $b^2 > 0$. *Así, para todo* $x \in \mathbb{R}$, $p(x) > 0$. *De esta forma,* $p(x)$ *no tiene raíces en* $\mathbb{R}$. *Dado que* $gr(p) = 2$, *entonces* $p(x) = x^2 - 2ax + a^2 + b^2$ *es irreducible sobre* $\mathbb{R}$.

Sea K una extensión de un cuerpo 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,

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

En forma similar a como se demuestra que el conjunto $F[x]$ es un dominio de integridad, es posible probar que $F[\alpha]$ es un dominio de integridad. Denotaremos por $F(\alpha)$ al cuerpo de fracciones de $F[\alpha]$. Luego,

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

De acuerdo a la Observación 1.2, $F(\alpha)$ es el cuerpo más pequeño que contiene a F y α.

Teorema 3.3. *Sea K una extensión de un cuerpo F y $\alpha \in K$. Entonces*

a) $\phi_\alpha : F[x] \to K$ 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 de integridad isomorfos.

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

Demostración. La demostración de (a) la dejamos como ejercicio para el lector.
b) Si $\alpha \in K$ es trascendente sobre F, entonces (Definición 3.3) no existe un polinomio no nulo $f(x) \in F[x]$ tal que $f(\alpha) = 0$. Luego, $Ker(\phi_\alpha) = \{0\}$ y así, $\phi_\alpha : F[x] \to K$ es una función inyectiva. Como el recorrido de la función ϕ_α es $F[\alpha] = \{f(\alpha) \ / \ f(x) \in F[x]\}$, entonces obtenemos que $F[x]$ y $F[\alpha]$ son dominios de integridad isomorfos, lo que demuestra (b).
c) Si $\alpha \in K$ es algebraico sobre F y $p(x)$ es el polinomio irreducible de α sobre F, entonces $p(x)$ es un generador del ideal $J = \{f(x) \in F[x] \ / \ f(\alpha) = 0\}$ del anillo $F[x]$ (Lema 3.1 (a)). Dado que $J = Ker(\phi_\alpha)$, entonces por el primer teorema de isomorfismo de anillos, los anillos $F[x]/\langle p(x)\rangle$ e $Im(\phi_\alpha) = F[\alpha]$ son isomorfos. Pero, $F[x]/\langle p(x)\rangle$ es cuerpo, dado que $p(x)$ es irreducible sobre F. Por lo tanto, $F[\alpha]$ es un cuerpo. Como $F[\alpha]$ es un cuerpo que contiene a F y α, entonces necesariamente $F(\alpha) = F[\alpha]$. □

Ejemplo 3.9. *Los cuerpos $\mathbb{Q}(x)$ y $\mathbb{Q}(\pi)$ son isomorfos. En efecto, como $\pi \in \mathbb{R}$ es un elemento trascendente sobre $\mathbb{Q}$, entonces del Teorema 3.3 (b), $\mathbb{Q}[x]$ y $\mathbb{Q}[\pi]$ son dominios de integridad isomorfos. Luego, sus respectivos cuerpos de fracciones $\mathbb{Q}(x)$ y $\mathbb{Q}(\pi)$ son isomorfos.*

Ejemplo 3.10. *Los cuerpos $\mathbb{R}[x]/\langle x^2+1\rangle$ y $\mathbb{C}$ son isomorfos. En efecto, del Teorema 3.3, sabemos que la función $\phi_i : \mathbb{R}[x] \to \mathbb{C}$ definida por $\phi_i(f(x)) = f(i)$ para todo $f(x) \in \mathbb{R}[x]$, es un homomorfismo de anillos. El núcleo de esta función es el ideal maximal $\langle x^2+1\rangle$ de $\mathbb{R}[x]$ y su recorrido es $\mathbb{R}[i] = \mathbb{R}(i)$. Pero $\mathbb{R}(i) = \mathbb{C}$, por el primer teorema de isomorfismo de anillos, se obtiene que $\mathbb{R}[x]/\langle x^2+1\rangle$ y $\mathbb{C}$ son cuerpos isomorfos.*

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

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

Teorema 3.4. *Sea K una extensión de un cuerpo F, $\alpha \in K$ algebraico sobre F y $p(x) \in F[x]$ el polinomio irreducible de α sobre F con $gr(p) = n$. 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

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

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 $F(\alpha) = U$, del Teorema 3.3 (c), basta probar que $U = F[\alpha]$. Es claro que $U \subset F[\alpha]$. Consideremos ahora, $f(\alpha)$ un elemento cualquiera en $F[\alpha]$, donde $f(x) \in F[x]$. Por el algoritmo de Euclides existen polinomios $q(x)$, $r(x)$ en $F[x]$ tales que $f(x) = p(x)q(x) + r(x)$, donde $r(x) = 0$ ó $gr(r) < gr(p) = n$. Luego,

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

Por lo tanto,

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

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 (a). 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 $gr(g) \leq n - 1$ y además, $gr(g) = gr(p) + gr(q) = n + gr(q)$, lo cual implica $gr(g) \geq n$, una contradicción. Por lo tanto, $g(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1} = 0$, 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 cuerpo 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 cuerpo $F(\alpha)(\beta)$ por $F(\alpha, \beta)$.

Teorema 3.5. *Sea K una extensión de un cuerpo 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 cuerpo F, entonces existe un polinomio no nulo $q(x) \in F[x]$ tal que $q(\beta) = 0$. Pero $q(x) \in (F(\alpha))[x]$, luego β es algebraico sobre $F(\alpha)$ y en consecuencia, $(F(\alpha))(\beta) = F(\alpha, \beta)$ es una extensión finita de $F(\alpha)$. De esta forma tenemos

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

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

Observación 3.3. *Si en el teorema anterior tenemos* $[F(\alpha) : F] = n$ *y* $[F(\alpha)(\beta) : F(\alpha)] = m$*, entonces por el Teorema 3.1,* $\{1, \ldots, \alpha^{n-1}\}$ *es una base de* $F[\alpha]$ *sobre* F *y* $\{1, \ldots, \beta^{m-1}\}$ *es una base de* $F(\alpha)(\beta)$ *sobre* $F(\alpha)$*. Así,* $\{\beta^i\alpha^j \ / \ i \in \{0, \ldots, n-1\}, j \in \{0, \ldots, m-1\}\}$ *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 cuerpo* F *y* $\alpha_1, \alpha_2, \ldots, \alpha_n \in K$ *son algebraicos sobre* F*, entonces denotaremos* $F(\alpha_1,\alpha_2) = (F(\alpha_1))(\alpha_2)$*,* $F(\alpha_1,\alpha_2,\alpha_3) = (F(\alpha_1,\alpha_2))(\alpha_3)$ *y, en general,* $F(\alpha_1,\alpha_2,\ldots,\alpha_n) = (F(\alpha_1,\alpha_2,\ldots,a_{n-1}))(\alpha_n)$*.*

Además, si $\sigma : \{1,2,\ldots,n\} \to \{1,2,\ldots,n\}$ *es una biyección, entonces*

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

Utilizando la observación anterior y el Teorema 3.5, se demuestra inductivamente el siguiente resultado:

Corolario 3.2. *Sea* K *una extensión de un cuerpo* 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,*

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

Teorema 3.6. *Si* E *es una extensión finita de un cuerpo* F*, entonces existen elementos* $\alpha_1, \ldots, \alpha_n \in E$ *tales que* $E = F(\alpha_1, \ldots, \alpha_n)$*.*

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, α_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, α_1, α_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 cuerpo* E *y* E *es una extensión algebraica de un cuerpo* F*, entonces* K *es una extensión algebraica de* F*.*

Demostración. Sea α un elemento cualquiera en K. Nuestro objetivo es demostrar 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 $b_0, b_1, \ldots, b_n$ en 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, $[F(b_1, b_2, \ldots, b_n)(\alpha) : F(b_1, b_2, \ldots, b_n)]$, $[F(b_1, b_2, \ldots, b_n) : F]$ finitos, implican que $[F(b_1, b_2, \ldots, b_n)(\alpha) : F]$ es finito, lo que demuestra que α es algebraico sobre F (Teorema 3.2). □

Ejemplo 3.11. *Del ejemplo 3.7, sabemos que* $p(x) = x^4 - 14x^2 + 9$ *es el polinomio irreducible de* $\sqrt{2} + \sqrt{5}$ *sobre* $\mathbb{Q}$. *Luego,* $[\mathbb{Q}(\sqrt{2} + \sqrt{5}) : \mathbb{Q}] = 4$ *y* $\{1, \sqrt{2} + \sqrt{5}, (\sqrt{2} + \sqrt{5})^2, (\sqrt{2} + \sqrt{5})^3\}$ *es una base de* $\mathbb{Q}(\sqrt{2} + \sqrt{5})$ *como espacio vectorial sobre* $\mathbb{Q}$. *Por lo tanto, los elementos del cuerpo* $\mathbb{Q}(\sqrt{2} + \sqrt{5})$ *son de la forma* $a + b(\sqrt{2} + \sqrt{5}) + c(\sqrt{2} + \sqrt{5})^2 + d(\sqrt{2} + \sqrt{5})^3$ *con* $a, b, c, d \in \mathbb{Q}$.

Ejemplo 3.12. *Demostraremos que* $[\mathbb{Q}(\sqrt{2}, \sqrt{5}) : \mathbb{Q}] = 4$. *Sabemos que* $\mathbb{Q}(\sqrt{2}, \sqrt{5}) = (\mathbb{Q}(\sqrt{2}))(\sqrt{5})$. *Así tenemos*

$$\begin{array}{c} (\mathbb{Q}(\sqrt{2}))(\sqrt{5}) \\ | \\ \mathbb{Q}(\sqrt{2}) \\ | \\ \mathbb{Q} \end{array}$$

El polinomio irreducible de $\sqrt{2}$ *sobre* $\mathbb{Q}$ *es claramente* $q(x) = x^2 - 2$. *Luego,* $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \ / \ a, b \in \mathbb{Q}\}$. *Demostraremos que el polinomio irreducible de* $\sqrt{5}$ *sobre* $\mathbb{Q}(\sqrt{2})$ *es* $p(x) = x^2 - 5$. *Para demostrar que* $p(x) = x^2 - 5$ *es irreducible sobre* $\mathbb{Q}(\sqrt{2})$, *basta probar que* $p(x) = x^2 - 5$ *no tiene raíces en* $\mathbb{Q}(\sqrt{2})$. *Supongamos que* $a + b\sqrt{2}$ *con* $a, b \in \mathbb{Q}$ *es una raíz de* $p(x) = x^2 - 5$. *Entonces* $p(a + b\sqrt{2}) = (a + b\sqrt{2})^2 - 5 = a^2 + 2b^2 - 5 + 2ab\sqrt{2} = 0$. *Como* $1, \sqrt{2}$ *son linealmente independientes sobre* $\mathbb{Q}$, *entonces* $a^2 + 2b^2 - 5 = 0$ *y* $2ab = 0$. *Ahora, si* $a = 0$, *entonces* $b^2 = \frac{5}{2}$ *y si* $b = 0$, *entonces* $a^2 = 5$. *En ambos casos se obtiene una contradicción. Por lo tanto,* $p(x) = x^2 - 5$ *es el polinomio irreducible de* $\sqrt{5}$ *sobre* $\mathbb{Q}(\sqrt{2})$ *y así,* $[(\mathbb{Q}(\sqrt{2}))(\sqrt{5}) : \mathbb{Q}(\sqrt{2})] = 2$.

Dado que, $\{1, \sqrt{2}\}$ *es una base de* $\mathbb{Q}(\sqrt{2})$ *como espacio vectorial sobre* $\mathbb{Q}$ *y* $\{1, \sqrt{5}\}$ *es una base de* $(\mathbb{Q}(\sqrt{2}))(\sqrt{5})$ *como espacio vectorial sobre* $\mathbb{Q}(\sqrt{2})$, *entonces por el Teorema 3.1,* $[\mathbb{Q}(\sqrt{2}, \sqrt{5}) : \mathbb{Q}] = 4$. *Además,* $\{1, \sqrt{2}, \sqrt{5}, \sqrt{10}\}$ *es una base de* $(\mathbb{Q}(\sqrt{2}))(\sqrt{5})$ *como espacio vectorial sobre* $\mathbb{Q}$.

Ejemplo 3.13. *Demostraremos que* $[\mathbb{Q}(\sqrt{2}, \sqrt{5}) : \mathbb{Q}(\sqrt{10})] = 2$. *Puesto que* $\sqrt{2}$, $\sqrt{5}$ *son elementos del cuerpo* $\mathbb{Q}(\sqrt{2}, \sqrt{5})$, *entonces* $\sqrt{10} = \sqrt{2}\sqrt{5} \in \mathbb{Q}(\sqrt{2}, \sqrt{5})$. *Así,*

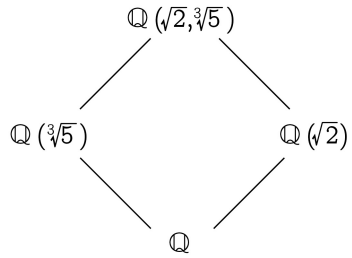
$\mathbb{Q}(\sqrt{10})$ *es un subcuerpo de* $\mathbb{Q}(\sqrt{2},\sqrt{5})$. *Ahora,*

$$\begin{array}{c} \mathbb{Q}(\sqrt{2},\sqrt{5}) \\ | \\ \mathbb{Q}(\sqrt{10}) \\ | \\ \mathbb{Q} \end{array}$$

El polinomio $p(x) = x^2 - 10$ *no tiene raíces en* $\mathbb{Q}$ *y* $gr(p) = 2$, *en consecuencia,* $p(x)$ *es el polinomio irreducible de* $\sqrt{10}$ *sobre* $\mathbb{Q}$. *Así,* $[\mathbb{Q}(\sqrt{10}) : \mathbb{Q}] = 2$. *Ahora, de* $[\mathbb{Q}(\sqrt{2},\sqrt{5}) : \mathbb{Q}(\sqrt{10})][\mathbb{Q}(\sqrt{10}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2},\sqrt{5}) : \mathbb{Q}] = 4$ *obtenemos que* $[\mathbb{Q}(\sqrt{2},\sqrt{5}) : \mathbb{Q}(\sqrt{10})] = 2$.

Ejemplo 3.14. *Demostraremos que* $\mathbb{Q}(\sqrt{2},\sqrt{5}) = \mathbb{Q}(\sqrt{2}+\sqrt{5})$. *Claramente* $\sqrt{2}+\sqrt{5} \in \mathbb{Q}(\sqrt{2},\sqrt{5})$ *y luego,* $\mathbb{Q}(\sqrt{2}+\sqrt{5})$ *es un subcuerpo de* $\mathbb{Q}(\sqrt{2},\sqrt{5})$. *Como* $[\mathbb{Q}(\sqrt{2}+\sqrt{5}) : \mathbb{Q}] = 4$ *(Ejemplo 3.11) y* $[\mathbb{Q}(\sqrt{2},\sqrt{5}) : \mathbb{Q}] = 4$ *(Ejemplo 3.12), entonces* $[\mathbb{Q}(\sqrt{2},\sqrt{5}) : \mathbb{Q}(\sqrt{2}+\sqrt{5})] = 1$. *Por lo tanto,* $\mathbb{Q}(\sqrt{2},\sqrt{5}) = \mathbb{Q}(\sqrt{2}+\sqrt{5})$.

Ejemplo 3.15. *Demostraremos que* $\mathbb{Q}(\sqrt{2},\sqrt[3]{5})$ *es una extensión finita de* $\mathbb{Q}$ *de grado* 6. *Sabemos que* $\mathbb{Q}(\sqrt{2},\sqrt[3]{5}) = \mathbb{Q}(\sqrt{2})(\sqrt[3]{5}) = \mathbb{Q}(\sqrt[3]{5})(\sqrt{2})$. *Luego,*



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

El polinomio $q(x) = x^3 - 5 \in \mathbb{Q}(\sqrt{2})[x]$ *se anula en* $\sqrt[3]{5}$. *Luego, el polinomio irreducible de* $\sqrt[3]{5}$ *sobre* $\mathbb{Q}(\sqrt{2})$ *es un divisor de* $q(x)$. *Por lo tanto,* $[\mathbb{Q}(\sqrt[3]{5})(\sqrt{2}) : \mathbb{Q}(\sqrt{2})] \leq 3$.

Utilizando nuevamente el Teorema 3.1, concluimos que $[\ \mathbb{Q}(\sqrt{2},\sqrt[3]{5}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[3]{5})(\sqrt{2}) : \mathbb{Q}(\sqrt{2})]\ [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] \leq 6$. *Por lo tanto,* $[\mathbb{Q}(\sqrt{2},\sqrt[3]{5}) : \mathbb{Q}] = 6$. *Además, obtenemos que* $q(x) = x^3 - 5$ *es el polinomio irreducible de* $\sqrt[3]{5}$ *sobre* $\mathbb{Q}(\sqrt{2})$. *Así,* $\{1,\ \sqrt[3]{5},\ \sqrt[3]{25}\}$ *es una base de* $\mathbb{Q}(\sqrt{2},\sqrt[3]{5})$ *sobre* $\mathbb{Q}(\sqrt{2})$. *Como* $\{1,\ \sqrt{2}\}$ *es una base*

de $\mathbb{Q}(\sqrt{2})$ *sobre* $\mathbb{Q}$, *obtenemos que* $\{1, \sqrt[3]{5}, \sqrt[3]{25}, \sqrt{2}, \sqrt{2}\sqrt[3]{5}, \sqrt{2}\sqrt[3]{25}\}$ *es una base de* $\mathbb{Q}(\sqrt{2}, \sqrt[3]{5})$ *sobre* $\mathbb{Q}$.

Ejemplo 3.16. *Demostraremos que* $\mathbb{Q}(\sqrt{2}+\sqrt[3]{5}) = \mathbb{Q}(\sqrt{2}, \sqrt[3]{5})$ *y encontraremos el polinomio irreducible de* $\sqrt{2}+\sqrt[3]{5}$ *sobre* $\mathbb{Q}$.

Observemos que $\sqrt{2}+\sqrt[3]{5}$ *es un elemento en el cuerpo* $\mathbb{Q}(\sqrt{2}, \sqrt[3]{5})$. *Luego,* $\mathbb{Q}(\sqrt{2}+\sqrt[3]{5})$ *es un subcuerpo de* $\mathbb{Q}(\sqrt{2}, \sqrt[3]{5})$. *Como* $\mathbb{Q}(\sqrt{2}+\sqrt[3]{5})$ *es un subespacio vectorial de* $\mathbb{Q}(\sqrt{2}, \sqrt[3]{5})$ *y* $\mathbb{Q}(\sqrt{2}, \sqrt[3]{5})$ *es un espacio vectorial de dimensión* 6 *sobre* $\mathbb{Q}$ *(Ejemplo 3.15), entonces* $\mathbb{Q}(\sqrt{2}+\sqrt[3]{5})$ *es un espacio vectorial de dimensión finita sobre* $\mathbb{Q}$. *Luego, tenemos*

$$[\mathbb{Q}(\sqrt{2}, \sqrt[3]{5}) : \mathbb{Q}(\sqrt{2}+\sqrt[3]{5})][\mathbb{Q}(\sqrt{2}+\sqrt[3]{5}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, \sqrt[3]{5}) : \mathbb{Q}] = 6.$$

Dado que $\sqrt{2}+\sqrt[3]{5} \notin \mathbb{Q}$, *entonces* $1 < [\mathbb{Q}(\sqrt{2}+\sqrt[3]{5}) : \mathbb{Q}] \leq 6$. *Así,* $[\mathbb{Q}(\sqrt{2}+\sqrt[3]{5}) : \mathbb{Q}] = 2,\ 3$ *ó* 6. *Si* $[\mathbb{Q}(\sqrt{2}+\sqrt[3]{5}) : \mathbb{Q}] = 2$, *entonces existe un polinomio irreducible mónico* $p(x) = x^2 + ax + b \in \mathbb{Q}[x]$ *tal que*

$$\begin{aligned} p(\sqrt{2}+\sqrt[3]{5}) &= (\sqrt{2}+\sqrt[3]{5})^2 + a(\sqrt{2}+\sqrt[3]{5}) + b \\ &= b + 2 + \sqrt[3]{25} + a\sqrt{2} + a\sqrt[3]{5} + 2\sqrt{2}\sqrt[3]{5} = 0. \end{aligned}$$

Por el ejemplo 3.15, sabemos que $1, \sqrt[3]{5}, \sqrt[3]{25}, \sqrt{2}, \sqrt{2}\sqrt[3]{5}, \sqrt{2}\sqrt[3]{25}$ *son linealmente independientes sobre* $\mathbb{Q}$. *Luego, obtenemos que* $1 = 0$, *una contradicción. Por lo tanto,* $[\mathbb{Q}(\sqrt{2}+\sqrt[3]{5}) : \mathbb{Q}] \neq 2$. *Si* $[\mathbb{Q}(\sqrt{2}+\sqrt[3]{5}) : \mathbb{Q}] = 3$, *entonces existe un polinomio irreducible mónico* $p(x) = x^3 + ax^2 + bx + c \in \mathbb{Q}[x]$ *tal que*

$$\begin{aligned} p(\sqrt{2}+\sqrt[3]{5}) &= (\sqrt{2}+\sqrt[3]{5})^3 + a(\sqrt{2}+\sqrt[3]{5})^2 + b(\sqrt{2}+\sqrt[3]{5}) + c \\ &= (2a + c + 5) + (b + 6)\sqrt[3]{5} + a\sqrt[3]{25} + (2 + b)\sqrt{2} + 2a\sqrt{2}\sqrt[3]{5} \\ &\quad +3\sqrt{2}\sqrt[3]{25} = 0. \end{aligned}$$

Luego, obtenemos $3 = 0$, *una contradicción. Por lo tanto,* $[\mathbb{Q}(\sqrt{2}+\sqrt[3]{5}) : \mathbb{Q}] \neq 3$ *y necesariamente* $[\mathbb{Q}(\sqrt{2}+\sqrt[3]{5}) : \mathbb{Q}] = 6$. *Luego,* $[\mathbb{Q}(\sqrt{2}, \sqrt[3]{5}) : \mathbb{Q}(\sqrt{2}+\sqrt[3]{5})] = 1$ *y en consecuencia,* $\mathbb{Q}(\sqrt{2}+\sqrt[3]{5}) = \mathbb{Q}(\sqrt{2}, \sqrt[3]{5})$.

Encontraremos el polinomio irreducible de $\sqrt{2}+\sqrt[3]{5}$ *sobre* $\mathbb{Q}$. *Si* $\alpha = \sqrt{2}+\sqrt[3]{5}$, *entonces* $\alpha - \sqrt{2} = \sqrt[3]{5}$ *y luego,* $(\alpha-\sqrt{2})^3 = (\sqrt[3]{5})^3 = 5$. *Así,* $6\alpha+\alpha^3-2\sqrt{2}-3\sqrt{2}\alpha^2 = 5$, *de donde* $2\sqrt{2} + 3\sqrt{2}\alpha^2 = 6\alpha + \alpha^3 - 5$. *Ahora, de* $(2\sqrt{2} + 3\sqrt{2}\alpha^2)^2 = (6\alpha + \alpha^3 - 5)^2$ *obtenemos que* $\alpha^6 - 6\alpha^4 - 10\alpha^3 + 12\alpha^2 - 60\alpha + 17 = 0$. *Por lo tanto,* $\sqrt{2}+\sqrt[3]{5}$ *es una raíz del polinomio* $q(x) = x^6 - 6x^4 - 10x^3 + 12x^2 + 60x + 17 \in \mathbb{Q}[x]$.

Necesariamente $q(x)$ *debe ser irreducible sobre* $\mathbb{Q}$. *En efecto, si suponemos que* $q(x)$ *no lo es, entonces* $[\mathbb{Q}(\sqrt{2}+\sqrt[3]{5}) : \mathbb{Q}] < 6$, *lo que contradice lo demostrado anteriormente.*

Ejemplo 3.17. *Sea* K *una extensión de un cuerpo* F, $\alpha \in K$ *y* $b \in F$.

a) Demostraremos que $F(b+\alpha) = F(\alpha)$.

b) Si $b \in F$ *es no nulo, demostraremos que* $F(b\alpha) = F(\alpha)$.

a) Como b, $\alpha \in F(\alpha)$ *y* $F(\alpha)$ *es un cuerpo, obtenemos que* $b+\alpha \in F(\alpha)$. *Así,* $F(b+\alpha)$ *es un subcuerpo de* $F(\alpha)$. *Dado que* $(-b)$, $b+\alpha$ *son elementos en* $F(b+\alpha)$ *y* $F(b+\alpha)$ *es cuerpo, entonces* $(-b)+b+\alpha = \alpha \in F(b+\alpha)$. *Luego,* $F(\alpha)$ *es un subcuerpo de* $F(b+\alpha)$. *Finalmente,* $F(b+\alpha) \subset F(\alpha)$ *y* $F(\alpha) \subset F(b+\alpha)$ *implican* $F(b+\alpha) = F(\alpha)$.

b) Como b, $\alpha \in F(\alpha)$ *y* $F(\alpha)$ *es un cuerpo, obtenemos que* $b\alpha \in F(\alpha)$. *Luego,* $F(b\alpha)$ *es un subcuerpo de* $F(\alpha)$. *Dado que* b, $b\alpha \in F(b\alpha)$, *entonces* $b^{-1}(b\alpha) = \alpha \in F(b\alpha)$ *y por lo tanto,* $F(\alpha)$ *es un subcuerpo de* $F(b\alpha)$. *Finalmente,* $F(b\alpha) \subset F(\alpha)$ *y* $F(\alpha) \subset F(b\alpha)$ *implican* $F(b\alpha) = F(\alpha)$.

Ejemplo 3.18. *Demostraremos que* $[\mathbb{Q}(\sqrt{2},\sqrt{10}) : \mathbb{Q}] = 4$. *Notemos que* $\mathbb{Q}(\sqrt{2},\sqrt{10}) = (\mathbb{Q}(\sqrt{2}))(\sqrt{10}) = (\mathbb{Q}(\sqrt{2}))(\sqrt{2}\sqrt{5})$. *Como* $\sqrt{2} \in \mathbb{Q}(\sqrt{2})$, *utilizando lo demostrado en el Ejemplo 3.17 (b), obtenemos que* $(\mathbb{Q}(\sqrt{2}))(\sqrt{2}\sqrt{5}) = (\mathbb{Q}(\sqrt{2}))(\sqrt{5}) = \mathbb{Q}(\sqrt{2},\sqrt{5})$. *El ejemplo 3.12 implica que* $[\mathbb{Q}(\sqrt{2},\sqrt{10}) : \mathbb{Q}] = 4$.

Ejercicios 3.3.

1. Encontrar $[\mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{5}) : \mathbb{Q}]$, $[\mathbb{Q}(\sqrt{2},\sqrt[3]{2}) : \mathbb{Q}]$, $[\mathbb{Q}(\sqrt{3},\sqrt[3]{2}) : \mathbb{Q}]$.
2. Encontrar $[\mathbb{Q}(\sqrt{2},\sqrt{6}) : \mathbb{Q}(\sqrt{3})]$, $[\mathbb{Q}(\sqrt{2}+\sqrt{3}) : \mathbb{Q}(\sqrt{3})]$, $[\mathbb{Q}(\sqrt{2},\sqrt{6}+\sqrt{10}) : \mathbb{Q}(\sqrt{3}+\sqrt{5})]$.
3. Demostrar que el polinomio $p(x) = x^2 - 3$ es irreducible sobre $\mathbb{Q}(\sqrt[3]{2})$.
4. Demostrar que $\mathbb{Q}(\sqrt{3}+\sqrt{7}) = \mathbb{Q}(\sqrt{3},\sqrt{7})$. Encontrar el polinomio irreducible de $\sqrt{3}+\sqrt{7}$ sobre $\mathbb{Q}$.
5. Sea E una extensión finita de un cuerpo F y $p(x) \in F[x]$ un polinomio irreducible sobre F, cuyo grado es primo relativo con $[E : F]$. Demostrar que $p(x)$ no tiene raíces en el cuerpo E.
6. Demostrar que el polinomio irreducible de $\sqrt[4]{3}$ sobre $\mathbb{Q}$ es $x^4 - 3$ y sobre $\mathbb{Q}(\sqrt{3})$ es $x^2 - \sqrt{3}$.
7. Sea E una extensión finita de un cuerpo F tal que $[E : F]$ es primo. Demostrar que no existen cuerpos intermedios entre F y E.
8. Sea E una extensión finita de un cuerpo F y $\alpha \in E$ algebraico sobre F. Si el polinomio irreducible de α sobre F es de grado impar, demostrar que $F(\alpha) = F(\alpha^2)$.
9. Encontrar el polinomio irreducible de $\sqrt{6}$ sobre el cuerpo $\mathbb{Q}(\sqrt{2},\sqrt{3})$.

3.2 Raíces de Polinomios Irreducibles

Podemos afirmar que, si F es un subcuerpo 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 cuerpo cualquiera F, que no necesariamente es un subcuerpo de $\mathbb{C}$, como lo demuestra el siguiente teorema.

Teorema 3.8. Teorema de Kronecker.
Sea F un cuerpo y $p(x) \in F[x]$ un polinomio irreducible sobre F con $gr(p) = n$. Entonces el cuerpo $E = F[x]/\langle p(x)\rangle$ 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. Dado que $p(x) \in F[x]$ es un polinomio irreducible sobre F, entonces el anillo cuociente $E = F[x]/\langle p(x)\rangle$ es un cuerpo. Es fácil probar que la función $\sigma : F \to F[x]/\langle p(x)\rangle$ definida por $\sigma(a) = a+\langle p(x)\rangle$ para todo $a \in F$, es un monomorfismo de anillos. 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.

Demostraremos a continuación que E es una extensión finita de grado n sobre F. Del Lema 2.4, sabemos que $E = \{a_0+a_1x+\cdots+a_{n-1}x^{n-1}+\langle p(x)\rangle / a_0, \ldots, a_{n-1} \in F\}$. Claramente 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 $gr(p) = n$, necesariamente $a_0 + a_1x + \cdots + a_{n-1}x^{n-1} = 0$, lo cual implica que $a_0 = a_1 = \cdots = a_{n-1} = 0$. Por lo tanto, E es una extensión finita de F y $[E : F] = n$.

Supongamos que $p(x) = b_0 + b_1x + \cdots + b_nx^n \in F[x]$. Entonces $\alpha = x + \langle p(x)\rangle$ es una raíz de $p(x)$. En efecto,

$$\begin{aligned} p(\alpha) &= b_0 + b_1(x + \langle p(x)\rangle) + \cdots + b_n(x + \langle p(x)\rangle)^n \\ &= b_0 + b_1(x + \langle p(x)\rangle) + \cdots + b_n(x^n + \langle p(x)\rangle) \\ &= b_0 + b_1x + \cdots + b_nx^n + \langle p(x)\rangle \\ &= p(x) + \langle p(x)\rangle = 0 + \langle p(x)\rangle = 0. \end{aligned}$$

Finalmente, como $[F(\alpha) : F] = n$, $[E : F] = n$ y $F(\alpha)$ es un subcuerpo de E, tenemos que $F(\alpha) = E$. □

Corolario 3.3. *Sea F un cuerpo y $f(x) \in F[x]$ un polinomio no constante. Entonces existe una extensión finita E de F con $[E : F] \leq gr(f)$ 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 $[E : F] = gr(p)$ y $\alpha \in E$ tal que $p(\alpha) = 0$. Claramente $\alpha \in E$ es una raíz de $f(x)$ y $[E : F] \leq gr(f)$. □

Ejemplo 3.19. *Sea* $f(x) = x^4 - 5x^2 + 6 \in \mathbb{Q}[x]$. *Construiremos una extensión* E *de* $\mathbb{Q}$, *donde* $f(x)$ *tenga una raíz. Notemos que* $f(x) = (x^2 - 3)(x^2 - 2)$ *no tiene raíces en* $\mathbb{Q}$. *El polinomio* $p(x) = x^2 - 3 \in \mathbb{Q}[x]$ *es un factor de* $f(x)$, *irreducible sobre* $\mathbb{Q}$. *Por el Corolario 2.4, el anillo cuociente* $E = \mathbb{Q}[x] \diagup \left\langle x^2 - 3 \right\rangle$ *es un cuerpo. Además,* E *es una extensión finita de* $\mathbb{Q}$, $[E : \mathbb{Q}] = gr(x^2 - 3) = 2$ *y* $\alpha = x + \left\langle x^2 - 3 \right\rangle \in E$ *es una raíz del polinomio* $x^2 - 3 \in \mathbb{Q}[x]$. *Claramente* α *también es una raíz de* $f(x)$.

La demostración del Teorema 3.8 nos entrega un método para construir extensiones de un cuerpo F. En el siguiente ejemplo construiremos una extensión finita del cuerpo $\mathbb{Z}_2 = \{\overline{0}, \overline{1}\}$ con 4 elementos. Para simplificar la notación escribiremos $\overline{a} = a$ para $\overline{a} \in \mathbb{Z}_2$.

Ejemplo 3.20. *El polinomio* $p(x) = x^2 + x + 1 \in \mathbb{Z}_2[x]$ *es irreducible sobre* $\mathbb{Z}_2$ *dado que* $gr(p) = 2$ *y* $p(x)$ *no tiene raíces en* $\mathbb{Z}_2$. *Por lo tanto,* $\langle p(x) \rangle$ *es un ideal maximal del anillo* $\mathbb{Z}_2[x]$ *y en consecuencia, el anillo* $E = \mathbb{Z}_2[x] \diagup \langle p(x) \rangle$ *es un cuerpo. 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* $a = a + \langle p(x) \rangle$. *Sabemos que*

$$E = \{a + bx + \langle p(x) \rangle / a, b \in \mathbb{Z}_2\} = \{0 + \langle p(x) \rangle, 1 + \langle p(x) \rangle, x + \langle p(x) \rangle, 1 + x + \langle p(x) \rangle\}.$$

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 cuerpo 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 3.21. *Por los mismos argumentos dados en el 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 cuociente* $E = \mathbb{Z}_2[x] \diagup \langle p(x) \rangle$ *es un cuerpo.*

$$\begin{aligned} E &= \{a + bx + cx^2 + \langle p(x) \rangle / a, b, c \in \mathbb{Z}_2\} \\ &= \{0 + \langle p(x) \rangle, 1 + \langle p(x) \rangle, x + \langle p(x) \rangle, \quad 1 + x + \langle p(x) \rangle, \\ &\qquad x^2 + \langle p(x) \rangle, 1 + x^2 + \langle p(x) \rangle, x + x^2 + \langle p(x) \rangle, 1 + x + x^2 + \langle p(x) \rangle\}. \end{aligned}$$

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,* $E = \{0, 1, \alpha, \alpha + 1, \alpha^2, \alpha^2 + 1, \alpha^2 + \alpha, \alpha^2 + \alpha + 1\}$.

Hemos construido un cuerpo finito con 8 *elementos. Dejamos como ejercicio la construcción de las tablas de adición y multiplicación.*

3.3 Clausuras Algebraicas

En esta sección demostraremos que el conjunto

$$\overline{\mathbb{Q}} = \{\alpha \in \mathbb{C} \ / \ \alpha \text{ es algebraico sobre } \mathbb{Q}\}$$

es una extensión algebraica de $\mathbb{Q}$ y algebraicamente cerrada. Este resultado nos permitirá demostrar que el recíproco del Teorema 3.2 no es necesariamente válido.

Teorema 3.9. *Sea E una extensión de un cuerpo F. Entonces el conjunto*

$$\overline{F}_E = \{\alpha \in E \ / \ \alpha \text{ es algebraico sobre } F\}$$

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

Demostración. Sean α, $\beta \in \overline{F}_E$. Como α, β son algebraicos sobre F, entonces por el Teorema 3.5, $F(\alpha, \beta)$ es una extensión finita de F y por el Teorema 3.2, $F(\alpha, \beta)$ es una extensión algebraica de F, de donde $F(\alpha, \beta) \subset \overline{F}_E$. Así, $\alpha + \beta$, $-\alpha$, $\alpha\beta$ y también α^{-1} para $\alpha \neq 0$, son todos elementos en $F(\alpha, \beta) \subset \overline{F}_E$. De esta forma, por el Lema 1.3, $\overline{F}_E$ es un subcuerpo de E. □

Observación 3.4. *Es claro que $\overline{F}_E = E$, cuando E es una extensión algebraica de un cuerpo F, situación que se tiene cada vez que E es una extensión finita de F.*

Ejemplo 3.22. *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 cuerpo algebraicamente cerrado.*

Demostración. Debemos demostrar que el cuerpo $\overline{\mathbb{Q}}_{\mathbb{C}} = \{\alpha \in \mathbb{C} \ / \ \alpha$ es algebraico sobre $\mathbb{Q}\}$ es algebraicamente cerrado. Denotemos $\overline{\mathbb{Q}} = \overline{\mathbb{Q}}_{\mathbb{C}}$ y sea $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in \overline{\mathbb{Q}}[x]$ con $gr(f) = n \geq 1$. Por el Teorema Fundamental del Álgebra, existe un elemento $\alpha \in \mathbb{C}$ tal que $f(\alpha) = 0$. Demostraremos que $\alpha \in \overline{\mathbb{Q}}$. Como a_0, $a_1, \cdots$, a_n son algebraicos sobre $\mathbb{Q}$, entonces $\mathbb{Q}(a_0, \ldots, a_n)$ es una extensión finita sobre $\mathbb{Q}$ y en consecuencia, $\mathbb{Q}(a_0, \ldots, a_n)$ 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 $\mathbb{Q}$, de donde α es algebraico sobre $\mathbb{Q}$. Hemos demostrado que $\alpha \in \overline{\mathbb{Q}}$. □

Observación 3.5. *Estamos en condiciones de probar que el recíproco del Teorema 3.2 no es válido. En efecto, $\overline{\mathbb{Q}} = \{\alpha \in \mathbb{C} \ / \ \alpha$ es algebraico sobre $\mathbb{Q}\}$ es un cuerpo. Además, $\overline{\mathbb{Q}}$ es una extensión no finita de $\mathbb{Q}$. Si suponemos que $[\overline{\mathbb{Q}} : \mathbb{Q}] = n$, entonces $\sqrt[n+1]{2}$ es un elemento en $\overline{\mathbb{Q}}$ ($\sqrt[n+1]{2}$ es un raíz del polinomio $p(x) = x^{n+1} - 2 \in \mathbb{Q}[x]$) y luego, $\mathbb{Q}(\sqrt[n+1]{2}) \subset \overline{\mathbb{Q}}$. Por el criterio de Schönemann-Eisenstein, $p(x)$ es irreducible 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.*

Ejercicios 3.4.

1. Sea E una extensión de un cuerpo F. Demuestre que todo $\alpha \in E$ que no es un elemento en $\overline{F}_E$, es transcendental sobre $\overline{F}_E$.
2. Sea E un cuerpo algebraicamente cerrado que es una extensión de un cuerpo F. Demostrar que $\overline{F}_E$ es un cuerpo algebraicamente cerrado.
3. Si E es una extensión algebraica de un cuerpo F algebraicamente cerrado, demostrar que $F = E$.

A continuación enunciamos este importante resultado de la Teoría de Cuerpos:

Teorema 3.11. *Si F es un cuerpo, entonces existe una extensión algebraica K de F que es algebraicamente cerrada. Esta extensión de F es única (salvo isomorfismo) y es llamada la* ***clausura algebraica de*** *F.*

En [5] y [6] se incluyen demostraciones de este resultado.

3.4 Derivada de un Polinomio

Daremos una definición algebraica de la derivada de un polinomio sin requerir del concepto de límite y probaremos algunos resultados que nos permitirán demostrar que, si F es un subcuerpo 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 $\mathbb{C}$. Dicho resultado será de gran utilidad en la teoría de Galois que desarrollaremos en el capítulo 5.

Definición 3.5. *Sea F un cuerpo y $f(x) = a_0 + a_1x + \cdots + a_ix^i + \cdots + a_nx^n$ un polinomio en $F[x]$. Entonces la* ***derivada*** *de $f(x)$, denotada por $f'(x)$, es el polinomio $f'(x) = a_1 + \cdots + ia_ix^{i-1} + \cdots + na_nx^{n-1}$ en $F[x]$.*

En los cursos básicos 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 se considera un polinomio con coeficientes en un cuerpo 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.

Probaremos a continuación las análogas de las reglas formales de diferenciación que tan bien conocemos.

Lema 3.2. *Sea F un cuerpo, $f(x)$, $g(x) \in F[x]$ y $\alpha \in F$.*

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

Demostración. Las demostraciones (a) y (b) se dejan como ejercicios para el lector. Para probar (c), sólo es suficiente demostrar el resultado en el caso muy especial

$f(x) = x^n$ y $g(x) = x^m$, donde m, n son enteros positivos. Entonces $h(x) = x^{n+m}$, de donde $h'(x) = (n+m)x^{n+m-1}$. Por otro lado,

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

Por lo tanto, $h'(x) = f'(x)g(x)+f(x)g'(x)$. La demostración de (d) es un fácil ejercicio de inducción matemática. □

Teorema 3.12. *Sea F un cuerpo, $\overline{F}$ 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, $f'(\alpha) = g(\alpha) \neq 0$ lo que es una contradicción. Por lo tanto, necesariamente $m > 1$. □

Ejercicios 3.5.

1. Demostrar que el polinomio $f(x) = x^4 + x \in \mathbb{C}[x]$ no tiene raíces en $\mathbb{C}$ de multiplicidad mayor que 1.
2. Sea p un número primo y $f(x) = x^p + 1 \in \mathbb{Z}_p[x]$, ¿tiene $f(x)$ raíces de multiplicidad mayor que 1 en la clausura algebraica $\overline{\mathbb{Z}_p}$ de $\mathbb{Z}_p$?
3. Demostrar que las raíces en $\mathbb{C}$ del polinomio $f(x) = x^5 - 5x + 1 \in \mathbb{C}[x]$ tienen multiplicidad 1.
4. Demostrar que las raíces en $\mathbb{C}$ del polinomio $f(x) = x^n - 1 \in \mathbb{C}[x]$ tienen multiplicidad 1.

Corolario 3.4. *Sea F un subcuerpo de los números complejos y $p(x) \in F[x]$ un polinomio mónico irreducible sobre F. Si $gr(p) = n$, 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 que $n > 1$. Sea $\alpha \in \mathbb{C}$ una raíz de $p(x)$. Entonces $p(x)$ es el polinomio irreducible de α sobre F. Si suponemos que la multiplicidad de α es $m > 1$, de acuerdo al Teorema 3.12, $p'(\alpha) = 0$. Pero $p'(x) \in F[x]$ y $gr(p') = n - 1 \geq 1$. Así, obtenemos que $p'(x) \in \langle p(x) \rangle$, de donde $gr(p') \geq gr(p)$, una contradicción. Por lo tanto, $m = 1$. □

3.5 Cuerpos Finitos

La caracterización y unicidad de los cuerpos finitos aparecen en los trabajos de Evariste Galois (1811-1832). Cuando p es un número primo, sabemos que $\mathbb{Z}_p$ es un cuerpo finito con p elementos. En esta subsección, demostraremos que, si K es un cuerpo finito, entonces K tiene p^n elementos donde p es un número primo y n es algún entero positivo. Recíprocamente probaremos que, dado un número primo p y un entero positivo n, existe un único cuerpo (salvo isomorfismo) con p^n elementos.

Teorema 3.13. *Sea F un cuerpo 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 K debe tener q^n elementos. □

Corolario 3.5. *Si K es un cuerpo 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 cuerpo finito, entonces del Teorema 1.6 (c), la característica de K es un número primo p y K contiene un subcuerpo 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 3.13, obtenemos que K tiene p^n elementos. □

Lema 3.3. *Si un cuerpo 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 cuerpo K tiene p^n elementos, entonces el polinomio $f(x) = x^{p^n} - x \in K[x]$ se factoriza en $K[x]$ como $f(x) = (x - a_1)\cdots(x - a_{p^n})$, donde $K = \{a_1, \ldots, a_{p^n}\}$.*

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 $gr(q_1) = p^n - 1$. 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 $gr(q_2) = p^n - 2$, $q_2(a_i) = 0$ 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 3.14. *Para todo número primo p y todo entero positivo n, existe un cuerpo con p^n elementos.*

Demostración. Consideremos el cuerpo 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 $K = \{\alpha \in \overline{\mathbb{Z}_p} \ / \ \alpha^{p^n} = \alpha\}$. Demostraremos a continuación que K es un cuerpo con p^n elementos. Utilizaremos el Lema 1.3 para probar que K es un subcuerpo de $\overline{\mathbb{Z}_p}$. Claramente 0 y 1 son elementos en K. Sean α, $\beta \in K$. Entonces $\alpha^{p^n} = \alpha$ y $\beta^{p^n} = \beta$. Ahora,

$$(\alpha - \beta)^{p^n} = \alpha^{p^n} + \sum_{k=1}^{p^n-1} \left(\begin{array}{c} p^n \\ k \end{array} \right) \alpha^{p^n-k}(-\beta)^k + (-1)^{p^n}\beta^{p^n}.$$

Como la característica de $\overline{\mathbb{Z}_p}$ es p y p es un divisor de $\left(\begin{array}{c} p^n \\ k \end{array} \right)$ para todo entero k con $1 \leq k < p^n$, entonces

$$\sum_{k=1}^{p^n-1} \left(\begin{array}{c} p^n \\ k \end{array} \right) \alpha^{p^n-k}(-\beta)^k = 0$$

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 $(\alpha^{-1})^{p^n} = (\alpha^{p^n})^{-1} = \alpha^{-1}$, lo cual demuestra que $\alpha^{-1} \in K$. De esta forma, hemos demostrado que K es un cuerpo. Finalmente, como $f'(x) = p^n x^{p^n-1} - 1 = -1$, según el Teorema 3.12, las raíces de $f(x)$ son todas distintas y así, K tiene p^n elementos. □

Las demostraciones de los dos teoremas que siguen no serán incluidas en esta monografía. En [5] y [6] se demuestran dichos resultados.

Teorema 3.15. *El cuerpo finito con p^n elementos, construido en el teorema anterior, es único (salvo isomorfismo).*

Teorema 3.16. *Sea K un cuerpo y G un subgrupo finito del grupo multiplicativo $K - \{0\}$. Entonces G es un grupo cíclico.*

Corolario 3.7. *Si K es un cuerpo finito, entonces $(K - \{0\}, \cdot)$ es un grupo cíclico.*

Demostración. Considerando $G = K - \{0\}$ en el teorema anterior, obtenemos el resultado. □

Ejemplo 3.23. *Construiremos un cuerpo con 3^2 elementos. Nuestro punto de partida será considerar el cuerpo $\mathbb{Z}_3 = \{0, 1, 2\}$. Del Teorema 3.13, debemos encontrar una extensión de $\mathbb{Z}_3$ de grado 2.*

Consideremos el polinomio $p(x) = x^2 + x + 2 \in \mathbb{Z}_3[x]$. *Como* $gr(p) = 2$ *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. Del Teorema 3.4,*

$$\mathbb{Z}_3(\beta) = \{a + b\beta / a, b \in \mathbb{Z}_3\} = \{0, 1, 2, \beta, \beta + 1, \beta + 2, 2\beta, 2\beta + 1, 2\beta + 2\}.$$

Ejemplo 3.24. *Encontraremos el polinomio irreducible de* $\beta + 1 \in \mathbb{Z}_3(\beta)$ *sobre* $\mathbb{Z}_3$, *donde* $\mathbb{Z}_3(\beta)$ *es el cuerpo construido en el ejemplo 3.23. 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 *y luego, 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 3.25. *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* $gr(p) = 3$, *sólo 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*

$$\begin{aligned} p(a + b\beta) &= (a + b\beta)^3 + 2(a + b\beta) + 2 = 2a + a^3 + 2 + 2b\beta + b^3\beta^3 \\ &= 2a + a^3 + 2 + 2b\beta + b^3(2\beta + 2) = 2a + a^3 + 2b^3 + 2 + 2(b + b^3)\beta, \end{aligned}$$

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* $\mathbb{Z}_3(\beta)$.

Ejercicios 3.6.

1. Por el Corolario 3.7, los elementos no nulos del cuerpo $\mathbb{Z}_3(\beta)$, construido en el Ejemplo 3.23, forman un grupo cíclico bajo la multiplicación de $\mathbb{Z}_3(\beta)$, ¿es β un generador de este grupo cíclico?, ¿qué elementos de $\mathbb{Z}_3(\beta)$ no son generadores de este grupo cíclico?
   a) ¿Cuáles de los siguientes polinomios son irreducibles sobre el cuerpo $\mathbb{Z}_3(\beta)$?
      a) $x^3 + 2x^2 + 2x + 2$ *b)* $x^3 + x^2 + x + 2$ *c)* $x^3 + 2x^2 + x + 2$
   b) Escribir cada polinomio como un producto de factores irreducibles en $\mathbb{Z}_3(\beta)[x]$.
      a) $x^3 + 2x^2 + 2$ *b)* $x^3 + x^2 + 4$ *c)* $x^3 + x^2 + x + 1$

2. Construir un cuerpo con 16 elementos. Sugerencia: considerar el cuerpo $\mathbb{Z}_2$ y demostrar que el polinomio $p(x) = x^4 + x + 1 \in \mathbb{Z}_2[x]$ es irreducible sobre $\mathbb{Z}_2$.

3.6 Ejercicios de Reforzamiento

1. Determinar si son verdaderas o falsas las siguientes afirmaciones:
   a) Toda extensión finita E de un cuerpo F es una extensión algebraica.
   b) Toda extensión algebraica E de un cuerpo F es una extensión finita.
   c) $\mathbb{R}$ es un cuerpo algebraicamente cerrado.

d) Los cuerpos $\mathbb{Q}[x]/\langle x^2+1\rangle$ y $\mathbb{Q}(i)$ son isomorfos.
e) $\mathbb{Q}(\frac{1}{2}+\sqrt{5}) = \mathbb{Q}(\frac{1}{3}+\sqrt{5})$.
f) Existe un cuerpo finito con 250 elementos.
g) La función $\sigma : \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt{3})$ definida por $\sigma(a+b\sqrt{2}) = a+b\sqrt{3}$ para todo $a, b \in \mathbb{Q}$, es un isomorfismo de anillos.

2. Sea E una extensión finita de un cuerpo F tal que $[E : F]$ es un número primo. Si $\alpha \in E$ y $\alpha \notin F$, demostrar que $E = F(\alpha)$.
3. Encontrar un polinomio no nulo $f(x) \in \mathbb{Q}[x]$ tal que $f(\alpha) = 0$, donde $\alpha = \frac{2+\sqrt{2}}{1-\sqrt{3}}$. Es decir, α es algebraico sobre $\mathbb{Q}$.
4. Sea E una extensión finita de un cuerpo F, $\alpha \in E$ y $\beta \in F(\alpha)$. Si m es el grado del polinomio irreducible de β sobre F y n es el grado del polinomio irreducible de α sobre F, demostrar que m es un divisor de n.
5. Calcular el polinomio irreducible de $\sqrt{2}+i\sqrt{2}$ sobre $\mathbb{Q}(\sqrt{2})$.
6. Demostrar que $\mathbb{Q}(\sqrt{2}, i\sqrt{2}) = \mathbb{Q}(\sqrt{2}+i\sqrt{2})$. Encontrar una base de $\mathbb{Q}(\sqrt{2}+i\sqrt{2})$ como espacio vectorial sobre $\mathbb{Q}(\sqrt{2})$.
7. Escribir el polinomio $f(x) = x^4-5x^2+6$ como un producto de factores irreducibles sobre el cuerpo $\mathbb{Q}(\sqrt{2})$.
8. ¿Es $\sqrt[3]{2}(1+\sqrt{3}i)$ algebraico sobre $\mathbb{Q}(\sqrt[3]{2})$?
9. ¿Es verdadera la siguiente afirmación?, si $\alpha \in \mathbb{C}$ es algebraico sobre $\mathbb{Q}$ y $[\mathbb{Q}(\alpha) : \mathbb{Q}] = n \geq 2$, entonces $[\mathbb{Q}(\alpha^2) : \mathbb{Q}] < n$.
10. Sean p, q números primos distintos. Demostrar que $[\mathbb{Q}(\sqrt{p}, \sqrt{q}) : \mathbb{Q}] = 4$.
11. Encontrar una base de $K = \mathbb{Q}(\sqrt{1+\sqrt{3}})$ como espacio vectorial sobre $\mathbb{Q}$. Demostrar que $\sqrt{3} \in \mathbb{Q}(\sqrt{1+\sqrt{3}})$ y que $[\mathbb{Q}(\sqrt{1+\sqrt{3}}) : \mathbb{Q}(\sqrt{3})] = 2$.
12. Demostrar que los cuerpos $\mathbb{Q}(\sqrt{2})$ y $\mathbb{Q}(i\sqrt{2})$ no son isomorfos. Sugerencia: -1 es la suma de dos cuadrados en $\mathbb{Q}(i\sqrt{2})$.
13. Demostrar que existe un cuerpo finito con 243 elementos.
14. Sea K un cuerpo finito de característica p, ¿es $\sigma : K \to K$ definida por $\sigma(x) = x^p$ para todo $x \in K$ un automorfismo de K?

Capítulo 4: Construcciones con Regla y Compás

El problema que estudiaremos en este capítulo, ya considerado en la Grecia clásica, es decidir si un problema geométrico dado se puede resolver, utilizando solamente regla y compás. Los antiguos geómetras griegos propusieron tres problemas que se volvieron notorios por su dificultad: cuadrar un círculo, duplicar un cubo y trisectar un ángulo.

La cuadratura del círculo fue un problema propuesto por Anaxágoras en el año 500 a.C. Se trata de construir un cuadrado de igual área que un círculo dado, utilizando sólo regla y compás. En el año 450 a.C., Anaxágoras fue encarcelado por afirmar que el sol no era un Dios, mientras estuvo en prisión intentó resolver el problema antes mencionado sin éxito. En 1882, el matemático alemán Ferdinand Lindemann probó que π es un número trascendente, lo que implica (como veremos) que es imposible cuadrar el círculo usando regla y compás.

La duplicación de un cubo es un problema que aparece en Atenas. Se 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, recinto sagrado dedicado principalmente al dios Apolo que tenía en el centro su gran templo. Hasta él acudían los griegos para preguntar a los dioses sobre cuestiones inquietantes y para pedirle una solución a ellas. La respuesta de los dioses fue que la crisis desaparecería si construían para los dioses un altar cúbico, con el doble de volumen que el existente. Los atenienses lo intentaron, pero lo que es seguro es que no lo consiguieron, utilizando sólo regla y compás.

La trisección de un ángulo es un problema que ya se planteaban los griegos 500 años a.C. Se trata de trisectar un ángulo cualquiera, utilizando sólo regla y compás. En el año 1837, el matemático francés Pierre Wantzel demostró que no es posible trisectar un ángulo arbitrario utilizando sólo regla y compás. Decir que los ángulos no son trisectables con regla y compás, significa que existen ángulos no trisectables. Muchos ángulos, por ejemplo, el que mide 90^o es trisectable con regla y compás.

Estos tres problemas planteados tienen en común un enunciado sencillo, el que puede ser comprendido por un individuo ajeno a las matemáticas, pero sus demostraciones requieren de matemáticas más avanzadas. Estas demostraciones serán incluidas en este capítulo.

Definiremos lo que entenderemos por un número real constructible y demostraremos que, si $\alpha \notin \mathbb{Q}$ es un real constructible, entonces $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ es una potencia de 2. También demostraremos que es posible construir un pentágono regular con regla y compás.

Si deseamos construir un polígono regular en el plano, utilizando regla y compás, la clave en la resolución del problema es la construcción de los vértices, problema que abordaremos en el capítulo: Elementos de la Teoría de Galois.

4.1 Primeras Construcciones

Definición 4.1. *Sea S un conjunto de dos o más puntos del 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.*

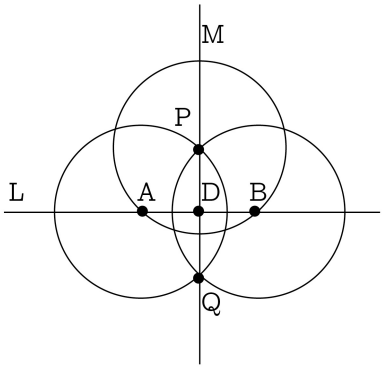
Definición 4.2. *Construir con regla y compás significa que, a partir de un conjunto S de puntos (de por lo menos dos puntos del plano), se pueden obtener otros puntos, utilizando sólo las siguientes operaciones:*

1. *Intersectando dos rectas constructibles a partir de S.*
2. *Intersectando una recta con una circunferencia, ambas constructibles a partir de S.*
3. *Intersectando dos circunferencias constructibles a partir de S.*

Los nuevos puntos obtenidos se dicen **puntos constructibles a partir de** S. Empezaremos este capítulo con una conocida construcción con regla y compás.

Ejemplo 4.1. *Sea L una recta del plano y P un punto del plano no contenido en L. Construiremos, solamente usando regla y compás, una recta que pase por P y que sea perpendicular a la recta L.*

Sea A un punto cualquiera de la recta L. Con el compás, tracemos la circunferencia de centro P y radio el segmento PA. Naturalmente, A es uno de los puntos de intersección de L con la circunferencia. Sea B el otro punto de intersección. Nuevamente con el compás, tracemos dos circunferencias de radio AP, una con cen-



tro en A y la otra con centro en B. Entonces P es uno de los puntos de intersección de ambas circunferencias. Sea Q el otro punto de intersección. Ahora, con la regla, tracemos la recta M que pasa por lo puntos P y Q. Sea D el punto de intersección de las rectas L y M.

Utilizando los teoremas de congruencias de triángulos, es fácil demostrar que los triángulos ADP y BDP son congruentes, lo cual implica que los ángulos ADP y BDP son congruentes. Como la suma de estos ángulos miden 180^0, entonces cada uno de ellos es un ángulo recto y, por lo tanto, la recta M es perpendicular a L y pasa por P.

Las siguientes construcciones serán utilizadas en las demostraciones de algunos resultados de este capítulo.

Ejercicios 4.1.

Demostrar que los siguientes problemas son resolubles con regla y compás.

1. Construir una recta que pase por un punto dado del plano y que sea paralela a una recta dada del plano.
2. Dada un recta en el plano y un punto en ella, construir una recta en el plano que sea perpendicular a la recta dada y que pase por el punto dado.
3. Construir el punto medio de un segmento dado del plano.
4. Construir un cuadrado conociendo uno de sus lados.

4.2 Números y Cuerpos Constructibles

Ejemplo 4.2. *Supongamos que nos dan dos puntos distintos A, B en el plano, nos dicen que el segmento AB tiene longitud 1 y nos piden que construyamos un segmento de longitud $\sqrt{2}$.*

En este caso, podemos trazar la recta L que pasa por los puntos A y B. Utilizando el problema 2, de los Ejercicios 4.1, podemos trazar una recta L' en el plano que sea perpendicular a L y que pase por B. Tracemos la circunferencia en el plano de centro B y radio el segmento AB. Sea Q uno de los puntos de intersección de la circunferencia y la recta L'. Naturalmente los segmentos AB y BQ tienen longitud 1 y son perpendiculares. Notemos que el segmento AQ es la hipotenusa de un triángulo rectángulo. Por el Teorema de Pitágoras, AQ tiene longitud $\sqrt{2}$.

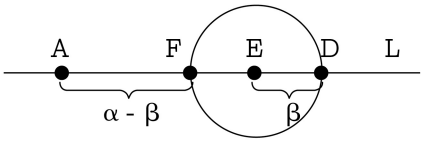
Del ejemplo anterior podemos decir que $\sqrt{2}$ es un número que se puede construir con regla y compás, esto es, $\sqrt{2}$ es constructible.

Definición 4.3. *Un número real a se dice que es un **número constructible**, si podemos construir, usando sólo regla y compás, un segmento rectilineo de longitud $|a|$ en un número finito de pasos, a partir de un segmento de longitud unitaria.*

Ejemplo 4.3. *Todo número entero es constructible.*

Teorema 4.1. *El conjunto de números constructibles forman un subcuerpo W, del cuerpo de los números reales.*

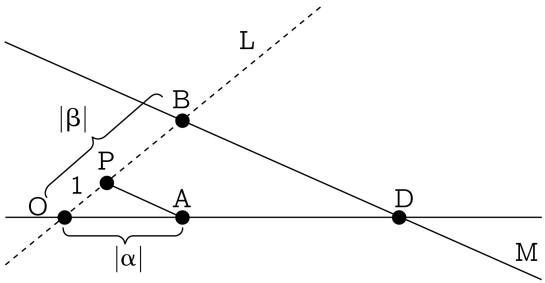
Demostración. Debemos demostrar las propiedades del Lema 1.3. Claramente 0 y 1 son elementos en W. Si $\alpha \in W$, entonces $-\alpha \in W$. En efecto, como existe un segmento de longitud $|\alpha| = |-\alpha|$, entonces $-\alpha \in W$. Sean $\alpha, \beta \in W$. Debemos probar que $\alpha - \beta \in W$. Como lo inversos aditivos de números constructibles lo son, basta considerar α, β positivos y demostrar que: $\alpha-(-\beta) = \alpha+\beta$ y $\alpha-\beta$ son constructibles.



Sean α, β 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 y D los puntos de intersección de la circunferencia con la recta L, tal que B está entre A y D. El segmento AD tiene longitud $|AD| = \alpha + \beta$.

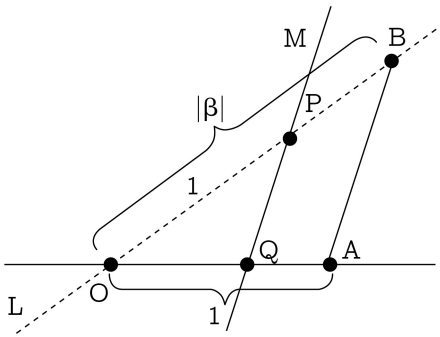
Demostraremos a continuación que $\alpha-\beta$ es constructible. Podemos suponer $\alpha \neq \beta$ y luego, $\alpha > \beta$ ó $\alpha < \beta$. Si $\alpha > \beta$, entonces F está entre A y B. Así, los segmentos FB y BD tienen longitud β. Ahora, el segmento AF tiene longitud $\alpha - \beta$. El caso $\alpha < \beta$, queda como ejercicio.

Demostraremos ahora que W es cerrado con el producto. 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 y B puntos de 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 $|\alpha\beta|$.

Demostraremos 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 conteniendo al 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 M con la recta que contiene al segmento OA. Los triángulos OQP y OAB son semejantes. Luego, $\frac{|OQ|}{1} = \frac{1}{|\beta|} = \left|\frac{1}{\beta}\right|$. Por lo tanto, OQ es de longitud $\left|\frac{1}{\beta}\right|$. □

Concluimos que, si $\alpha \in W$ y $\beta \in W$ con $\beta \neq 0$, entonces $\alpha \cdot \frac{1}{\beta} = \frac{\alpha}{\beta} \in W$. Como los números enteros son constructibles, obtenemos que:

Corolario 4.1. *Cada número racional es constructible.*

Ejemplo 4.4. *Como $\mathbb{Q}$ es un subcuerpo de W y $\sqrt{2} \in W$ (Ejemplo 4.2), entonces 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 subcuerpo de W.*

En el Ejemplo 4.8, demostraremos que es posible la construcción con regla y compás de un pentágono regular. Veremos que la solución del problema se reduce a probar que el real $\cos(\frac{2\pi}{5})$ es un número constructible. Interesa saber entonces, qué números reales son constructibles.

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 4.5. *Demostraremos que $\sqrt{5}$ es un número constructible. Consideremos $S = \mathbb{Q} \times \mathbb{Q}$, en la 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. Como sabemos, 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 $y = 0$. La intersección de la circunferencia con la recta son los puntos $P = (-\sqrt{5}, 0)$*

y $Q = (\sqrt{5}, 0)$. *Así,* P *y* Q *son puntos constructibles a partir de* $\mathbb{Q} \times \mathbb{Q}$. *La distancia del segmento de extremos* $(0,0)$ *y* $(\sqrt{5}, 0)$ *tiene longitud* $\sqrt{5}$, *lo que demuestra que* $\sqrt{5}$ *es un número constructible.*

Sea K un subcuerpo cualquiera de $\mathbb{R}$ 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 ahora reemplazamos S por el plano de K, en la definición 4.1, las rectas constructibles y las circunferencias constructibles están en el plano real euclideano y por lo tanto, tienen representaciones algebraicas. Utilizando geometría analítica elemental y el hecho que K es un cuerpo, es posible demostrar fácilmente los siguientes resultados:

Ejercicios 4.2.

1. 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.
2. 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.
3. Cualquier circunferencia que tenga como centro un punto del plano de K y como radio un elemento positivo en K, es una circunferencia en K.
4. Dos rectas distintas en K que se intersectan (en el plano real), se intersectan en un punto en el plano de K.

Si una recta en el plano de K y una circunferencia en el plano de K se intersectan en el plano real, entonces sus puntos de intersección (o el punto de intersección) no son necesariamente puntos en el plano de K, como veremos en el Teorema 4.2.

Definición 4.4. *Diremos que* K *es un* ***cuerpo constructible****, si* K *es un subcuerpo de* W. *Es decir,* K *es un subcuerpo de* $\mathbb{R}$ *y todo elemento en* K *es un número constructible.*

Teorema 4.2. *Sea* K *un subcuerpo 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 en el plano de* $K(\sqrt{\gamma})$ *donde* γ *en un real positivo en* K *y* $K(\sqrt{\gamma})$ *es una extensión de* K *de grado* 2. *Además, si* K *es un cuerpo 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. Sean $a_1x + b_1y + c_1 = 0$ y $x^2 + y^2 + a_2x + b_2y + c_2 = 0$ las ecuaciones de la recta y circunferencia en K que se intersectan en el plano real. Si suponemos que $b_1 \neq 0$, entonces $y = mx + n$, donde m, $n \in K$. Reemplazando y por $mx + n$, en la ecuación de la circunferencia, obtenemos una

ecuación de la forma $x^2 + bx + c = 0$, donde b, $c \in K$. Como existe intersección, sabemos que $b^2 - 4c \geq 0$.

Si $b^2 - 4c = \gamma$ es un cuadrado en K, entonces los puntos de intersección están en el plano de K. En consecuencia, necesariamente $b^2 - 4c = \gamma$ es positivo y no es un cuadrado en K. Luego, el polinomio $f(x) = x^2 + bx + c$ es irreducible en $K[x]$. Las raíces de $f(x)$ son $\frac{1}{2}(-b+\sqrt{\gamma})$ y $\frac{1}{2}(-b-\sqrt{\gamma})$. Así, $f(x)$ es el polinomio irreducible de $\frac{1}{2}(-b+\sqrt{\gamma})$ sobre K y por lo tanto, $K(\frac{1}{2}(-b+\sqrt{\gamma})) = K(\sqrt{\gamma})$ es una extensión de grado 2 de K.

Ahora, la intersección de la recta en K y la circunferencia en K (en el plano real) son los puntos

$$P(\frac{1}{2}(-b+\sqrt{\gamma}), \frac{1}{2}m(-b+\sqrt{\gamma})+n) \text{ y } Q(\frac{1}{2}(-b-\sqrt{\gamma}), \frac{1}{2}m(-b-\sqrt{\gamma})+n)$$

los cuales están en el plano de $K(\sqrt{\gamma})$.

El segmento de extremos $(0,0)$ y $(\frac{1}{2}(-b+\sqrt{\gamma}), 0)$ tiene longitud $\left|\frac{1}{2}(-b+\sqrt{\gamma})\right|$. Si suponemos que K es un cuerpo constructible, entonces $\frac{1}{2}(-b+\sqrt{\gamma})$ es un número constructible. El Teorema 4.1 implica que $\sqrt{\gamma}$ es constructible. Así,

$$K(\sqrt{\gamma}) = \{a + b\sqrt{\gamma} \,/\, a, b \in K\}$$

es un cuerpo constructible. □

Corolario 4.2. *Sea K un subcuerpo de $\mathbb{R}$. Si dos circunferencias en K se intersectan en el plano real, entonces sus puntos de intersección están en el plano de K o en el plano de $K(\sqrt{\gamma})$, donde γ en un real positivo en K y $K(\sqrt{\gamma})$ es una extensión de K de grado 2. Además, si K es un cuerpo 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 intersectan en el plano de K. Sabemos que

$$(a_1 - a_2)x + (b_1 - b_2)y + c_1 - c_2 = 0$$

es una recta que pasa por los puntos de intersección de ambas circunferencias. Por lo tanto, el problema se reduce a la intersección en el plano real de una recta y una circunferencia, ambas en K. Utilizando el teorema anterior se obtiene el Corolario. □

Teorema 4.2 y Corolario 4.2 implican que, cuando K es un cuerpo constructible, entonces los próximos números constructibles a partir de K (si es que existen) son números que están en cuerpos constructibles de la forma $K(\sqrt{\gamma})$, para algún $\gamma > 0$ en K.

Corolario 4.3. *Si α es un real positivo constructible, entonces $\sqrt{\alpha}$ es constructible.*

Demostración. Como $\mathbb{Q}$ es un cuerpo constructible y α es constructible, entonces $\mathbb{Q}(\alpha)$ es un subcuerpo de W. Podemos suponer que $\sqrt{\alpha} \notin \mathbb{Q}(\alpha)$. Ahora, $(0, \frac{1}{2}(\alpha - 1))$ es un punto en el plano de $\mathbb{Q}(\alpha)$ y $\frac{1}{2}(\alpha + 1) > 0$ es un número positivo en $\mathbb{Q}(\alpha)$,

entonces $x^2 + (y - \frac{1}{2}(\alpha - 1))^2 = (\frac{1}{2}(\alpha + 1))^2$ es una circunferencia en el plano de $\mathbb{Q}(\alpha)$. La intersección de la circunferencia con la recta $y = 0$ son los puntos $(\sqrt{\alpha}, 0)$ y $(-\sqrt{\alpha}, 0)$, los cuales están en el plano de $\mathbb{Q}(\alpha)(\sqrt{\alpha}) = \mathbb{Q}(\sqrt{\alpha})$. Por el Teorema 4.2, concluimos que $\sqrt{\alpha}$ es un número constructible. □

Una conclusión inmediata de este resultado es el que sigue:

Corolario 4.4. *Si K es un cuerpo constructible y $\alpha \in K$ es un número positivo, entonces $K(\sqrt{\alpha})$ es un cuerpo constructible.*

Ejemplo 4.6. *$\mathbb{Q}(\sqrt[4]{3})$ es un cuerpo constructible. En efecto, dado que $3 \in \mathbb{Q}$ es constructible, entonces $\mathbb{Q}(\sqrt{3})$ es un cuerpo constructible (Corolario 4.4). Como $\sqrt{3} \in \mathbb{Q}(\sqrt{3})$, entonces $\mathbb{Q}(\sqrt{3})(\sqrt{\sqrt{3}}) = \mathbb{Q}(\sqrt[4]{3})$ es un cuerpo constructible.*

Podemos observar que, utilizando el criterio de Schöneman-Eisenstein, el polinomio $p(x) = x^4 - 3$ es irreducible en $\mathbb{Q}[x]$. Así, $[\mathbb{Q}(\sqrt[4]{3}) : \mathbb{Q}] = 2^2$.

Observación 4.1. *El Teorema 4.2 y sus Corolarios naturalmente son válidos si reemplazamos el cuerpo K por $\mathbb{Q}$. Así, podemos obtener cuerpos 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 cuerpo 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 cuerpo 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 cuerpo constructible. (Demostrar que se puede continuar en forma infinita con este proceso).

Lema 4.1. *Sea F un cuerpo 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 cuerpo construcible.*

Demostración. Como $[E : F] = 2$, existe una base $\{1, \alpha\}$ de E como espacio vectorial sobre F. Por lo tanto, $E = F(1, \alpha) = F(\alpha)$. Sea $q(x) = x^2 + bx + c \in F[x]$ el polinomio irreducible de α sobre F. Ahora, $\alpha = \frac{1}{2}(-b + \sqrt{b^2 - 4c})$ ó $\alpha = \frac{1}{2}(-b - \sqrt{b^2 - 4c})$. Dado que, $b^2 - 4c$ es un real positivo (α es un número real y $\alpha \notin F$) y constructible, entonces por el Corolario 4.2, $E = F(\alpha) = F(\sqrt{b^2 - 4c})$ es un cuerpo constructible. □

Teorema 4.3. *Un número real $\alpha \notin \mathbb{Q}$ es un número constructible, si podemos encontrar una sucesión finita de cuerpos $F_0 = \mathbb{Q}$, $F_1, \ldots, F_k$ 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 cuerpos 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 cuerpo constructible, por el Lema 4.1, F_1 lo es. Utilizando nuevamente el Lema 4.1, F_2 es un cuerpo constructible. Continuando con el mismo argumento, obtenemos que F_k es un cuerpo 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 cuerpos $F_0 = \mathbb{Q}$, $F_1, \ldots, F_k$ 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

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

y cada término del producto es 2, obtenemos que $[F_k : \mathbb{Q}] = 2^k$. □

Ejemplo 4.7. *Demostraremos que $\alpha = \sqrt[8]{2}$ es un número constructible. Notemos que $\alpha^2 = \sqrt[4]{2}$ y $\alpha^4 = \sqrt{2}$. Por el criterio de Schöneman-Eisenstein, $p(x) = x^8 - 2$ es el polinomio irreducible de α sobre $\mathbb{Q}$. Así, $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 8$. Claramente, $\mathbb{Q}(\alpha) = \mathbb{Q}(\alpha^4, \alpha^2, \alpha)$ y como $\alpha^4 \in \mathbb{Q}(\alpha^2)$, entonces tenemos*

$$\begin{array}{c} \mathbb{Q}(\alpha) \\ | \\ \mathbb{Q}(\alpha^2) \\ | \\ \mathbb{Q}(\alpha^4) \\ | \\ \mathbb{Q} \end{array}$$

Claramente, $[\mathbb{Q}(\alpha^4) : \mathbb{Q}] = 2$. Por el criterio de Schöneman-Eisenstein, $q(x) = x^4 - 2$ es el polinomio irreducible de α^2 sobre $\mathbb{Q}$. Luego, $[\mathbb{Q}(\alpha^2) : \mathbb{Q}] = 4$ y necesariamente $[\mathbb{Q}(\alpha^2) : \mathbb{Q}(\alpha^4)] = 2$. 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, $[\mathbb{Q}(\alpha) : \mathbb{Q}(\alpha^2)] = 2$. Concluimos que $\alpha = \sqrt[8]{2}$ es un número constructible.

Ejercicios 4.3.

1. Demostrar que $\mathbb{Q}(\sqrt{2}, \sqrt{5})$ es un cuerpo constructible.
2. Demostrar que $\sqrt{2} + \sqrt{5}$ es un número constructible.

El siguiente teorema nos entrega un criterio para determinar la no constructibilidad de un número real.

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.*

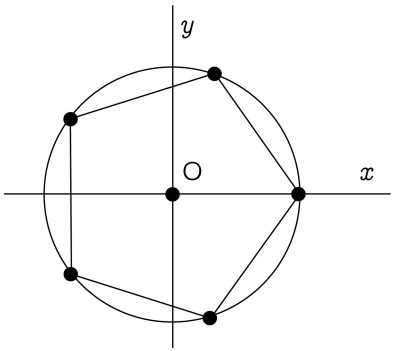
Demostración. Si α es constructible, entonces de acuerdo al Corolario 4.5 existe una extensión finita K de $\mathbb{Q}$ tal que $\alpha \in K$ y $[K : \mathbb{Q}] = 2^r$ para algún $r \geq 2$. Pero $\mathbb{Q}(\alpha) \subset K$. Luego, $[K : \mathbb{Q}] = [K : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}] = 2^r$, de donde necesariamente $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ es una potencia de 2. □

Desde los tiempos de Euclides (300 a.C.) se conocían construcciones con regla y compás para polígonos regulares de 3, 4, 5 y 15 lados. Gauss, a la edad de 19

años, demostró la construcción del polígono regular de 17 lados y fue el primero en determinar qué polígonos regulares se podían construir con regla y compás. Este resultado apareció publicado en su primer libro "Disquisitiones Arithmeticae" en 1801 (considerado una de las obras maestras de las matemáticas), pero su demostración quedó incompleta, siendo el matemático francés Pierre Wantzel el responsable en concluirla en 1837.

La demostración del resultado que sigue fue realizada por Eric T. Eekhoff, quien utiliza las ideas dadas por Gauss.

Ejemplo 4.8. *Demostraremos que es posible construir un pentágono regular con regla y compás. Consideremos un sistema coordenado cartesiano rectangular en el plano. Las raíces complejas de la ecuación* $x^5 - 1 = 0$, *geométricamente son puntos de la circunferencia unitaria y los vértices de un pentágono regular en el plano, como se indica en la figura.*



Las soluciones de la ecuación $x^5 - 1 = 0$ *son los complejos* α_0, α_1, α_2, α_3, α_4, *donde* $\alpha_k = \cos(\frac{2\pi k}{5}) + isen(\frac{2\pi k}{5})$ *para* $k = 0, 1, 2, 3, 4$.

Sea β_k *la parte real de cada* α_k. *Luego* $\beta_k = \cos(\frac{2\pi k}{5})$ *para* $k = 0, 1, 2, 3, 4$. *Dado que* $x^5 - 1 = (x-1)(x-\alpha_1)\cdots(x-\alpha_4)$, *entonces* $1 + \alpha_1 + \alpha_2 + \alpha_3 + \alpha_4 = 0$, *de donde* $1 + \beta_1 + \beta_2 + \beta_3 + \beta_4 = 0$.

Como $\cos(2\pi - \frac{2\pi}{5}) = \cos(\frac{2\pi}{5})$, *entonces* $\cos(\frac{8\pi}{5}) = \cos(\frac{2\pi}{5})$. *Luego,* $\beta_4 = \beta_1$. *Ahora, de* $\beta_2 = \cos(\frac{4\pi}{5}) = \cos(\pi - \frac{\pi}{5}) = -\cos(\frac{\pi}{5})$ *y* $\beta_3 = \cos(\frac{6\pi}{5}) = \cos(\pi + \frac{\pi}{5}) = -\cos(\frac{\pi}{5})$, *obtenemos que* $\beta_2 = \beta_3$. *Por lo tanto,* $2\beta_1 + 2\beta_2 = -1$.

Reemplazando θ *por* $\frac{4\pi}{5}$ *y* σ *por* $\frac{2\pi}{5}$, *en la identidad* $\cos(\theta + \sigma) + \cos(\theta - \sigma) = 2\cos(\theta)\cos(\sigma)$, *obtenemos que* $\beta_1 + \beta_2 = 2\beta_1\beta_2$. *De esta última relación y dado que* $2\beta_1 + 2\beta_2 = -1$, *obtenemos que* $4\beta_1^2 + 2\beta_1 - 1 = 0$. *Luego.* $\beta_1 = \frac{1}{4}(-1 \pm \sqrt{5})$. *Como* $\beta_1 > 0$ *(α_1 es un punto en el primer cuadrante), entonces* $\beta_1 = \frac{1}{4}(-1 + \sqrt{5})$. *Por lo tanto,* $\beta_4 = \frac{1}{4}(-1 + \sqrt{5})$ *y* $\beta_2 = \beta_3 = \frac{1}{4}(-1 - \sqrt{5})$ *que claramente son números constructibles.*

4.3 Imposibilidad de ciertas Construcciones Geométricas

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.

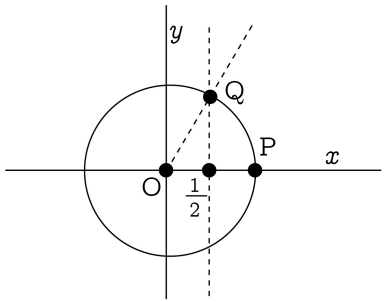
   Consideremos un cubo de lado igual a 1. Así, su volumen es 1. Deseamos construir el lado de un cubo de modo que su volumen sea 2. Luego, el lado de dicho volumen debe ser $\sqrt[3]{2}$. Como $p(x) = x^3 - 2$ es el polinomio irreducible de $\sqrt[3]{2}$ sobre $\mathbb{Q}$, entonces $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$. Por el Teorema 4.4, $\sqrt[3]{2}$ no es constructible.

2. **Cuadrar un círculo.** Dado un círculo no siempre es posible construir con regla y compás un cuadrado que tenga la misma área del círculo dado.

   Consideremos un círculo de radio 1. Así, su área es π. Deseamos construir un cuadrado de lado $\sqrt{\pi}$. Como π es trascendente, entonces $\sqrt{\pi}$ también lo es. En consecuencia, $\sqrt{\pi}$ no es constructible.

3. **Trisectar un ángulo.** Existen ángulos que no son posibles de trisectar con regla y compás.

   Demostraremos que no es posible trisectar un ángulo de 60^0. Consideremos un sistema coordenado cartesiano rectangular en el plano y la circunferencia de ecuación $x^2+y^2 = 1$. El punto $Q = (\frac{1}{2}, \frac{\sqrt{3}}{2})$ es constructible, pues sus coordenadas



   lo son. Si $P = (1, 0)$ y $O = (0, 0)$, entonces el coseno del ángulo POQ es $\frac{1}{2}$, luego el ángulo POQ mide 60^0. Para construir un ángulo de 20^0, necesitamos la construcción de un segmento de longitud $\cos(20^0)$.

   Sabemos que $\cos(3\theta) = 4\cos^3(\theta) - 3\cos(\theta)$ es una identidad. Haciendo $\theta = 20^0$, obtenemos que $4\cos^3(20^0) - 3\cos(20^0) = \frac{1}{2}$, de donde $\alpha = \cos(20^0)$ es una raíz del polinomio $p(x) = 8x^3 - 6x - 1$. Es fácil verificar que $p(x)$ es el polinomio irreducible de α sobre $\mathbb{Q}$ y por lo tanto, $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$. Del Teorema 4.4, α no es constructible.

Sea n un entero positivo y $\varphi : \mathbb{Z}^+ \to \mathbb{Z}^+$ la función tal que $\varphi(n)$ es el número de enteros positivos menores o iguales a n y primos relativos con n. Con los resultados del capítulo 5, demostraremos que cuando n es un entero con $n \geq 3$ y $\varphi(n)$ es una potencia de 2, entonces es posible construir con regla y compás un polígono regular de n lados.

4.4 Ejercicios de Reforzamiento

1. Determinar si las siguientes afirmaciones son verdaderas o falsas.
   a) El número real $\alpha = \frac{2-\sqrt{2}}{1+\sqrt{3}}$ no es constructible.
   b) Si α es un real tal que $\alpha^5 = 7$, entonces α es constructible.
   c) El real $\sqrt[4]{7}$ es un número constructible.
   d) El ángulo π no puede ser trisectado con regla y compás.
   e) El ángulo $\frac{1}{4}\pi$ es constructible con regla y compás.
2. Sea $\alpha \in \mathbb{R}$ una raíz del polinomio $p(x) = x^4 - 16x^2 + 4 \in \mathbb{Q}[x]$. Encontrar una extensión K de $\mathbb{Q}$ tal que $[K : \mathbb{Q}] = 2$ y $[\mathbb{Q}(\alpha) : K] = 2$. Concluir que α es un real constructible.
3. Sean α, β reales no nulos tales que α es constructible y β no lo es, ¿es $\alpha + \beta$ constructible?
4. ¿Puede construirse el ángulo $\frac{2}{5}\pi$ con regla y compás? ¿Puede trisectarse el ángulo $\frac{2}{5}\pi$ con regla y compás?
5. Demostrar que el ángulo θ puede ser trisectado con regla y compás, si y solo si, el polinomio $4x^3 - 4x - \cos(\theta)$ es reducible sobre $\mathbb{Q}(\cos(\theta))$.
6. ¿Es correcto el siguiente razonamiento? Si a, b son reales constructibles, entonces considerando un sistema coordenado cartesiano rectangular en el plano, podemos construir un punto de coordenadas (a, b). Como $(a, b) = a + bi$, entonces el número complejo $a + bi$ es constructible con regla y compás.

Capítulo 5: Elementos de la Teoría de Galois

La teoría de Galois es una colección de resultados que conectan la teoría de cuerpos con la teoría de grupos. La teoría de Galois debe su nombre a su creador, el matemático francés Évariste Galois fallecido a los 20 años. El nacimiento de dicha teoría estuvo motivada por el intento de responder a la siguiente pregunta: ¿por qué no existe una fórmula para la resolución de ecuaciones polinómicas de quinto grado (o superior) en términos de los coeficientes del polinomio, usando operaciones algebraicas (suma, resta, multiplicación, división) y la extracción de raíces (raíces cuadradas, cúbicas, etc.), tal como existe para las ecuaciones de segundo, tercer y cuarto grado?

Évariste Galois (1811-1832), considerado un genio de las matemáticas, se interesó por esta disciplina a la edad de 15 años, motivado por su profesor Hippolyte Jean Vernier. Después de asimilar rápidamente las matemáticas que enseñaban en su escuela, Galois empezó a estudiar textos más avanzados de aquella época: estudio la geometría de Legendre y el álgebra de Lagrange. Galois se interesó por el estudio del álgebra, llegando a conocer varios problemas no resueltos de esta disciplina. Empezó a trabajar, intentando encontrar una fórmula que diera cuenta de las raíces de un polinomio de quinto grado. Galois le asoció a un polinomio el grupo de permutaciones de sus raíces, ahora llamado el grupo de Galois en su honor. En esa época el concepto de grupo existía sólo en forma rudimentaria, fue Galois el primero en reconocer su importancia. Mucho se ha escrito sobre la vida de Galois. En [2], [10] y [17] se incluyen biografías de este talentoso matemático.

El resultado principal de este capítulo es el Teorema Fundamental de la Teoría de Galois. En dicho teorema se demuestra la existencia de una estrecha relación entre las raíces de un polinomio $f(x) \in F[x]$ (F un subcuerpo de los complejos) y un grupo asociado a $f(x)$ llamado el grupo de Galois de $f(x)$. Más precisamente, si $gr(f) = n \geq 1$ y $\alpha_1, \ldots, \alpha_n$ son todas las raíces complejas de $f(x)$ y consideramos el cuerpo $K = F(\alpha_1, \ldots, \alpha_n)$, llamado **el cuerpo de descomposición de** $f(x)$, entonces existe una correspondencia biyectiva entre los subcuerpos de K que contienen a F y los subgrupos del grupo de automorfismos σ del cuerpo K, para los cuales $\sigma(x) = x$ para todo $x \in F$.

Estudiaremos el grupo de Galois de un polinomio de grado 3 y demostraremos que los polinomios no constantes de grados ≤ 4 son solubles por radicales.

Como una aplicación del Teorema Fundamental de la Teoría de Galois, demostraremos que: un polígono regular de n lados es constructible, si y solo si, $\varphi(n)$ es una potencia de 2 y $n \geq 3$, donde $\varphi : \mathbb{Z}^+ \to \mathbb{Z}^+$ es la función φ de Euler.

Todos los cuerpos considerados en este capítulo serán subcuerpos de los números complejos $\mathbb{C}$. Sean F, L cuerpos. Diremos que $\sigma : F \to L$ es un homomorfismo, cuando $\sigma : F \to L$ sea un homomorfismo de anillos y diremos que $\sigma : F \to L$ es un monomorfismo, cuando $\sigma : F \to L$ sea monomorfismo de anillos.

5.1 Introducción

Iniciamos este capítulo con dos ejemplos con los que pretendemos motivar el estudio de la teoría que desarrollaremos, la que nos permitirá demostrar el Teorema Fundamental de la Teoría de Galois.

Ejemplo 5.1. *Consideremos el polinomio $p(x) = x^2+1 \in \mathbb{Q}[x]$. El cuerpo de descomposición de $p(x)$ es $\mathbb{Q}(i, -i) = \mathbb{Q}(i)$. Como $p(x) = x^2 + 1$ es el polinomio irreducible de i sobre $\mathbb{Q}$, entonces $\mathbb{Q}(i) = \{a + bi \ / \ a, \ b \in \mathbb{Q}\}$. Encontraremos a continuación todos los automorfismos del cuerpo $\mathbb{Q}(i)$.*

Sea $\sigma : \mathbb{Q}(i) \to \mathbb{Q}(i)$ un automorfismo. La restricción de σ a $\mathbb{Q}$, es decir, $\sigma_{\mathbb{Q}} : \mathbb{Q} \to \mathbb{Q}(i)$ tal que $\sigma_{\mathbb{Q}}(a) = \sigma(a)$ para todo $a \in \mathbb{Q}$, es un monomorfismo. Luego, del Corolario 1.1, $\sigma(a) = a$ para todo $a \in \mathbb{Q}$. Como $(\sigma(i))^2 = \sigma(i)\sigma(i) = \sigma(i^2) = \sigma(-1) = -1$, entonces $\sigma(i) = i$ ó $\sigma(i) = -i$. Por lo tanto, $\sigma(i) \in \mathbb{Q}(i)$. De esta forma, tenemos dos posibles automorfismos del cuerpo $\mathbb{Q}(i)$:

$$\sigma_1 : \mathbb{Q}(i) \to \mathbb{Q}(i) \ \ con \ \ \sigma_1(i) = i, \quad y \quad \sigma_2 : \mathbb{Q}(i) \to \mathbb{Q}(i) \ \ con \ \ \sigma_2(i) = -i.$$

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

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

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

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

Es fácil demostrar que σ_2 es un automorfismo de $\mathbb{Q}(i)$. El lector puede verificar que $G = \{\sigma_1, \ \sigma_2\}$ es un grupo con la composición de funciones. Observemos que $[\mathbb{Q}(i) : \mathbb{Q}] = \circ(G)$, donde $\circ(G)$ denota el orden de G.

Ejemplo 5.2. *Consideremos el polinomio $f(x) = (x^2 - 2)(x^2 - 5) \in \mathbb{Q}[x]$. El cuerpo de descomposición de $f(x)$ es $\mathbb{Q}(\sqrt{2}, -\sqrt{2}, \sqrt{5}, -\sqrt{5}) = \mathbb{Q}(\sqrt{2}, \sqrt{5})$. Encontraremos los automorfismos del cuerpo $\mathbb{Q}(\sqrt{2}, \sqrt{5})$.*

Sea $\sigma : \mathbb{Q}(\sqrt{2}, \sqrt{5}) \to \mathbb{Q}(\sqrt{2}, \sqrt{5})$ un automorfismo. Por el mismo argumento dado en el ejemplo anterior, $\sigma(a) = a$ para todo $a \in \mathbb{Q}$. Como $(\sigma(\sqrt{2}))^2 = \sigma(\sqrt{2})\sigma(\sqrt{2}) = \sigma(\sqrt{2}\sqrt{2}) = \sigma(2) = 2$, entonces $\sigma(\sqrt{2}) = \pm\sqrt{2}$. Luego, $\sigma(\sqrt{2}) \in \mathbb{Q}(\sqrt{2}, \sqrt{5})$. Análogamente, $\sigma(\sqrt{5}) = \pm\sqrt{5}$ y así, $\sigma(\sqrt{5}) \in \mathbb{Q}(\sqrt{2}, \sqrt{5})$. Por lo tanto, tenemos 4 posibles automorfismos del cuerpo $\mathbb{Q}(\sqrt{2}, \sqrt{5})$:

$$\sigma_1 : \mathbb{Q}(\sqrt{2}, \sqrt{5}) \to \mathbb{Q}(\sqrt{2}, \sqrt{5}) \ \ con \ \ \sigma_1(\sqrt{2}) = \sqrt{2} \ \ y \ \ \sigma_1(\sqrt{5}) = \sqrt{5}.$$

$$\sigma_2 : \mathbb{Q}(\sqrt{2}, \sqrt{5}) \to \mathbb{Q}(\sqrt{2}, \sqrt{5}) \ \ con \ \ \sigma_2(\sqrt{2}) = \sqrt{2} \ \ y \ \ \sigma_2(\sqrt{5}) = -\sqrt{5}.$$

$$\sigma_3 : \mathbb{Q}(\sqrt{2}, \sqrt{5}) \to \mathbb{Q}(\sqrt{2}, \sqrt{5}) \ \ con \ \ \sigma_3(\sqrt{2}) = -\sqrt{2} \ \ y \ \ \sigma_3(\sqrt{5}) = \sqrt{5}.$$

$$\sigma_4 : \mathbb{Q}(\sqrt{2},\sqrt{5}) \to \mathbb{Q}(\sqrt{2},\sqrt{5}) \ \ con\ \ \sigma_4(\sqrt{2}) = -\sqrt{2}\ \ y\ \ \sigma_4(\sqrt{5}) = -\sqrt{5}.$$

Del Ejemplo 3.12, sabemos que

$$\mathbb{Q}(\sqrt{2},\sqrt{5}) = \{a + b\sqrt{2} + c\sqrt{5} + d\sqrt{10} \ / \ a,\ b,\ c,\ d \in \mathbb{Q}\}$$

El lector puede verificar que las funciones σ_1, σ_2, σ_3, σ_4 definidas por:

$$\begin{aligned}
&\sigma_1(a + b\sqrt{2} + c\sqrt{5} + d\sqrt{10}) = a + b\sqrt{2} + c\sqrt{5} + d\sqrt{10},\\
&\sigma_2(a + b\sqrt{2} + c\sqrt{5} + d\sqrt{10}) = a + b\sqrt{2} - c\sqrt{5} - d\sqrt{10},\\
&\sigma_3(a + b\sqrt{2} + c\sqrt{5} + d\sqrt{10}) = a - b\sqrt{2} + c\sqrt{5} - d\sqrt{10},\\
&\sigma_4(a + b\sqrt{2} + c\sqrt{5} + d\sqrt{10}) = a - b\sqrt{2} - c\sqrt{5} + d\sqrt{10},
\end{aligned}$$

son automorfismos del cuerpo $\mathbb{Q}(\sqrt{2},\sqrt{5})$ y que $G = \{\sigma_1, \sigma_2, \sigma_3, \sigma_4\}$ es un grupo con la composición de funciones. Los subgrupos de G son: $H_1 = \{\sigma_1\}$, $H_2 = \{\sigma_1, \sigma_2\}$, $H_3 = \{\sigma_1, \sigma_3\}$, $H_4 = \{\sigma_1, \sigma_4\}$ y $H_5 = G$. Podemos observar que $[\mathbb{Q}(\sqrt{2},\sqrt{5}) : \mathbb{Q}] = \circ(G) = 4$. Ahora, a cada subgrupo H de G, le asociaremos el conjunto

$$\{x \in \mathbb{Q}(\sqrt{2},\sqrt{5}) \ / \ \sigma(x) = x \text{ para todo } \sigma \in H\}$$

que resulta ser un subcuerpo de $\mathbb{Q}(\sqrt{2},\sqrt{5})$. Las demostraciones de las siguientes afirmaciones quedan como ejercicios para el lector:

$H_1 = \{\sigma_1\}$ *le asociamos el cuerpo* $\mathbb{Q}(\sqrt{2},\sqrt{5})$,
$H_2 = \{\sigma_1, \sigma_2\}$ *le asociamos el cuerpo* $\mathbb{Q}(\sqrt{2})$,
$H_3 = \{\sigma_1, \sigma_3\}$ *le asociamos el cuerpo* $\mathbb{Q}(\sqrt{5})$,
$H_4 = \{\sigma_1, \sigma_4\}$ *le asociamos el cuerpo* $\mathbb{Q}(\sqrt{10})$,
$H_5 = G$ *le asociamos el cuerpo* $\mathbb{Q}$.

El Teorema Fundamental de la Teoría de Galois nos permitirá afirmar que la correspondencia encontrada anteriormente resulta ser una biyección entre los subgrupos de G y los subcuerpos de $\mathbb{Q}(\sqrt{2},\sqrt{5})$.

Como decíamos al comienzo de este capítulo, los cuerpos considerados en el desarrollo de la Teoría de Galois, serán subcuerpos de $\mathbb{C}$. Iniciamos esta teoría, recordando un resultado de Teoría de Grupos. Si S es un conjunto no vacío, entonces el conjunto $A(S) = \{\phi \ / \ \phi : S \to S \text{ es biyección } \}$ es un grupo con la composición de funciones. En el caso que $S = E$ y E es un cuerpo, entonces el conjunto

$$Aut(E) = \{\phi \ / \ \phi : E \to E \text{ es un automorfismo de anillos}\}$$

resulta ser un subgrupo de $A(E)$. La demostración de dicho resultado la dejamos como ejercicio para el lector. Así, $Aut(E)$ es un grupo con la composición de funciones, llamado el **grupo de automorfismos del cuerpo** E.

Consideremos una extensión E de un cuerpo F. Si $\sigma : E \to E$ es un automorfismo del cuerpo E tal que $\sigma(x) = x$ para todo $x \in F$, diremos que σ es un **automorfismo de E que fija** F. Demostraremos que tales automorfismos forman un grupo con la composición de funciones.

Teorema 5.1. *Sea E una extensión de un cuerpo F. Entonces el conjunto*

$$G(E/F) = \{\sigma \ / \ \sigma : E \to E \text{ es un automorfismo que fija } F\}$$

es un subgrupo del grupo de automorfismos de E.

Demostración. Sean σ, $\tau \in G(E/F)$ y $a \in F$. Entonces $\sigma\tau(a) = \sigma(\tau(a)) = \sigma(a) = a$. De este modo, $\sigma\tau \in G(E/F)$. Claramente la función identidad de E es un elemento en $G(E/F)$. Si $\sigma \in G(E/F)$ y $a \in F$, entonces $\sigma(a) = a$. Así, $\sigma^{-1}(a) = \sigma^{-1}\sigma(a) = a$ y por lo tanto, $\sigma^{-1} \in G(E/F)$. □

Definición 5.1. *El grupo $G(E/F)$ del Teorema 5.1, se dice que es el* ***grupo de automorfismos de*** *E* ***que fijan*** *F o que es el* ***grupo de*** *E* ***sobre*** *F.*

Ejemplo 5.3. *En el Ejemplo 5.1, encontramos que el grupo de automorfismo del cuerpo $\mathbb{Q}(i)$ es $Aut(\mathbb{Q}(i)) = \{\sigma_1, \sigma_2\}$, siendo σ_1 y σ_2 automorfismos que fijan $\mathbb{Q}$. En consecuencia, $G(\mathbb{Q}(i)/\mathbb{Q}) = \{\sigma_1, \sigma_2\}$ es el grupo de $\mathbb{Q}(i)$ sobre $\mathbb{Q}$.*

Ejemplo 5.4. *Del Ejemplo 5.2, obtenemos que*

$G(\mathbb{Q}(\sqrt{2}, \sqrt{5})/\mathbb{Q}) = \{\sigma_1, \sigma_2, \sigma_3, \sigma_4\}$,
$G(\mathbb{Q}(\sqrt{2}, \sqrt{5})/\mathbb{Q}(\sqrt{2})) = \{\sigma_1, \sigma_2\}$,
$G(\mathbb{Q}(\sqrt{2}, \sqrt{5})/\mathbb{Q}(\sqrt{5})) = \{\sigma_1, \sigma_3\}$,
$G(\mathbb{Q}(\sqrt{2}, \sqrt{5})/\mathbb{Q}(\sqrt{10})) = \{\sigma_1, \sigma_4\}$.

Ejemplo 5.5. *Encontraremos el grupo de automorfismos de $\mathbb{Q}(\sqrt[3]{5})$ que fijan $\mathbb{Q}$. El polinomio irreducible de $\sqrt[3]{5}$ sobre $\mathbb{Q}$ es $p(x) = x^3 - 5$ y la única raíz real de $p(x)$ es $\sqrt[3]{5}$.*

Sea $\sigma : \mathbb{Q}(\sqrt[3]{5}) \to \mathbb{Q}(\sqrt[3]{5})$ un automorfismo que fija $\mathbb{Q}$. Dado que $(\sigma(\sqrt[3]{5}))^3 = \sigma((\sqrt[3]{5})^3) = \sigma(5) = 5$ y $\sigma(\sqrt[3]{5})$ es un real, entonces $\sigma(\sqrt[3]{5}) = \sqrt[3]{5}$. Un elemento cualquiera de $\mathbb{Q}(\sqrt[3]{5})$ es de la forma $a + b\sqrt[3]{5} + c(\sqrt[3]{5})^2$ con a, b, $c \in \mathbb{Q}$. Luego, $\sigma(a + b\sqrt[3]{5} + c(\sqrt[3]{5})^2) = \sigma(a) + \sigma(b)\sigma(\sqrt[3]{5}) + \sigma(c)(\sigma(\sqrt[3]{5}))^2 = a + b\sqrt[3]{5} + c(\sqrt[3]{5})^2$, es decir, $\sigma = I$ es la identidad de $\mathbb{Q}(\sqrt[3]{5})$. Por lo tanto, el grupo de automorfismos de $\mathbb{Q}(\sqrt[3]{5})$ que fijan $\mathbb{Q}$ es $G(\mathbb{Q}(\sqrt[3]{5})/\mathbb{Q}) = \{I\}$.

5.2 Monomorfismos

Para encontrar los automorfismos del cuerpo $\mathbb{Q}(\sqrt{2}, \sqrt{5})$, del ejemplo 5.2, podríamos haber razonado de la siguiente forma: primero encontrar los monomorfismos de $\mathbb{Q}(\sqrt{2})$ en $\mathbb{C}$ y posteriormente, para cada monomorfismo $\tau : \mathbb{Q}(\sqrt{2}) \to \mathbb{C}$, encontrar los monomorfismos $\sigma : (\mathbb{Q}(\sqrt{2}))(\sqrt{5}) \to \mathbb{C}$ para los cuales $\sigma(a + b\sqrt{2}) = \tau(a + b\sqrt{2})$ para todo a, $b \in \mathbb{Q}$. De esta forma, habríamos encontrado todos los monomorfismos de $\mathbb{Q}(\sqrt{2}, \sqrt{5})$ en $\mathbb{C}$ y elegimos aquéllos que resultan ser automorfismos de $\mathbb{Q}(\sqrt{2}, \sqrt{5})$.

La demostración del Teorema 5.2, nos entregará un método que nos permitirá construir todos los monomorfismos $\tau : F(\alpha) \to \mathbb{C}$, para los cuales $\tau(x) = \sigma(x)$ para todo $x \in F$, donde F es un cuerpo, $\alpha \in \mathbb{C}$ es algebraico sobre F y $\sigma : F \to \mathbb{C}$ es un monomorfismo.

Sea F un cuerpo y $\sigma : F \to \mathbb{C}$ un monomorfismo. Para el polinomio $f(x) = a_0 + a_1x + \cdots + a_nx^n \in F[x]$, definimos el polinomio $\sigma f(x) = \sigma(a_0) + \sigma(a_1)x + \cdots + \sigma(a_n)x^n \in \mathbb{C}[x]$. Es claro que $\sigma(F) = \{\sigma(a) \ / \ a \in F\}$ es un cuerpo isomorfo a F y que $\sigma f(x) \in \sigma(F)[x]$. Además, tenemos los siguientes resultados:

Lema 5.1. *Sea F un cuerpo y $\sigma : F \to \mathbb{C}$ un monomorfismo. Entonces:*

a) Para todo $f(x), g(x) \in F[x] : \sigma(f(x)+g(x)) = \sigma f(x)+\sigma g(x)$ y $\sigma(f(x)g(x)) = \sigma f(x) \cdot \sigma g(x)$.
b) Si $f(x) \in F[x]$ es no nulo, entonces $gr(f(x)) = gr(\sigma f(x))$.
c) Si $g_0(x) \in \sigma(F)[x]$, entonces existe $g(x) \in F[x]$ tal que $\sigma g(x) = g_0(x)$.
d) Si $f(x), g(x) \in F[x]$ y $\sigma f(x) = \sigma g(x)$, entonces $f(x) = g(x)$.

Demostración. Las demostraciones de (a) y (d) quedan como ejercicios. Para probar (b) consideremos $f(x) = a_0 + a_1x + \cdots + a_nx^n \in F[x]$ con $a_n \neq 0$. Como $\sigma : F \to \mathbb{C}$ es inyectiva, entonces $\sigma(a_n) \neq 0$, lo que demuestra (b).

Para (c), sea $g_0(x) = d_0+d_1x+\cdots+d_nx^n \in \sigma(F)[x]$. Como cada $d_i \in \sigma(F)$, existe $b_i \in F$ tal que $\sigma(b_i) = d_i$. Así, $g_0(x) = \sigma(b_0) + \sigma(b_1)x + \cdots + \sigma(b_n)x^n$. Definiendo $g(x) = b_0 + b_1x + \cdots + b_nx^n \in F[x]$ obtenemos que $\sigma g(x) = g_0(x)$. □

Corolario 5.1. *Sea F un cuerpo y $\sigma : F \to \mathbb{C}$ un monomorfismo. Si $p(x)$ es un polinomio irreducible en $F[x]$, entonces $\sigma p(x)$ es un polinomio irreducible en $\sigma(F)[x]$.*

Demostración. Supongamos que $\sigma p(x)$ es un polinomio reducible en $\sigma(F)[x]$. Existen $g_0(x)$, $h_0(x) \in \sigma(F)[x]$ tales que $\sigma p(x) = g_0(x)h_0(x)$ con $gr(g_0) < gr(\sigma p) = gr(p)$ y $gr(h_0) < gr(\sigma p) = gr(p)$. De la parte (c) y (b) del Lema 5.1, existen $g(x)$, $h(x) \in F[x]$ tales que $\sigma g(x) = g_0(x)$ y $\sigma h(x) = h_0(x)$ con $gr(g) = gr(g_0)$ y $gr(h) = gr(h_0)$. Así, $\sigma p(x) = \sigma g(x) \cdot \sigma h(x) = \sigma(g(x)h(x))$. Ahora, del Lema 5.1 (d), $p(x) = g(x)h(x)$. Como $gr(g) < gr(p)$ y $gr(h) < gr(p)$, obtenemos una contradicción, dado que por hipótesis $p(x)$ es irreducible en $F[x]$. □

Lema 5.2. *Sea F un cuerpo, $f(x) \in F[x]$ y $\alpha \in \mathbb{C}$ algebraico sobre F. Si $\sigma : F(\alpha) \to \mathbb{C}$ es un monomorfismo, entonces $(\sigma f)(\sigma(\alpha)) = \sigma(f(\alpha))$. En particular, si α es una raíz de $f(x)$, entonces $\sigma(\alpha)$ es una raíz de $\sigma f(x)$.*

Demostración Si $f(x) = a_0 + a_1x + \cdots + a_nx^n \in F[x]$, entonces $\sigma f(x) = \sigma(a_0) + \sigma(a_1)x + \cdots + \sigma(a_n)x^n$. Luego,

$$\begin{aligned}(\sigma f)(\sigma(\alpha)) &= \sigma(a_0) + \sigma(a_1)\sigma(\alpha) + \cdots + \sigma(a_n)\sigma(\alpha)^n \\ &= \sigma(a_0) + \sigma(a_1)\sigma(\alpha) + \cdots + \sigma(a_n)\sigma(\alpha^n) \\ &= \sigma(a_0) + \sigma(a_1\alpha) + \cdots + \sigma(a_n\alpha^n) \\ &= \sigma(a_0 + a_1\alpha + \cdots + a_n\alpha^n) = \sigma(f(\alpha)).\end{aligned}$$ □

Definición 5.2. *Sea F un cuerpo, $\sigma : F \to \mathbb{C}$ un monomorfismo y E una extensión de F. Un monomorfismo $\tau : E \to \mathbb{C}$ se dice que es una extensión de σ, si $\tau(x) = \sigma(x)$ para todo $x \in F$.*

Ejemplo 5.6. *La función $\sigma : \mathbb{Q} \to \mathbb{C}$ definida por $\sigma(x) = x$ para todo $x \in \mathbb{Q}$, es un monomorfismo. Ahora, $\tau : \mathbb{Q}(\sqrt{5}) \to \mathbb{C}$ definida por $\tau(a+b\sqrt{5}) = a-b\sqrt{5}$ para todo a, $b \in \mathbb{Q}$, es un monomorfismo (dejamos la demostración como ejercicio). Observemos que $\tau(a) = a$ para todo $a \in \mathbb{Q}$ y luego, $\tau(x) = \sigma(x)$ para todo $x \in \mathbb{Q}$. Por lo tanto, $\tau : \mathbb{Q}(\sqrt{5}) \to \mathbb{C}$ es una extensión de σ.*

Sea F un cuerpo, $\sigma : F \to \mathbb{C}$ un monomorfismo y $\alpha \in \mathbb{C}$ algebraico sobre F. La demostración del teorema que sigue nos entrega un método para construir todas las extensiones $\tau : F(\alpha) \to \mathbb{C}$ de σ.

Teorema 5.2. *Sea F un cuerpo y $\sigma : F \to \mathbb{C}$ un monomorfismo. Sea $\alpha \in \mathbb{C}$ algebraico sobre F, $p(x) \in F[x]$ el polinomio irreducible de α sobre F y $\beta \in \mathbb{C}$ una raíz de $\sigma p(x) \in \mathbb{C}[x]$. Entonces:*

a) Existe una extensión $\tau : F(\alpha) \to \mathbb{C}$ de σ tal que $\tau(\alpha) = \beta$.

b) Para toda extensión $\tau : F(\alpha) \to \mathbb{C}$ de σ se tiene que $\tau(\alpha)$ es una raíz de $\sigma p(x)$.

Demostración. Recordemos primero que $F(\alpha) = \{f(\alpha) \ / \ f(x) \in F[x]\}$. Para probar (a), consideremos $\tau : F(\alpha) \to \mathbb{C}$ definida por $\tau(f(\alpha)) = \sigma f(\beta)$. Es decir,

$$\tau(a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_n\alpha^n) = \sigma(a_0) + \sigma(a_1)\beta + \sigma(a_2)\beta^2 + \cdots + \sigma(a_n)\beta^n.$$

Debemos demostrar que $\tau : F(\alpha) \to \mathbb{C}$ está bien definida. Esto es necesario, ya que podríamos tener dos polinomios distintos $f(x)$, $g(x)$ en $F[x]$ tales que $f(\alpha) = g(\alpha)$ con $\sigma f(\beta) \neq \sigma g(\beta)$. Demostraremos que tal situación no sucede.

Sean $f(x)$, $g(x)$ en $F[x]$ tales que $f(\alpha) = g(\alpha)$. El polinomio $f(x) - g(x)$ se anula en α. Así, $f(x) - g(x) \in \langle p(x) \rangle$ y luego, $f(x) - g(x) = p(x)q(x)$ con $q(x) \in F[x]$. De esta forma, $\sigma(f(x) - g(x)) = \sigma(p(x)q(x))$, de donde $\sigma f(x) - \sigma g(x) = \sigma p(x) \cdot \sigma q(x)$. Luego, $\sigma f(\beta) - \sigma g(\beta) = \sigma p(\beta) \cdot \sigma q(\beta) = 0$, lo cual implica que $\tau : F(\alpha) \to \mathbb{C}$ está bien definida.

Utilizando el Lema 5.1 (a), obtenemos que $\tau : F(\alpha) \to \mathbb{C}$ es un homomorfismo y claramente $\tau(\alpha) = \beta$. Sólo nos falta probar que $\tau : F(\alpha) \to \mathbb{C}$ es inyectiva.

Sea $\tau(f(\alpha)) = \tau(g(\alpha))$, donde $f(x)$, $g(x) \in F[x]$. Debemos demostrar que $f(\alpha) = g(\alpha)$. Por el algoritmo de Euclides existen polinomios $q(x)$, $r(x) \in F[x]$ tales que $f(x) - g(x) = p(x)q(x) + r(x)$, donde $r(x) = 0$ ó $gr(r) < gr(p)$. Por lo tanto, $\sigma f(x) - \sigma g(x) = \sigma p(x) \cdot \sigma q(x) + \sigma r(x)$, de donde obtenemos que $\sigma f(\beta) - \sigma g(\beta) = \sigma p(\beta) \cdot \sigma q(\beta) + \sigma r(\beta) = \sigma r(\beta)$. Pero $\tau(f(\alpha)) = \tau(g(\alpha))$, es decir, $\sigma f(\beta) = \sigma g(\beta)$. De esta forma, $\sigma r(\beta) = 0$. Por el Corolario 5.1, $\sigma p(x)$ es un polinomio irreducible y mónico en $\sigma(F)[x]$. Luego, $\sigma p(x)$ es el polinomio irreducible de β sobre $\sigma(F)$. Dado que $\sigma r(x) \in \sigma(F)[x]$, β es una raíz de $\sigma r(x)$ y $gr(\sigma r) = gr(r) < gr(p) = gr(\sigma p)$, entonces necesariamente $\sigma r(x) = 0$. El Lema 5.1 (d), implica que $r(x) = 0$. Finalmente, $f(x) - g(x) = p(x)q(x)$ y así, $f(\alpha) - g(\alpha) = p(\alpha)q(\alpha) = 0$.

La parte (b) del teorema es una conclusión inmediata del Lema 5.2. □

Ejemplo 5.7. *Encontraremos todos los monomorfismos de $\mathbb{Q}(\sqrt{2})$ en $\mathbb{C}$. Observemos primero que, si $\phi : \mathbb{Q}(\sqrt{2}) \to \mathbb{C}$ es un monomorfismo, entonces la restricción de*

ϕ a $\mathbb{Q}$ también lo es. Interesa saber cómo son los monomorfismos $\sigma : \mathbb{Q} \to \mathbb{C}$. El Corolario 1.1, nos dice que existe una única tal función $\sigma : \mathbb{Q} \to \mathbb{C}$ definida por $\sigma(x) = x$ para todo $x \in \mathbb{Q}$. En consecuencia, deseamos encontrar todas las extensiones $\phi : \mathbb{Q}(\sqrt{2}) \to \mathbb{C}$ de σ, para lo cual disponemos del Teorema 5.2.

El polinomio irreducible de $\sqrt{2}$ sobre $\mathbb{Q}$ es $p(x) = x^2 - 2$ y luego, $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \ / \ a, b \in \mathbb{Q}\}$. De acuerdo al Teorema 5.2, deseamos encontrar una raíz $\beta \in \mathbb{C}$ del polinomio $\sigma p(x) = x^2 - \sigma(2) = x^2 - 2$. Así, $\beta = \sqrt{2}$ o $\beta = -\sqrt{2}$. Por lo tanto, existen extensiones $\sigma_1 : \mathbb{Q}(\sqrt{2}) \to \mathbb{C}$ y $\sigma_2 : \mathbb{Q}(\sqrt{2}) \to \mathbb{C}$ de σ tales que $\sigma_1(\sqrt{2}) = \sqrt{2}$ y $\sigma_2(\sqrt{2}) = -\sqrt{2}$. Además, $\sigma_1(x) = \sigma_2(x) = \sigma(x) = x$ para todo $x \in \mathbb{Q}$. De esta forma, para todo $a, b \in \mathbb{Q}$:

$$\sigma_1(a + b\sqrt{2}) = \sigma_1(a) + \sigma_1(b)\sigma_1(\sqrt{2}) = a + b\sqrt{2}$$

y

$$\sigma_2(a + b\sqrt{2}) = \sigma_2(a) + \sigma_2(b)\sigma_2(\sqrt{2}) = a + b(-\sqrt{2}) = a - b\sqrt{2}.$$

Ejemplo 5.8. *Encontraremos todos los monomorfismos de $\mathbb{Q}(\sqrt[3]{2})$ en $\mathbb{C}$. En forma similar al ejemplo anterior, el problema a resolver es el de encontrar todas las extensiones $\tau : \mathbb{Q}(\sqrt[3]{2}) \to \mathbb{C}$ de la función $\sigma : \mathbb{Q} \to \mathbb{C}$ definida por $\sigma(x) = x$ para todo $x \in \mathbb{Q}$.*

El polinomio $p(x) = x^3 - 2$ no tiene raíces en $\mathbb{Q}$ y es de grado 3. Por lo tanto, $p(x) = x^3 - 2$ es el polinomio irreducible de $\sqrt[3]{2}$ sobre $\mathbb{Q}$, lo cual implica que $\mathbb{Q}(\sqrt[3]{2}) = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} \ / \ a, b, c \in \mathbb{Q}\}$.

Las raíces complejas de $\sigma p(x) = x^3 - \sigma(2) = x^3 - 2$ son $\sqrt[3]{2}$, $\sqrt[3]{2}\omega$ y $\sqrt[3]{2}\omega^2$, siendo $\omega = -\frac{1}{2} + \frac{1}{2}\sqrt{3}i$. Por lo tanto, existen extensiones $\sigma_1 : \mathbb{Q}(\sqrt[3]{2}) \to \mathbb{C}$, $\sigma_2 : \mathbb{Q}(\sqrt[3]{2}) \to \mathbb{C}$ y $\sigma_3 : \mathbb{Q}(\sqrt[3]{2}) \to \mathbb{C}$ de σ tales que $\sigma_1(\sqrt[3]{2}) = \sqrt[3]{2}$, $\sigma_2(\sqrt[3]{2}) = \sqrt[3]{2}\omega$ y $\sigma_3(\sqrt[3]{2}) = \sqrt[3]{2}\omega^2$. De esta forma, para todo a, b, $c \in \mathbb{Q}$:

$$\begin{aligned}
\sigma_1(a + b\sqrt[3]{2} + c\sqrt[3]{4}) &= \sigma_1(a) + \sigma_1(b)\sigma_1(\sqrt[3]{2}) + \sigma_1(c)\sigma_1(\sqrt[3]{2}\sqrt[3]{2})) \\
&= a + b\sqrt[3]{2} + c\sigma_1(\sqrt[3]{2})\sigma_1(\sqrt[3]{2}) = a + b\sqrt[3]{2} + c\sqrt[3]{4},
\end{aligned}$$

$$\begin{aligned}
\sigma_2(a + b\sqrt[3]{2} + c\sqrt[3]{4}) &= \sigma_2(a) + \sigma_2(b)\sigma_2(\sqrt[3]{2}) + \sigma_2(c)\sigma_2(\sqrt[3]{2}\sqrt[3]{2})) \\
&= a + b\sqrt[3]{2}\omega + c\sigma_2(\sqrt[3]{2})\sigma_2(\sqrt[3]{2}) \\
&= a + b\sqrt[3]{2}\omega + c\sqrt[3]{2}\omega\sqrt[3]{2}\omega \\
&= a + b\sqrt[3]{2}\omega + c\sqrt[3]{4}\omega^2,
\end{aligned}$$

$$\begin{aligned}
\sigma_3(a + b\sqrt[3]{2} + c\sqrt[3]{4}) &= \sigma_3(a) + \sigma_3(b)\sigma_3(\sqrt[3]{2}) + \sigma_3(c)\sigma_3(\sqrt[3]{2}\sqrt[3]{2})) \\
&= a + b\sqrt[3]{2}\omega^2 + c\sigma_3(\sqrt[3]{2})\sigma_3(\sqrt[3]{2}) \\
&= a + b\sqrt[3]{2}\omega^2 + c\sqrt[3]{2}\omega^2\sqrt[3]{2}\omega^2 \\
&= a + b\sqrt[3]{2}\omega^2 + c\sqrt[3]{4}\omega^4 \\
&= a + b\sqrt[3]{2}\omega^2 + c\sqrt[3]{4}\omega.
\end{aligned}$$

El resultado que sigue es una conclusión inmediata del Teorema 5.2.

Corolario 5.2. *Sea F un cuerpo, $\sigma : F \to \mathbb{C}$ un monomorfismo, $\alpha \in \mathbb{C}$ algebraico sobre F y $p(x)$ el polinomio irreducible de α sobre F de grado n. Entonces, el número posible de extensiones $\tau : F(\alpha) \to \mathbb{C}$ de σ es igual a $[F(\alpha) : F] = n$.*

Demostración. Del Lema 5.1 (b), $gr(p(x)) = gr(\sigma p(x)) = n$. Del Corolario 5.1, $\sigma p(x)$ es irreducible en $\sigma(F)[x]$ y del Corolario 3.4, las n raíces en $\mathbb{C}$ de $\sigma p(x)$ son distintas. Utilizando el Teorema 5.2, obtenemos el Corolario. □

Ejercicios 5.1.

1. Encontrar todos los monomorfismos de $\mathbb{Q}(\sqrt[3]{3})$ en $\mathbb{C}$.
2. Encontrar todas las extensiones $\tau : \mathbb{Q}(i, \sqrt{3}) \to \mathbb{C}$ de $\sigma : \mathbb{Q}(i) \to \mathbb{C}$ definida por $\sigma(a + bi) = a - bi$ para todo $a, b \in \mathbb{Q}$. Recordar que $\mathbb{Q}(i, \sqrt{3}) = \mathbb{Q}(i)(\sqrt{3})$.
3. Encontrar todos los monomorfismos de $\mathbb{Q}(\sqrt{2} + i)$ en $\mathbb{C}$.

Corolario 5.3. *Sea F un cuerpo, $\sigma : F \to \mathbb{C}$ un monomorfismo y $\alpha, \beta \in \mathbb{C}$ algebraicos sobre F. Entonces, el número de extensiones $\tau : F(\alpha, \beta) \to \mathbb{C}$ de σ es igual a $[F(\alpha, \beta) : F]$.*

Demostración. Sea $[F(\alpha) : F] = n$. Por el Corolario 5.2, el número posible de extensiones de $F(\alpha)$ en $\mathbb{C}$ de σ es igual a $[F(\alpha) : F] = n$. Sean $\sigma_1, \ldots, \sigma_n$ tales extensiones. Para cada $j \in \{1, \ldots, n\}$, $\sigma_j : F(\alpha) \to \mathbb{C}$ es un monomorfismo. El número posible de extensiones de $F(\alpha, \beta) = F(\alpha)(\beta)$ en $\mathbb{C}$ de σ_j es $[F(\alpha)(\beta) : F(\alpha)]$. Luego, existen $n[F(\alpha)(\beta) : F(\alpha)]$ extensiones $\tau : F(\alpha, \beta) \to \mathbb{C}$ de σ. Del Corolario 3.1, obtenemos que $n[F(\alpha)(\beta) : F(\alpha)] = [F(\alpha) : F][F(\alpha)(\beta) : F(\alpha)] = [F(\alpha, \beta) : F]$. □

El resultado que sigue es una generalización del Corolario 5.3, el que se demuestra por inducción.

Corolario 5.4. *Sea F un cuerpo, $\sigma : F \to \mathbb{C}$ un monomorfismo de cuerpos y $\alpha_1, \ldots, \alpha_k \in \mathbb{C}$ algebraicos sobre F. Entonces, el número de extensiones*

$$\tau : F(\alpha_1, \ldots, \alpha_k) \to \mathbb{C}$$

de σ es igual a $[F(\alpha_1, \ldots, \alpha_k) : F]$.

Ejemplo 5.9. *Encontraremos todos los monomorfismos de $\mathbb{Q}(\sqrt{2}, i)$ en $\mathbb{C}$. Recordemos que $\mathbb{Q}(\sqrt{2}, i) = \mathbb{Q}(\sqrt{2})(i)$. Así tenemos*

$$\begin{array}{c} \mathbb{Q}(\sqrt{2})(i) \\ | \\ \mathbb{Q}(\sqrt{2}) \\ | \\ \mathbb{Q} \end{array}$$

Demostrar como ejercicio que $\{1, \sqrt{2}\}$ es una base de $\mathbb{Q}(\sqrt{2})$ como espacio vectorial sobre $\mathbb{Q}$ y $\{1, i\}$ es una base de $\mathbb{Q}(\sqrt{2})(i)$ como espacio vectorial sobre $\mathbb{Q}(\sqrt{2})$.

Ahora, $\{1, \sqrt{2}, i, \sqrt{2}i\}$ *es una base de* $\mathbb{Q}(\sqrt{2}, i)$ *como espacio vectorial sobre* $\mathbb{Q}$ *y en consecuencia,* $\mathbb{Q}(\sqrt{2}, i) = \{a + b\sqrt{2} + ci + d\sqrt{2}i \ / \ a, b, c, d \in \mathbb{Q}\}$.

Cualquier monomorfismo de $\mathbb{Q}(\sqrt{2}, i)$ *en* $\mathbb{C}$ *es una extensión de la función* $\sigma : \mathbb{Q} \to \mathbb{C}$ *tal que* $\sigma(x) = x$ *para todo* $x \in \mathbb{Q}$. *Del Ejemplo 5.7, sabemos que* $\sigma_1 : \mathbb{Q}(\sqrt{2}) \to \mathbb{C}$ *y* $\sigma_2 : \mathbb{Q}(\sqrt{2}) \to \mathbb{C}$ *definidas por* $\sigma_1(a + b\sqrt{2}) = a + b\sqrt{2}$ *y* $\sigma_2(a + b\sqrt{2}) = a - b\sqrt{2}$ *para todo* $a, b \in \mathbb{Q}$, *son las únicas extensiones de* σ. *Por lo tanto, cualquier monomorfismo de* $\mathbb{Q}(\sqrt{2}, i)$ *en* $\mathbb{C}$ *debe ser una extensión de* σ_1 *ó* σ_2.

Encontraremos las extensiones $\tau : \mathbb{Q}(\sqrt{2})(i) \to \mathbb{C}$ *de* σ_1. *El polinomio irreducible de* i *sobre* $\mathbb{Q}(\sqrt{2})$ *es* $p(x) = x^2 + 1$. *Las raíces de* $\sigma_1 p(x) = x^2 + \sigma_1(1) = x^2 + 1$ *son* i, $-i$. *De esta forma, existen dos extensiones de* σ_1. *Estas son:* $\tau_1 : \mathbb{Q}(\sqrt{2})(i) \to \mathbb{C}$ *tal que* $\tau_1(i) = i$ *y* $\tau_2 : \mathbb{Q}(\sqrt{2})(i) \to \mathbb{C}$ *tal que* $\tau_2(i) = -i$. *Además,* $\tau_1(a + b\sqrt{2}) = \sigma_1(a + b\sqrt{2}) = a + b\sqrt{2}$ *para todo* a, $b \in \mathbb{Q}$ *y* $\tau_2(a + b\sqrt{2}) = \sigma_1(a + b\sqrt{2}) = a + b\sqrt{2}$ *para todo* a, $b \in \mathbb{Q}$.

A continuación encontraremos las extensiones $\tau : \mathbb{Q}(\sqrt{2})(i) \to \mathbb{C}$ *de* σ_2. *Como el polinomio irreducible de* i *sobre* $\mathbb{Q}(\sqrt{2})$ *es* $q(x) = x^2 + 1$, *entonces las raíces de* $\sigma_2 q(x) = x^2 + \sigma_2(1) = x^2 + 1$ *son* i, $-i$. *Así, existen dos extensiones de* σ_2. *Estas son* $\tau_3 : \mathbb{Q}(\sqrt{2})(i) \to \mathbb{C}$ *tal que* $\tau_3(i) = i$ *y* $\tau_4 : \mathbb{Q}(\sqrt{2})(i) \to \mathbb{C}$ *tal que* $\tau_4(i) = -i$. *Además,* $\tau_3(a + b\sqrt{2}) = \sigma_2(a + b\sqrt{2}) = a - b\sqrt{2}$ *para todo* $a, b \in \mathbb{Q}$ *y* $\tau_4(a + b\sqrt{2}) = \sigma_2(a + b\sqrt{2}) = a - b\sqrt{2}$ *para todo* $a, b \in \mathbb{Q}$.

Por lo tanto, obtenemos que $\tau_1(\sqrt{2}) = \sqrt{2}$, $\tau_1(i) = i$, $\tau_2(\sqrt{2}) = \sqrt{2}$, $\tau_2(i) = -i$, $\tau_3(\sqrt{2}) = -\sqrt{2}$, $\tau_3(i) = i$ *y* $\tau_4(\sqrt{2}) = -\sqrt{2}$, $\tau_4(i) = -i$. *Como era de esperar, encontramos* 4 *monomorfismos de* $\mathbb{Q}(\sqrt{2}, i)$ *en* $\mathbb{C}$:

$$\begin{aligned}
&\tau_1(a + b\sqrt{2} + ci + d\sqrt{2}i) = a + b\sqrt{2} + ci + d\sqrt{2}i \quad \text{para todo } a, b, c, d \in \mathbb{Q},\\
&\tau_2(a + b\sqrt{2} + ci + d\sqrt{2}i) = a + b\sqrt{2} - ci - d\sqrt{2}i \quad \text{para todo } a, b, c, d \in \mathbb{Q},\\
&\tau_3(a + b\sqrt{2} + ci + d\sqrt{2}i) = a - b\sqrt{2} + ci - d\sqrt{2}i \quad \text{para todo } a, b, c, d \in \mathbb{Q},\\
&\tau_4(a + b\sqrt{2} + ci + d\sqrt{2}i) = a - b\sqrt{2} - ci + d\sqrt{2}i \quad \text{para todo } a, b, c, d \in \mathbb{Q}.
\end{aligned}$$

Teorema 5.3. Teorema del elemento primitivo
Sea E *una extensión finita de un cuerpo* F. *Entonces existe un elemento* $\gamma \in E$ *tal que* $E = F(\gamma)$.

Demostración. Demostraremos que este teorema es una conclusión del siguiente resultado: si α, $\beta \in \mathbb{C}$ son algebraicos sobre F, entonces existe $\gamma \in F(\alpha, \beta)$ tal que $F(\alpha, \beta) = F(\gamma)$. La demostración de dicho resultado es la que sigue:

Sean α, $\beta \in \mathbb{C}$ algebraicos sobre F, $[F(\alpha, \beta) : F] = n$ y $\sigma : F \to \mathbb{C}$ definida por $\sigma(x) = x$ para todo $x \in F$. Por el Corolario 5.3, existen $\sigma_1, \ldots, \sigma_n$ extensiones de $F(\alpha, \beta)$ en $\mathbb{C}$ de σ todas distintas. Luego, cada $\sigma_i : F(\alpha, \beta) \to \mathbb{C}$ es un monomorfismo tal que $\sigma_i(x) = \sigma(x) = x$ para todo $x \in F$.

Probaremos que podemos encontrar un elemento $a \in F$ tal que $\sigma_i(\alpha + a\beta)$ son distintos para todo $i \in \{1, \ldots, n\}$. Observemos que el polinomio $\sigma_j(\alpha) - \sigma_i(\alpha) + (\sigma_j(\beta) - \sigma_i(\beta))x$ es no nulo, cuando $i \neq j$. De no ser así, tendríamos $\sigma_i = \sigma_j$ con $i \neq j$, lo que es una contradicción. Consideremos el polinomio $h(x) = \Pi_{i \neq j}(\sigma_j(\alpha) -$

$\sigma_i(\alpha) + (\sigma_j(\beta) - \sigma_i(\beta))x)$, que es no nulo. Dicho polinomio posee un número finito de raíces en $\mathbb{C}$, luego podemos encontrar un elemento $a \in F$ tal que $h(a) = \Pi_{i \neq j}(\sigma_j(\alpha) - \sigma_i(\alpha) + (\sigma_j(\beta) - \sigma_i(\beta))a) \neq 0$. Así, para $i \neq j$, $\sigma_j(\alpha) - \sigma_i(\alpha) + (\sigma_j(\beta) - \sigma_i(\beta))a = \sigma_j(\alpha + a\beta) - \sigma_i(\alpha + a\beta) \neq 0$, lo cual implica que $\sigma_i(\alpha + a\beta)$ son distintos para todo $i \in \{1, \ldots, n\}$. Sea $\gamma = \alpha + a\beta$. Claramente $F(\gamma)$ es un subcuerpo de $F(\alpha, \beta)$. Demostraremos que $F(\gamma) = F(\alpha, \beta)$.

Las restricciones de cada $\sigma_i : F(\alpha, \beta) \to \mathbb{C}$ a $F(\gamma)$ siguen siendo monomorfismos, es decir, extensiones de σ. Como $\sigma_1(\gamma), \ldots, \sigma_n(\gamma)$ son todos distintos, entonces $\sigma_1, \ldots, \sigma_n$ de $F(\gamma)$ en $\mathbb{C}$ son todos distintos. Por el Corolario 5.2, $[F(\gamma) : F] \geq n$. Dado que $F(\gamma)$ es un subespacio vectorial de $F(\alpha, \beta)$ sobre F, $[F(\alpha, \beta) : F] = n$ y $[F(\gamma) : F] \geq n$, entonces $F(\alpha, \beta) = F(\gamma)$.

Si E es una extensión finita de un cuerpo F, por el Teorema 3.6, existen elementos $\delta_1, \ldots, \delta_k$ en E tales que $E = F(\delta_1, \ldots, \delta_k)$. Por lo demostrado anteriormente, existe $\gamma_1 \in F(\delta_1, \delta_2)$ tal que $F(\delta_1, \delta_2) = F(\gamma_1)$. Ahora, $E = F(\delta_1, \ldots, \delta_k) = F(\delta_1, \delta_2)(\delta_3, \ldots, \delta_k) = F(\gamma_1)(\delta_3, \ldots, \delta_k) = F(\gamma_1, \delta_3, \ldots, \delta_k) = F(\gamma_1, \delta_3)(\delta_4, \ldots, \delta_k)$. Continuando inductivamente con este proceso, demostramos lo deseado. □

Ejercicios 5.2.

1. Encontrar $\gamma \in \mathbb{C}$ tal que $\mathbb{Q}(\sqrt{2}, \sqrt{5}) = \mathbb{Q}(\gamma)$.
2. Encontrar $\gamma \in \mathbb{C}$ tal que $\mathbb{Q}(\sqrt[3]{3}, i) = \mathbb{Q}(\gamma)$.
3. Encontrar todos los monomorfismos de $\mathbb{Q}(\sqrt{2}, \sqrt{2}i)$ en $\mathbb{C}$.
4. Encontrar todos los monomorfismos de $\mathbb{Q}(\sqrt{3}, \sqrt{5})$ en $\mathbb{C}$.

5.3 Extensión de Galois

Definición 5.3. *Sea E una extensión finita de un cuerpo F. Un monomorfismo $\tau : E \to \mathbb{C}$* ***se dice que fija*** *F, si $\tau(x) = x$ para todo $x \in F$.*

Observemos que los monomorfismos $\tau : E \to \mathbb{C}$ que fijan F son simplemente las extensiones $\tau : E \to \mathbb{C}$ de la función $\sigma : F \to \mathbb{C}$ definida por $\sigma(x) = x$ para todo $x \in F$.

Lema 5.3. *Sea K una extensión finita de un cuerpo F y $\tau : K \to \mathbb{C}$ un monomorfismo que fija F. Si $\tau(K) \subset K$, entonces $\tau(K) = K$.*

Demostración. Como $\tau : K \to \mathbb{C}$ fija F, entonces $\tau : K \to \mathbb{C}$ es una función lineal. En efecto, para $x, y \in K$ y $a \in F$ se tiene que $\tau(x+y) = \tau(x)+\tau(y)$ y $\tau(ax) = \tau(a)\tau(x) = a\tau(x)$. Dado que $\tau : K \to \mathbb{C}$ es lineal inyectiva, entonces $Ker(\tau) = \{0\}$. Ahora, $\dim_F(K) = \dim_F(Ker(\tau))+\dim_F(\tau(K))$ implica que $\dim_F(\tau(K)) = \dim_F(K)$. Como $\tau(K)$ es un subespacio de K, obtenemos que $\tau(K) = K$. □

Ejemplo 5.10. *En el Ejemplo 5.9, encontramos todos los monomorfismos*

$$\tau : \mathbb{Q}(\sqrt{2}, i) \to \mathbb{C}.$$

Estos monomorfismos fijan $\mathbb{Q}$ *y además,* $\tau(\mathbb{Q}(\sqrt{2},i)) \subset \mathbb{Q}(\sqrt{2},i)$. *Por el Lema 5.3,* τ_1, τ_2, τ_3, τ_4 *son todos los automorfismos de* $\mathbb{Q}(\sqrt{2},i)$. *En consecuencia,* $G(\mathbb{Q}(\sqrt{2},i)/\mathbb{Q}) = \{\tau_1, \tau_2, \tau_3, \tau_4\}$, *que como sabemos es un grupo bajo la composición de funciones.*

Dado que $\tau_1(\sqrt{2}) = \sqrt{2}$, $\tau_1(i) = i$, $\tau_2(\sqrt{2}) = \sqrt{2}$, $\tau_2(i) = -i$, $\tau_3(\sqrt{2}) = -\sqrt{2}$, $\tau_3(i) = i$, $\tau_4(\sqrt{2}) = -\sqrt{2}$, $\tau_4(i) = -i$, *entonces* $\tau_2\tau_3(\sqrt{2}) = \tau_2(\tau_3(\sqrt{2})) = \tau_2(-\sqrt{2}) = -\tau_2(\sqrt{2}) = -\sqrt{2}$ *y* $\tau_2\tau_3(i) = \tau_2(\tau_3(i)) = \tau_2(i) = -i$. *Por lo tanto,* $\tau_2\tau_3 = \tau_4$. *En forma similar se encuentran los otros productos, obteniéndose la tabla:*

$\circ$	τ_1	τ_2	τ_3	τ_4
τ_1	τ_1	τ_2	τ_3	τ_4
τ_2	τ_2	τ_1	τ_4	τ_3
τ_3	τ_3	τ_4	τ_1	τ_2
τ_4	τ_4	τ_3	τ_2	τ_1

Teorema 5.4. *Sea* G *el grupo de automorfismos de un cuerpo* K *y* H *un subgrupo de* G. *Entonces, el conjunto* $K^H = \{x \in K \,/\, \sigma(x) = x \;\; \forall\, \sigma \in H\}$ *es un cuerpo, llamado el* ***cuerpo fijo de*** H.

Demostración. Basta con demostrar que K^H es un subcuerpo de K. Es claro que para $\sigma \in H$, $\sigma(0) = 0$ y $\sigma(1) = 1$. Así, 1 y 0 son elementos de K^H.

Sean x, $y \in K^H$ y $\sigma \in H$. Entonces $\sigma(x) = x$ y $\sigma(y) = y$. Ahora, $\sigma(x - y) = \sigma(x) - \sigma(y) = x - y$ y $\sigma(xy) = \sigma(x)\sigma(y) = xy$ implican que $x - y \in K^H$ y $xy \in K^H$.

Sea $x \in K^H$ no nulo y $\sigma \in H$. Como $\sigma : (K^*, \cdot) \to (K^*, \cdot)$ es un homomorfismo de grupos, entonces $\sigma(x^{-1}) = \sigma(x)^{-1} = x^{-1}$ y por lo tanto, $x^{-1} \in K^H$. Hemos demostrado que K^H es un subcuerpo de K. □

Ejemplo 5.11. *Consideremos el grupo* $G = \{\tau_1, \tau_2, \tau_3, \tau_4\}$ *del ejemplo 5.9 y el subgrupo* $H = \{\tau_1, \tau_2\}$ *de* G. *Encontraremos el cuerpo fijo de* H. *Sabemos que* τ_1 *es la función identidad de* $\mathbb{Q}(\sqrt{2},i)$ *y* $\tau_2 : \mathbb{Q}(\sqrt{2},i) \to \mathbb{Q}(\sqrt{2},i)$ *está definida por* $\tau_2(a + b\sqrt{2} + ci + d\sqrt{2}i) = a + b\sqrt{2} - ci - d\sqrt{2}i$ *para todo* a, b, c, $d \in \mathbb{Q}$. *Ahora,*

$$\begin{aligned}(\mathbb{Q}(\sqrt{2},i))^H &= \{x \in \mathbb{Q}(\sqrt{2},i) \,/\, \tau_1(x) = x \text{ y } \tau_2(x) = x\} \\ &= \{a + b\sqrt{2} + ci + d\sqrt{2}i \,/\, \tau_2(a + b\sqrt{2} + ci + d\sqrt{2}i) = \\ &\qquad a + b\sqrt{2} + ci + d\sqrt{2}i\}.\end{aligned}$$

Si $\tau_2(a + b\sqrt{2} + ci + d\sqrt{2}i) = a + b\sqrt{2} + ci + d\sqrt{2}i$, *entonces* $a + b\sqrt{2} - ci - d\sqrt{2}i = a + b\sqrt{2} + ci + d\sqrt{2}i$. *Así,* $2(c + d\sqrt{2})i = 0$, *de donde* $c + d\sqrt{2} = 0$ *y luego,* $c = d = 0$. *Por lo tanto, el cuerpo fijo de* H *es*

$$(\mathbb{Q}(\sqrt{2},i))^H = \{a + b\sqrt{2} \,/\, a, b \in \mathbb{Q}\} = \mathbb{Q}(\sqrt{2}).$$

Ejercicios 5.3.

1. Considerar el grupo $G = \{\tau_1, \tau_2, \tau_3, \tau_4\}$ del ejemplo 5.9 y el subgrupo $H = \{\tau_1, \tau_4\}$ de G. Encontrar el cuerpo fijo de H.

2. Considerar el grupo $G = \{\tau_1, \tau_2, \tau_3, \tau_4\}$ del ejemplo 5.9. Encontrar el cuerpo fijo de G. .

Definición 5.4. *Una extensión finita K de un cuerpo F, se dice que es una* ***extensión de Galois****, si para todo monomorfismo $\sigma : K \to \mathbb{C}$ que fija F se tiene que $\sigma(K) = K$. Es decir, para todo monomorfismo $\sigma : K \to \mathbb{C}$ se tiene que $\sigma \in G(K/F)$.*

Ejemplo 5.12. *La extensión $\mathbb{Q}(\sqrt{2}, i)$ de $\mathbb{Q}$, considerada en el ejemplo 5.9, es una extensión de Galois.*

Ejemplo 5.13. *La extensión $\mathbb{Q}(\sqrt[3]{2})$ de $\mathbb{Q}$, considerada en el ejemplo 5.8, no es una extensión de Galois. En efecto, $\sigma_2(\sqrt[3]{2}) = \sqrt[3]{2}(-\frac{1}{2} + \frac{1}{2}\sqrt{3}i) \notin \mathbb{Q}(\sqrt[3]{2})$.*

Teorema 5.5. *Una extensión finita K de un cuerpo F es una extensión de Galois, si y solo si, K es el cuerpo de descomposición de algún polinomio $f(x) \in F[x]$.*

Demostración. Sea K una extensión de Galois de F. Como K es una extensión finita de F, existe $\alpha \in K$ tal que $K = F(\alpha)$ (Teorema 5.3). Sea $p(x)$ el polinomio irreducible de α sobre F y $gr(p) = n$. Sabemos que existen n distintos monomorfismo de K en $\mathbb{C}$ que fijan F. Como K es una extensión de Galois de F, entonces estos n homomorfismos son automorfismos de K. Sean $\sigma_1, \ldots, \sigma_n$ tales automorfismos de K. Por el Teorema 5.2, $\sigma_1(\alpha) = \alpha_1, \ldots, \sigma_n(\alpha) = \alpha_n$ son las n raíces de $p(x)$ y todas en K. Luego, $K = F(\alpha_1, \ldots, \alpha_n)$.

Inversamente, supongamos que K es el cuerpo de descomposición de un polinomio $f(x) \in F[x]$ (no necesariamente irreducible) con raíces $\alpha_1, \ldots, \alpha_n \in \mathbb{C}$. Así, $K = F(\alpha_1, \ldots, \alpha_n)$. Sea $\sigma : K \to \mathbb{C}$ un monomorfismo que fija F y α_i una de las raíces de $f(x)$. Si $q(x)$ es el polinomio irreducible de α_i sobre F, entonces $q(x)$ es un divisor de $f(x)$. Por el Teorema 5.2, $\sigma(\alpha_i)$ es una raíz de $q(x)$ y luego, una raíz de $f(x)$. Por lo tanto, $\sigma(\alpha_i) \in K$. Así, σ es un automorfismo de K, lo que demuestra que K es una extensión de Galois de F. □

Observación 5.1. *Consideremos F un cuerpo, $p(x) \in F[x]$ irreducible en $F[x]$ y $gr(p) = n$. Si $\alpha_1, \ldots, \alpha_n \in \mathbb{C}$ son las raíces de $p(x)$ (las que son todas distintas), $K = F(\alpha_1, \ldots, \alpha_n)$ es el cuerpo de descomposición de $p(x)$ y $\tau \in G(K/F)$, entonces $\tau(\alpha_1), \ldots, \tau(\alpha_n)$ son las mismas n raíces distintas de $p(x)$. Luego, τ permuta las raíces $\alpha_1, \ldots, \alpha_n$ de $p(x)$. De esta forma, podemos mirar a τ como un elemento del grupo de permutaciones S_n de n elementos $\{1, \ldots, n\}$. Concluimos que, $G(K/F)$ es isomorfo a un subgrupo de S_n.*

Del Corolario 5.4, el número de elementos del grupo $G(K/F)$ es $[K : F]$.

Ejercicios 5.4.

1. Sea K una extensión de Galois de un cuerpo F. Si $p(x) \in F[x]$ es irreducible en $F[x]$ y $\alpha \in K$ es una raíz de $p(x)$, demostrar que $p(x)$ tiene todas sus raíces en K.
2. Sea F un subcuerpo de $\mathbb{C}$ y $\alpha, \beta \in \mathbb{C}$ algebraicos sobre F. Si $F(\alpha)$, $F(\beta)$ son extensiones de Galois de F, demostrar que $F(\alpha, \beta)$ es una extensión de Galois de F.

5.4 Teorema Fundamental de la Teoría de Galois

Teorema 5.6. *Sea K una extensión de Galois de un cuerpo F. Sea $G = G(K/F)$ el grupo de automorfismos de K sobre F. Entonces F es el cuerpo fijo de G.*

Demostración. El cuerpo fijo de G es el conjunto

$$K^G = \{x \in K \ / \ \sigma(x) = x \text{ para todo } \sigma \in G\}.$$

Sea $E = K^G$. Debemos demostrar que $F = E$. Claramente $F \subset E$. Supongamos que $F \neq E$. Existe $\alpha \in E$ tal que $\alpha \notin F$. Como $\alpha \in K$ y K es algebraico sobre F, entonces existe el polinomio irreducible $p(x) \in F[x]$ de α sobre F. Necesariamente $gr(p) > 1$, dado que $\alpha \notin F$, así tenemos que $[F(\alpha) : F] = n > 1$. Luego, existe un monomorfismo $\sigma : F(\alpha) \to \mathbb{C}$ tal que $\sigma(\alpha) \neq \alpha$ (Teorema 5.2). Sea $\tau : K \to \mathbb{C}$ una extensión de $\sigma : F(\alpha) \to \mathbb{C}$. Como K es una extensión de Galois de F, entonces $\tau(K) = K$, de donde $\tau \in G$. Ahora, $\tau(\alpha) = \sigma(a) \neq \alpha$. En consecuencia, $\alpha \notin E$, lo que es una contradicción. Por lo tanto, $E = K^G = F$. □

Definición 5.5. *Si K es una extensión de Galois de un cuerpo F, entonces el grupo de automorfismos de K que fijan F (es decir, $G(K/F)$) es llamado* ***el grupo de Galois de*** *K* ***sobre*** *F.*

Si F es un cuerpo y K es el cuerpo de descomposición del polinomio $f(x) \in F[x]$, entonces diremos que $G(K/F)$ es el ***grupo de Galois de*** *$f(x)$.*

Teorema 5.7. Teorema Fundamental de Teoría de Galois.
Sea K una extensión de Galois de un cuerpo F y E un cuerpo tal que $F \leq E \leq K$. Entonces:

a) K es una extensión de Galois de E.
b) E es el cuerpo fijo del subgrupo $G(K/E)$ de $G(K/F)$ y $[K : E] = \circ(G(K/E))$.
c) La función: $E \to G(K/E)$ del conjunto de cuerpos intermedios entre F y K y el conjunto de subgrupos de $G(K/F)$ es inyectiva y sobreyectiva.
d) Si E_0 es un cuerpo tal que $F \leq E_0 \leq E \leq K$, entonces $G(K/E) \leq G(K/E_0)$.
e) Si H_0, H son subgrupos de $G(K/F)$ y $H_0 \leq H$, entonces $K^H \leq K^{H_0}$.

Demostración.
a) Sea $\tau : K \to \mathbb{C}$ una extensión de $\sigma : E \to \mathbb{C}$ definida por $\sigma(x) = x$ para todo $x \in E$. Ahora, $\sigma : E \to \mathbb{C}$ es una extensión de $i : F \to \mathbb{C}$ definida por $i(x) = x$ para todo $x \in F$. Como $\tau : K \to \mathbb{C}$ es una extensión de $i : F \to \mathbb{C}$ y K es una extensión de Galois de F, entonces $\tau(K) = K$. Por lo tanto, K es una extensión de Galois de E.
b) Es una conclusión inmediata de (*a*) y del Teorema 5.4.
c) Demostraremos primero que la función es inyectiva.

Sean E, E' cuerpos distintos tales que $F \leq E \leq K$ y $F \leq E' \leq K$. Sabemos que los cuerpos fijos de $G(K/E)$ y $G(K/E')$ son E y E', respectivamente. Como

$E \neq E'$, entonces necesariamente $G(K/E) \neq G(K/E')$ y por lo tanto, la función es inyectiva.

Demostraremos que la función es sobreyectiva. Sea H un subgrupo de $G(K/F)$. Debemos demostrar que existe un cuerpo E con $F \leq E \leq K$ tal que $H = G(K/E)$. Dado que K es una extensión finita de F, existe $\alpha \in K$ tal que $K = F(\alpha)$ (Teorema 5.3). Sea $H = \{\sigma_1, \ldots, \sigma_r\}$ y $f(x) = (x - \sigma_1(\alpha)) \cdots (x - \sigma_r(\alpha))$. Claramente $gr(f) = r$. Para cualquier $\sigma \in H$, los elementos $\sigma\sigma_1, \ldots, \sigma\sigma_r$ siguen estando en H y son todos distintos. Luego, $\{\sigma\sigma_1, \ldots, \sigma\sigma_r\} = \{\sigma_1, \ldots, \sigma_r\}$ lo cual implica que $\{\sigma\sigma_1(\alpha), \ldots, \sigma\sigma_r(\alpha)\} = \{\sigma_1(\alpha), \ldots, \sigma_r(\alpha)\}$. Por lo tanto, $\sigma f(x) = (x - \sigma\sigma_1(\alpha)) \cdots (x - \sigma\sigma_1(\alpha_r) = f(x)$. El coeficiente de x^{r-1} del polinomio $\sigma f(x)$ es

$$(-\sigma\sigma_1(\alpha)) - \cdots - \sigma\sigma_1(\alpha_r)) = \sigma(-\sigma_1(\alpha) - \cdots - \sigma_1(\alpha_r))$$

y el de $f(x)$ es

$$-\sigma_1(\alpha) - \cdots - \sigma_1(\alpha_r)$$

Se debe tener que

$$\sigma(-\sigma_1(\alpha) - \cdots - \sigma_1(\alpha_r)) = -\sigma_1(\alpha) - \cdots - \sigma_1(\alpha_r)$$

Así, el coeficiente a_{r-1} de x^{r-1} del polinomio $f(x)$ es invariante por los elementos de H. Esto es, $\sigma_i(a_{r-1}) = a_{r-1}$ para todo $i \in \{1, \ldots, r\}$. Por lo tanto, a_{r-1} es un elemento del cuerpo fijo de H, el que denotamos por E. El lector puede verificar que la misma situación ocurre con el resto de los coeficientes del polinomio $f(x)$. Es decir, los coeficientes de $f(x)$ son elementos en E. Así, $f(x)$ es un polinomio en $E[x]$ y que se anula en α, de donde $[K : E] \leq r$. Pero $\sigma_1, \ldots, \sigma_r$ son r distintos automorfismos de K que fijan E, en consecuencia $[K : E] \geq r$. Por lo tanto, $[K : E] = r$ y $H = G(K/E)$.

Las afirmaciones (d) y (e) son de fácil demostración. □

Observación 5.2. *Sea K una extensión de Galois de un cuerpo F y $G(K/F)$ el grupo de Galois de K sobre F. Si E_0, E son cuerpos tales que $F \leq E_0 \leq E \leq K$ y H_0, H son subgrupos de $G(K/F)$ tales que $H_0 \leq H$, de acuerdo al Teorema 5.7, obtenemos las correspondencias:*

$$\begin{array}{ccc} K & \to & \{I_K\} \\ | & & \downarrow \\ E & \to & G(K/E) \\ | & & \downarrow \\ E_0 & \to & G(K/E_0) \\ | & & \downarrow \\ F & \to & G(K/F) \end{array} \qquad y \qquad \begin{array}{ccc} G(K/F) & \to & F \\ | & & \downarrow \\ H & \to & K^H \\ | & & \downarrow \\ H_0 & \to & K^{H_0} \\ | & & \downarrow \\ \{I_K\} & \to & K \end{array}$$

Como

$$[K : E] = \circ(G(K/E)),\ [K : F] = \circ(G(K/F))\ \ y\ \ [K : E][E : F] = [K : F],$$

obtenemos que

$$[E : F] = \frac{\circ(G(K/F))}{\circ(G(K/E))}.$$

Ejemplo 5.14. *Consideremos el polinomio* $p(x) = x^3 - 2 \in \mathbb{Q}[x]$. *Las raíces en* $\mathbb{C}$ *de* $p(x)$ *son* $\sqrt[3]{2}$, $\sqrt[3]{2}(-\frac{1}{2} + \frac{1}{2}\sqrt{3}i)$, $\sqrt[3]{2}(-\frac{1}{2} - \frac{1}{2}\sqrt{3}i)$ *y el cuerpo de decomposición de* $p(x)$ *es* $K = \mathbb{Q}(\sqrt[3]{2}, \sqrt{3}i)$.

Encontraremos los elementos del grupo de Galois $G(K/\mathbb{Q})$ *y la correspondencia biyectiva entre los cuerpos* E *tales que* $\mathbb{Q} \leq E \leq K$ *y los subgrupos de* $G(K/\mathbb{Q})$. *Sea* $\alpha = \sqrt[3]{2}$ *y* $\omega = -\frac{1}{2} + \frac{1}{2}\sqrt{3}i$. *Notemos que* $\omega^2 = -\frac{1}{2} - \frac{1}{2}\sqrt{3}i$ *y* $\omega^3 = 1$. *Así, las raíces de* $p(x)$ *son* α, $\alpha\omega$ *y* $\alpha\omega^2$.

Como $p(x) = x^3 - 2$ *es irreducible en* $\mathbb{Q}[x]$, *entonces* $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$ *y luego, existen* σ_1, σ_2, σ_3 *monomorfismos de* $\mathbb{Q}(\alpha) \to \mathbb{C}$ *tales* $\sigma_1(\alpha) = \alpha$, $\sigma_2(\alpha) = \alpha\omega$ *y* $\sigma_3(\alpha) = \alpha\omega^2$.

$\mathbb{Q}(\alpha, \sqrt{3}i) = \mathbb{Q}(\alpha)(\sqrt{3}i)$ *es una extensión de grado* 2 *de* $\mathbb{Q}(\alpha)$. *En efecto,* $q(x) = x^2 + 3 \in \mathbb{Q}(\alpha)[x]$ *es el polinomio irreducible de* $\sqrt{3}i$ *sobre* $\mathbb{Q}(\alpha)$. *La raíces de* $q(x)$ *son* $\sqrt{3}i$ *y* $-\sqrt{3}i$.

Existen dos extensiones de $K \to \mathbb{C}$ *para cada* $\sigma_i : \mathbb{Q}(\alpha) \to \mathbb{C}$. *Como* K *es una extensión de Galois de* $\mathbb{Q}$, *entonces estas dos extensiones son automorfismos de* K. *Sean* τ_1, $\tau_2 : K \to K$ *las extensiones de* σ_1; τ_3, $\tau_4 : K \to K$ *las extensiones de* σ_2 *y* τ_5, $\tau_6 : K \to K$ *las extensiones de* σ_3, *tales que*

$$\begin{aligned}
&\tau_1(\sqrt{3}i) = \sqrt{3}i \text{ y } \tau_2(\sqrt{3}i) = -\sqrt{3}i \text{ y } \tau_1(\alpha) = \tau_2(\alpha) = \sigma_1(\alpha) = \alpha,\\
&\tau_3(\sqrt{3}i) = \sqrt{3}i \text{ y } \tau_4(\sqrt{3}i) = -\sqrt{3}i \text{ y } \tau_3(\alpha) = \tau_4(\alpha) = \sigma_2(\alpha) = \alpha\omega,\\
&\tau_5(\sqrt{3}i) = \sqrt{3}i \text{ y } \tau_6(\sqrt{3}i) = -\sqrt{3}i \text{ y } \tau_5(\alpha) = \tau_6(\alpha) = \sigma_3(\alpha) = \alpha\omega^2.
\end{aligned}$$

Observemos que

$$\tau_2(\omega) = \tau_2(-\frac{1}{2} + \frac{1}{2}\sqrt{3}i) = -\frac{1}{2} + \frac{1}{2}\tau_2(\sqrt{3}i) = -\frac{1}{2} - \frac{1}{2}\sqrt{3}i = \omega^2,$$

y que

$$\tau_2(\omega^2) = \tau_2(-\frac{1}{2} - \frac{1}{2}\sqrt{3}i) = -\frac{1}{2} - \frac{1}{2}\tau_2(\sqrt{3}i) = -\frac{1}{2} + \frac{1}{2}\sqrt{3}i = \omega.$$

En forma similar, obtenemos que $\tau_3(\omega) = \omega$, $\tau_3(\omega^2) = \omega^2$, $\tau_4(\omega) = \omega^2$, $\tau_4(\omega^2) = \omega$, $\tau_5(\omega) = \omega$, $\tau_5(\omega^2) = \omega^2$ *y* $\tau_6(\omega) = \omega^2$, $\tau_6(\omega^2) = \omega$. *Por la observación 5.1,* $G(K/\mathbb{Q}) = \{\tau_1, \tau_2, \tau_3, \tau_4, \tau_5, \tau_6\}$ *es isomorfo a un subgrupo de* S_3. *Pero* $G(K/\mathbb{Q})$ *tiene* 6 *elementos, luego* $G(K/\mathbb{Q})$ *es isomorfo a* S_3. *El grupo* S_3 *no es Abeliano y todos sus subgrupos propios son cíclicos.*

Encontraremos los subgrupos cíclicos de $G(K/\mathbb{Q})$. *Claramente* $\tau_2^2 = \tau_1$,

$$\begin{aligned}
&\tau_3^2(\alpha) = \tau_3(\alpha\omega) = \tau_3(\alpha)\tau_3(\omega) = \alpha\omega^2 \text{ y } \tau_3^2(\sqrt{3}i) = \sqrt{3}i,\\
&\tau_3^3(\alpha) = \tau_3(\tau_3^2(\alpha)) = \tau_3(\alpha\omega^2) = \alpha\omega^3 = \alpha \text{ y } \tau_3^3(\sqrt{3}i) = \sqrt{3}i,\\
&\tau_4^2(\alpha) = \tau_4(\alpha\omega) = \tau_4(\alpha)\tau_4(\omega) = \alpha \text{ y } \tau_4^2(\sqrt{3}i) = \sqrt{3}i,\\
&\tau_5^2(\alpha) = \tau_5(\alpha\omega^2) = \tau_5(\alpha)\tau_5(\omega^2) = \alpha\omega \text{ y } \tau_5^2(\sqrt{3}i) = \sqrt{3}i,\\
&\tau_5^3(\alpha) = \tau_5(\tau_5^2(\alpha)) = \tau_5(\alpha\omega) = \alpha\omega^3 = \alpha \text{ y } \tau_5^3(\sqrt{3}i) = \sqrt{3}i,\\
&\tau_6^2(\alpha) = \tau_6(\alpha\omega^2) = \tau_6(\alpha)\tau_6(\omega^2) = \alpha \text{ y } \tau_6^2(\sqrt{3}i) = \sqrt{3}i.
\end{aligned}$$

Por lo tanto, los subgrupos propios de $G(K/\mathbb{Q})$ *son* $H_0 = \{\tau_1\}$, $H_1 = \{\tau_1, \tau_2\}$, $H_2 = \{\tau_1, \tau_3, \tau_5\}$, $H_3 = \{\tau_1, \tau_4\}$ *y* $H_4 = \{\tau_1, \tau_6\}$.

Encontraremos los cuerpos fijos de cada subgrupo de $G(K/\mathbb{Q})$. *Sabemos que* $\{1, \alpha, \alpha^2, \sqrt{3}i, \alpha\sqrt{3}i, \alpha^2\sqrt{3}i\}$ *es una base de* K *como espacio vectorial sobre* $\mathbb{Q}$. *Claramente* $K^{H_0} = \{x \in K \ / \ \tau_1(x) = x\} = K$.

Encontraremos $K^{H_1} = \{x \in K \ / \ \tau_2(x) = x\}$. *Si*

$$\begin{aligned} \tau_2(b_0 + b_1\alpha + b_2\alpha^2 + b_3\sqrt{3}i \quad &+ \quad b_4\alpha\sqrt{3}i + b_5\alpha^2\sqrt{3}i) \\ &= \quad b_0 + b_1\alpha + b_2\alpha^2 + b_3\sqrt{3}i + b_4\alpha\sqrt{3}i + b_5\alpha^2\sqrt{3}i, \end{aligned}$$

entonces

$$\begin{aligned} b_0 + b_1\alpha + b_2\alpha^2 - b_3\sqrt{3}i \quad &- \quad b_4\alpha\sqrt{3}i - b_5\alpha^2\sqrt{3}i \\ &= \quad b_0 + b_1\alpha + b_2\alpha^2 + b_3\sqrt{3}i + b_4\alpha\sqrt{3}i + b_5\alpha^2\sqrt{3}i. \end{aligned}$$

Dado que $\{1, \alpha, \alpha^2, \sqrt{3}i, \alpha\sqrt{3}i, \alpha^2\sqrt{3}i\}$ *es una base de* K *como espacio vectorial sobre* $\mathbb{Q}$, *obtenemos que* $b_3 = b_4 = b_5 = 0$. *Así,*

$$K^{H_1} = \{b_0 + b_1\alpha + b_2\alpha^2 \ / \ b_0, b_1, b_2 \in \mathbb{Q}\} = \mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt[3]{2}).$$

Encontraremos $K^{H_2} = \{x \in K \ / \ \tau_3(x) = x \wedge \tau_5(x) = x\}$. *Si*

$$\begin{aligned} \tau_3(b_0 + b_1\alpha + b_2\alpha^2 + b_3\sqrt{3}i \quad &+ \quad b_4\alpha\sqrt{3}i + b_5\alpha^2\sqrt{3}i) \\ &= \quad b_0 + b_1\alpha + b_2\alpha^2 + b_3\sqrt{3}i + b_4\alpha\sqrt{3}i + b_5\alpha^2\sqrt{3}i, \end{aligned}$$

entonces

$$\begin{aligned} b_0 + b_1\alpha\omega + b_2\alpha^2\omega^2 + b_3\sqrt{3}i \quad &+ \quad b_4\alpha\omega\sqrt{3}i + b_5\alpha^2\omega^2\sqrt{3}i \\ &= \quad b_0 + b_1\alpha + b_2\alpha^2 + b_3\sqrt{3}i + b_4\alpha\sqrt{3}i + b_5\alpha^2\sqrt{3}i. \end{aligned}$$

Reemplazando ω *por* $-\frac{1}{2} + \frac{1}{2}\sqrt{3}i$, *obtenemos que* $b_2 = b_5$, $b_1 + b_4 = 0$, $b_1 = 3b_4$, $b_2 = 3b_5$ *y así,* $b_2 = b_5 = b_1 = b_4 = 0$. *Dado que* $\tau_5(b_0 + b_3\sqrt{3}i) = b_0 + b_3\sqrt{3}i$, *concluimos que*

$$K^{H_2} = \{b_0 + b_3\sqrt{3}i \ / \ b_0, b_3 \in \mathbb{Q}\} = \mathbb{Q}(\sqrt{3}i).$$

En forma similar, obtenemos que

$$\begin{aligned} K^{H_3} &= \{b_0 + b_1(\alpha + \alpha\sqrt{3}i) + b_2(\alpha^2 - \alpha^2\sqrt{3}i) \ / \ b_0, b_1, b_2 \in \mathbb{Q}\} \\ &= \mathbb{Q}(\alpha + \alpha\sqrt{3}i) = \mathbb{Q}(\sqrt[3]{2}(1 + \sqrt{3}i)). \end{aligned}$$

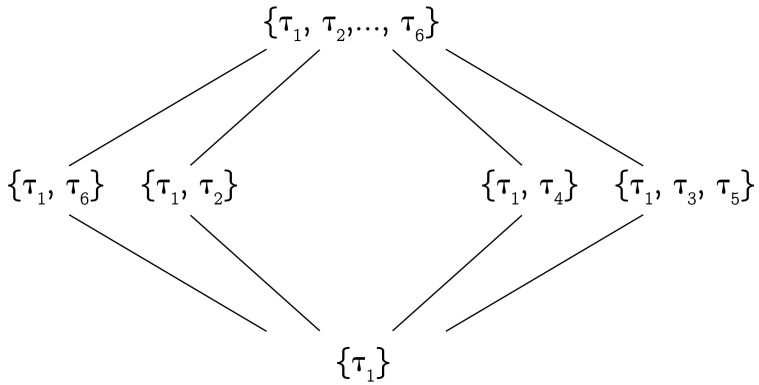
Notar que $q(x) = x^3 + 16 \in \mathbb{Q}[x]$ *es el polinomio irreducible de* $\sqrt[3]{2}(1 + \sqrt{3}i)$ *sobre* $\mathbb{Q}$. *Así,* $[\mathbb{Q}(\sqrt[3]{2}(1 + \sqrt{3}i)) : \mathbb{Q}] = 3$.

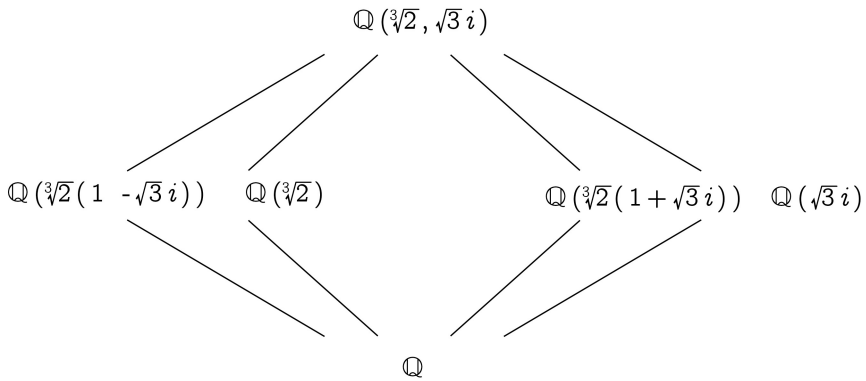
$$\begin{aligned} K^{H_4} &= \{b_0 + b_1(\alpha - \alpha\sqrt{3}i) + b_2(\alpha^2 + \alpha^2\sqrt{3}i) \ / \ b_0, b_1, b_2 \in \mathbb{Q}\} \\ &= \mathbb{Q}(\alpha - \alpha\sqrt{3}i)) = \mathbb{Q}(\sqrt[3]{2}(1 - \sqrt{3}i)). \end{aligned}$$

El polinomio irreducible de $\sqrt[3]{2}(1-\sqrt{3}i)$*sobre* $\mathbb{Q}$ *es* $q(x) = x^3 + 16 \in \mathbb{Q}[x]$. *De esta forma, la correspondencia biyectiva es*

$$\begin{aligned}
\mathbb{Q} &\rightarrow G(\mathbb{Q}(\sqrt[3]{2}, \sqrt{3}i)/\mathbb{Q}) = \{\tau_1, \tau_2, \tau_3, \tau_4, \tau_5, \tau_6\},\\
\mathbb{Q}(\sqrt{3}i) &\rightarrow H_2 = \{\tau_1, \tau_3, \tau_5\},\\
\mathbb{Q}(\sqrt[3]{2}) &\rightarrow H_1 = \{\tau_1, \tau_2\},\\
\mathbb{Q}(\sqrt[3]{2}(1+\sqrt{3}i)) &\rightarrow H_3 = \{\tau_1, \tau_4\},\\
\mathbb{Q}(\sqrt[3]{2}(1-\sqrt{3}i)) &\rightarrow H_4 = \{\tau_1, \tau_6\},\\
\mathbb{Q}(\sqrt[3]{2}, \sqrt{3}i) &\rightarrow H_0 = \{\tau_1\}.
\end{aligned}$$

Representamos la correspondencia biyectiva con los siguientes diagramas:





Ejemplo 5.15. *Consideremos el polinomio* $f(x) = x^4 - 3 \in \mathbb{Q}[x]$. *Por el criterio de Schöneman-Eisenstein, el polinomio* $f(x)$ *es irreducible en* $\mathbb{Q}[x]$ *y las raíces en* $\mathbb{C}$ *de*

$f(x)$ *son* $\sqrt[4]{3}$, $-\sqrt[4]{3}$, $\sqrt[4]{3}i$, $-\sqrt[4]{3}i$. *Si* $\alpha = \sqrt[4]{3}$, *entonces el cuerpo de descomposición de* $f(x)$ *es* $K = \mathbb{Q}(\alpha, -\alpha, \alpha i, -\alpha i) = \mathbb{Q}(\alpha, \alpha i) = \mathbb{Q}(\alpha)(\alpha i) = \mathbb{Q}(\alpha)(i) = \mathbb{Q}(\alpha, i)$.

Encontraremos los elementos del grupo de Galois $G(K/\mathbb{Q})$ *y la correspondencia biyectiva entre los subcuerpos de* K *y los subgrupos de* $G(K/\mathbb{Q})$ *(Notemos que cualquier subcuerpo de* K *contiene a* $\mathbb{Q}$*). Como* $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$, *entonces existen* 4 *monomorfismos,* σ_1, σ_2, σ_3, σ_4 *de* $\mathbb{Q}(\alpha)$ *en* $\mathbb{C}$ *tales que* $\sigma_1(\alpha) = \alpha$, $\sigma_2(\alpha) = -\alpha$, $\sigma_3(\alpha) = \alpha i$ *y* $\sigma_4(\alpha) = -\alpha i$. *Dado que* $[\mathbb{Q}(\alpha)(i) : \mathbb{Q}(\alpha)] = 2$, *entonces cada monomorfismo* $\sigma_i : \mathbb{Q}(\alpha) \to \mathbb{C}$ *da origen a dos automorfismos de* $\mathbb{Q}(\alpha)(i)$. *Si* τ_1, $\tau_2, \ldots, \tau_8$ *son los automorfismos de* $\mathbb{Q}(\alpha)(i)$, *entonces*

$\tau_1(\alpha) = \alpha$ *y* $\tau_1(i) = i$, $\tau_2(\alpha) = \alpha$ *y* $\tau_2(i) = -i$, $\tau_3(\alpha) = -\alpha$ *y* $\tau_3(i) = i$,
$\tau_4(\alpha) = -\alpha$ *y* $\tau_4(i) = -i$, $\tau_5(\alpha) = \alpha i$ *y* $\tau_5(i) = i$, $\tau_6(\alpha) = \alpha i$ *y* $\tau_6(i) = -i$,
$\tau_7(\alpha) = -\alpha i$ *y* $\tau_7(i) = i$, $\tau_8(\alpha) = -\alpha i$ *y* $\tau_8(i) = -i$.

Por lo tanto, el grupo de Galois de $f(x)$ *es*

$$G(\mathbb{Q}(\alpha, i)/\mathbb{Q}) = \{\tau_1, \tau_2, \tau_3, \ldots, \tau_8\}$$

y su tabla de multiplicación es:

$\circ$	τ_1	τ_2	τ_3	τ_4	τ_5	τ_6	τ_7	τ_8
τ_1	τ_1	τ_2	τ_3	τ_4	τ_5	τ_6	τ_7	τ_8
τ_2	τ_2	τ_1	τ_4	τ_3	τ_8	τ_7	τ_6	τ_5
τ_3	τ_3	τ_4	τ_1	τ_2	τ_7	τ_8	τ_5	τ_6
τ_4	τ_4	τ_3	τ_2	τ_1	τ_6	τ_5	τ_8	τ_7
τ_5	τ_5	τ_6	τ_7	τ_8	τ_3	τ_4	τ_1	τ_2
τ_6	τ_6	τ_5	τ_8	τ_7	τ_2	τ_1	τ_4	τ_3
τ_7	τ_7	τ_8	τ_5	τ_6	τ_1	τ_2	τ_3	τ_4
τ_8	τ_8	τ_7	τ_6	τ_5	τ_4	τ_3	τ_2	τ_1

Los subgrupos cíclicos de $G(\mathbb{Q}(\alpha, i)/\mathbb{Q})$ *son*

$\langle\tau_1\rangle = \{\tau_1\}$, $\langle\tau_2\rangle = \{\tau_1, \tau_2\}$, $\langle\tau_3\rangle = \{\tau_1, \tau_3\}$, $\langle\tau_4\rangle = \{\tau_1, \tau_4\}$,
$\langle\tau_5\rangle = \{\tau_1, \tau_5, \tau_3, \tau_7\}$, $\langle\tau_6\rangle = \{\tau_1, \tau_6\}$, $\langle\tau_7\rangle = \langle\tau_5\rangle$, $\langle\tau_8\rangle = \{\tau_1, \tau_8\}$.

Existen otros subgrupos de $G(\mathbb{Q}(\alpha, i)/\mathbb{Q})$ *que no son cíclicos y son los que siguen*
$\{\tau_1, \tau_2, \tau_3, \tau_4\}$ *y* $\{\tau_1, \tau_3, \tau_6, \tau_8\}$.

Encontraremos los cuerpos fijos de cada subgrupo de $G(K/\mathbb{Q})$. *Sabemos que*

$$\{1, \alpha, \alpha^2, \alpha^3, i, \alpha i, \alpha^2 i, \alpha^3 i\}$$

es una base de K *como espacio vectorial sobre* $\mathbb{Q}$.

Encontraremos $K^{\{\tau_1,\tau_3\}} = \{x \in K \ / \ \tau_3(x) = x\}$. *Si*

$$\begin{aligned}&\tau_3(a_0 + a_1\alpha + a_2\alpha^2 + a_3\alpha^3 + a_4 i + a_5\alpha i + a_6\alpha^2 i + a_7\alpha^3 i)\\ &= a_0 + a_1\alpha + a_2\alpha^2 + a_3\alpha^3 + a_4 i + a_5\alpha i + a_6\alpha^2 i + a_7\alpha^3 i,\end{aligned}$$

entonces

$$\begin{aligned}&a_0 - a_1\alpha + a_2\alpha^2 - a_3\alpha^3 + a_4 i - a_5\alpha i + a_6\alpha^2 i - a_7\alpha^3 i\\ &= a_0 + a_1\alpha + a_2\alpha^2 + a_3\alpha^3 + a_4 i + a_5\alpha i + a_6\alpha^2 i + a_7\alpha^3 i,\end{aligned}$$

de donde

$$K^{\{\tau_1,\tau_3\}} = \{a_0 + a_2\alpha^2 + a_4 i + a_6\alpha^2 i \,/\, a_0, a_2, a_4, a_6 \in \mathbb{Q}\} = \mathbb{Q}(\sqrt[4]{9}, i) = \mathbb{Q}(\sqrt{3}, i).$$

Encontraremos $K^{\{\tau_1,\tau_3,\tau_6,\tau_8\}} = \{x \in K \ / \ \tau_3(x) = x \wedge \tau_6(x) = x \wedge \tau_8(x) = x\}$. *Sabemos que*

$$\tau_3(a_0 + a_2\alpha^2 + a_4 i + a_6\alpha^2 i) = a_0 + a_2\alpha^2 + a_4 i + a_6\alpha^2 i.$$

Ahora,

$$\tau_6(a_0 + a_2\alpha^2 + a_4 i + a_6\alpha^2 i) = a_0 + a_2\alpha^2 + a_4 i + a_6\alpha^2 i$$

implica que

$$a_0 - a_2\alpha^2 - a_4 i + a_6\alpha^2 i = a_0 + a_2\alpha^2 + a_4 i + a_6\alpha^2 i.$$

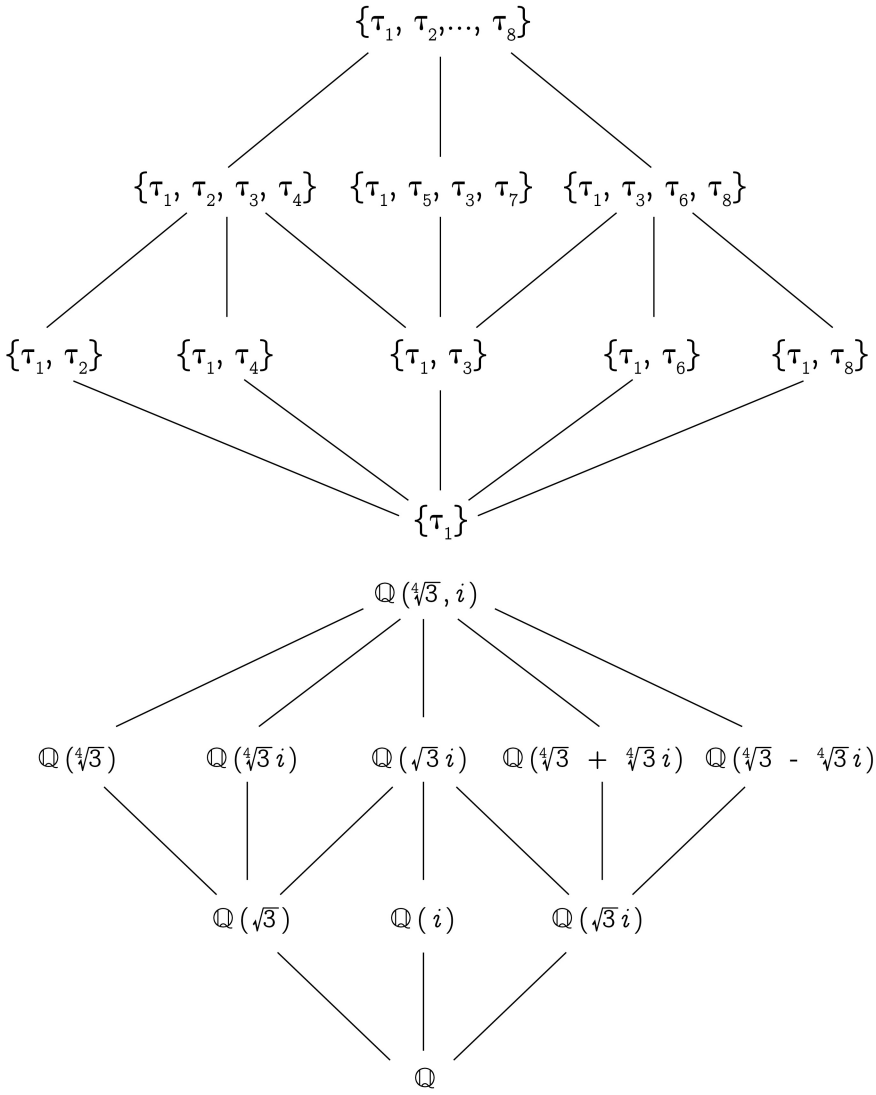
Luego, $\tau_6(a_0 + a_6\alpha^2 i) = a_0 + a_6\alpha^2 i$. *Como* $\tau_8(a_0 + a_6\alpha^2 i) = a_0 + a_6\alpha^2 i$, *entonces*

$$K^{\{\tau_1,\tau_3,\tau_6,\tau_8\}} = \{a_0 + a_6\alpha^2 i \,/\, a_0, a_6 \in \mathbb{Q}\} = \mathbb{Q}(\sqrt[4]{9}i) = \mathbb{Q}(\sqrt{3}i).$$

En forma similar se encuentran los cuerpos fijos restantes correspondientes a cada subgrupo de $G(K/\mathbb{Q})$. *Se obtienen* $K^{\{\tau_1,\tau_2\}} = \mathbb{Q}(\sqrt[4]{3})$, $K^{\{\tau_1,\tau_4\}} = \mathbb{Q}(\sqrt[4]{3}i)$, $K^{\{\tau_1,\tau_6\}} = \mathbb{Q}(\sqrt[4]{3} + \sqrt[4]{3}i)$, $K^{\{\tau_1,\tau_8\}} = \mathbb{Q}(\sqrt[4]{3} - \sqrt[4]{3}i)$, $K^{\{\tau_1,\tau_2,\tau_3,\tau_4\}} = \mathbb{Q}(\sqrt{3})$, $K^{\{\tau_1,\tau_5,\tau_3,\tau_7\}} = \mathbb{Q}(i)$. *De esta forma, la correspondencia biyectiva es*

$$\begin{aligned}\mathbb{Q} &\rightarrow G(\mathbb{Q}(\sqrt[4]{3}, i)/\mathbb{Q}) = \{\tau_1, \tau_2, \tau_3, \tau_4, \tau_5, \tau_6, \tau_7, \tau_8\},\\ \mathbb{Q}(\sqrt{3}, i) &\rightarrow \{\tau_1, \tau_3\},\\ \mathbb{Q}(\sqrt[4]{3}) &\rightarrow \{\tau_1, \tau_2\},\\ \mathbb{Q}(\sqrt[4]{3}i) &\rightarrow \{\tau_1, \tau_4\},\\ \mathbb{Q}(\sqrt[4]{3} + \sqrt[4]{3}i) &\rightarrow \{\tau_1, \tau_6\},\\ \mathbb{Q}(\sqrt[4]{3} - \sqrt[4]{3}i) &\rightarrow \{\tau_1, \tau_8\},\\ \mathbb{Q}(\sqrt{3}) &\rightarrow \{\tau_1, \tau_2, \tau_3, \tau_4\},\\ \mathbb{Q}(i) &\rightarrow \{\tau_1, \tau_5, \tau_3, \tau_7\},\\ \mathbb{Q}(\sqrt{3}i) &\rightarrow \{\tau_1, \tau_3, \tau_6, \tau_8\}.\end{aligned}$$

La correspondencia biyectiva está representada por los siguientes diagramas:



Ejercicios 5.5.

1. Demostrar que el polinomio $p(x) = x^4 + 1 \in \mathbb{Q}[x]$ es irreducible en $\mathbb{Q}[x]$. Encontrar el cuerpo de descomposición K de $p(x)$ y el grupo de Galois $G(K/\mathbb{Q})$. Encontrar la correspondencia biyectiva entre los subgrupos de $G(K/\mathbb{Q})$ y los subcuerpos de K.

2. Sea F un cuerpo y $p(x) = x^2 + bx + c \in F[x]$ irreducible en $F[x]$. Si K es el cuerpo de descomposición de $p(x)$, demostrar que el grupo de Galois $G(K/F)$ tiene 2 elementos.
3. Encontrar el cuerpo de descomposición K del polinomio $f(x) = x^4 - 4x^2 - 1 \in \mathbb{Q}[x]$. Encontrar el grupo de Galois $G(K/\mathbb{Q})$ de $f(x)$ y la correspondencia biyectiva entre los subgrupos de $G(K/\mathbb{Q})$ y los subcuerpos de K.

5.5 El Grupo de Galois de un Polinomio de Grado 3

Estudiaremos a continuación el grupo de Galois de un polinomio de grado 3 sobre un cuerpo F. Sea $f(x) = x^3 + ax^2 + bx + c \in F[x]$. El lector puede verificar que

$$f(x) = (x + \frac{1}{3}a)^3 + (b - \frac{1}{3}a^2)(x + \frac{1}{3}a) + c - \frac{1}{3}ab + \frac{2}{27}a^3.$$

Sea $y = x + \frac{1}{3}a$ y consideremos el polinomio

$$g(y) = y^3 + (b - \frac{1}{3}a^2)y + c - \frac{1}{3}ab + \frac{2}{27}a^3.$$

Ahora, si $\beta \in \mathbb{C}$ es una raíz de $f(x)$, entonces $\beta + \frac{1}{3}a$ es una raíz de $g(y)$. En efecto, $g(\beta + \frac{1}{3}a) = (\beta + \frac{1}{3}a)^3 + (b - \frac{1}{3}a^2)(\beta + \frac{1}{3}a) + c - \frac{1}{3}ab + \frac{2}{27}a^3 = c + b\beta + \beta^3 + a\beta^2 = 0$. Además, si $\gamma \in \mathbb{C}$ es una raíz de $g(y)$, entonces $\gamma - \frac{1}{3}a$ es una raíz de $f(x)$. Por lo tanto, obtenemos el siguiente resultado:

Lema 5.4. *Sea F un cuerpo. Entonces los polinomios $f(x) = x^3 + ax^2 + bx + c \in F[x]$ y $g(x) = x^3 + (b - \frac{1}{3}a^2)x + c - \frac{1}{3}ab + \frac{2}{27}a^3 \in F[x]$ tienen el mismo cuerpo de descomposición.*

Luego, para saber cuál es el grupo de Galois que le corresponde a un polinomio de grado 3 sobre un cuerpo F, basta estudiar polinomios de la forma $f(x) = x^3 + bx + c \in F[x]$.

Sea $p(x) = x^3 + bx + c \in F[x]$ irreducible en $F[x]$ y α, β, $\gamma \in \mathbb{C}$ las raíces de $p(x)$. De la relación existente entre las raíces de $p(x)$ y sus coeficientes obtenemos

$$\alpha + \beta + \gamma = 0,\ \alpha\beta + \alpha\gamma + \beta\gamma = b \text{ y } \alpha\beta\gamma = -c.$$

Sea

$$\delta = (\alpha - \beta)(\alpha - \gamma)(\beta - \gamma).$$

El lector puede verificar que

$$\delta^2 = -4b^3 - 27c^2.$$

Luego, $\delta^2 \in F$. Reemplazando $\gamma = -\alpha - \beta$ en $\delta = (\alpha - \beta)(\alpha - \gamma)(\beta - \gamma)$ y en $\alpha\beta + \alpha\gamma + \beta\gamma = b$, respectivamente, obtenemos que $\delta = (\alpha - \beta)(5\alpha\beta + 2\alpha^2 + 2\beta^2)$ y $\alpha\beta + \alpha^2 + \beta^2 = -b$. De estas últimas dos relaciones $\delta = (\alpha - \beta)(5\alpha\beta + 2(-b - \alpha\beta)) = 2b\beta - 2b\alpha - 3\alpha\beta^2 + 3\alpha^2\beta$.

Dado que $\alpha\beta\gamma = \alpha\beta(-\alpha - \beta) = -c$, entonces $\alpha\beta^2 = c - \alpha^2\beta$. Por lo tanto, $\delta = 2b\beta - 2b\alpha - 3(c - \alpha^2\beta) + 3\alpha^2\beta = 2b\beta - 2b\alpha - 3c + 6\alpha^2\beta$. Así, $\beta(6\alpha^2 + 2b) = \delta + 2b\alpha + 3c$.

Notemos que $6\alpha^2 + 2b \neq 0$, de lo contrario $p(x)$ no sería el polinomio irreducible de α sobre F. Concluimos que $\beta = \frac{\delta+2b\alpha+3c}{6\alpha^2+2b}$, de donde $\beta \in F(\delta, \alpha)$.

Del estudio anterior obtenemos el siguiente teorema:

Teorema 5.8. *Sea F un cuerpo y $p(x) = x^3 + bx + c \in F[x]$ irreducible en $F[x]$. Entonces $K = F(\delta_0, \alpha)$ es el cuerpo de descomposición de $p(x)$, donde $\delta_0 \in \mathbb{C}$ es una raíz del polinomio $q(x) = x^2 + 4b^3 + 27c^2$ y $\alpha \in \mathbb{C}$ es una raíz de $p(x)$.*

Demostración. Sean $\alpha, \beta, \gamma \in \mathbb{C}$ las raíces de $p(x)$, entonces el cuerpo de descomposición de $p(x)$ es $K = F(\alpha, \beta, \gamma)$. Por lo demostrado anteriormente $\beta \in F(\delta, \alpha)$, donde $\delta = (\alpha - \beta)(\alpha - \gamma)(\beta - \gamma)$. Como $\alpha + \beta + \gamma = 0$, entonces $\gamma \in F(\delta, \alpha)$. Claramente $K = F(\alpha, \beta, \gamma) = F(\delta, \alpha)$. Como δ es una raíz de $q(x)$, entonces $\delta_0 = \delta$ ó $\delta_0 = -\delta$. Concluimos que, $K = F(\delta_0, \alpha)$. □

Corolario 5.5. *Sea F un cuerpo, $p(x) = x^3 + bx + c \in F[x]$ irreducible en $F[x]$ y K el cuerpo de descomposición de $p(x)$.*

a) Si $-4b^3 - 27c^2$ es un cuadrado en F, entonces $G(K/F)$ es un grupo de orden 3. Es decir, isomorfo a $(\mathbb{Z}_3, +)$.

b) Si $-4b^3 - 27c^2$ no es un cuadrado en F, entonces $G(K/F)$ es un grupo isomorfo a S_3.

Demostración.

a) Si $-4b^3 - 27c^2$ es un cuadrado en F, entonces existe $\delta_0 \in F$ una raíz de $q(x) = x^2 + 4b^3 + 27c^2$. Si $\alpha \in \mathbb{C}$ es una raíz de $p(x)$, entonces por el Teorema 5.8, $K = F(\delta_0, \alpha) = F(\alpha)$. Dado que $[F(\alpha) : F] = 3$, obtenemos que $G(K/F)$ es un grupo de orden 3.

b) Si $-4b^3 - 27c^2$ no es un cuadrado en F, entonces el polinomio $q(x) = x^2 + 4b^3 + 27c^2$ no tiene raíces en F y por lo tanto, es irreducible en $F[x]$. Como $\delta = (\alpha - \beta)(\alpha - \gamma)(\beta - \gamma)$ es una raíz de $q(x)$, entonces $q(x)$ es el polinomio irreducible de δ sobre F. Si $\alpha \in \mathbb{C}$ es una raíz de $p(x)$, por el Teorema 5.8, $K = F(\delta, \alpha)$. Dado que $[F(\delta) : F] = 2$ y $[F(\alpha) : F] = 3$ son divisores de $[K : F]$, entonces 6 es un divisor de $[K : F]$. De la observación 5.1, $[K : F] = 6$. Por lo tanto, $G(K/F)$ es un grupo isomorfo a S_3. □

Ejemplo 5.16. *Encontraremos el grupo de Galois del polinomio $p(x) = x^3 - 3x + 1 \in \mathbb{Q}[x]$. Como $p(1) \neq 0$, $p(-1) \neq 0$ y $gr(p) = 3$, entonces $p(x)$ es irreducible en $\mathbb{Q}[x]$. Dado que $-4b^3 - 27c^2 = (-4)(-3)^3 - 27 = 9^2$, entonces el grupo de Galois de $p(x)$ es un grupo de orden 3.*

Ejemplo 5.17. *Encontraremos el grupo de Galois del polinomio $p(x) = x^3 + 3 \in \mathbb{Q}[x]$. Claramente $p(x)$ es irreducible en $\mathbb{Q}[x]$. Ahora, $-4b^3 - 27c^2 = -3^5$ no es un cuadrado en $\mathbb{Q}$. Por lo tanto, el grupo de Galois de $p(x)$ es isomorfo a S_3.*

Ejemplo 5.18. *Encontraremos el grupo de Galois del polinomio $p(x) = x^3 - x - 1 \in \mathbb{Q}(\sqrt{23}i)[x]$. Determinaremos, si $p(x)$ es irreducible o reducible en $\mathbb{Q}(\sqrt{23}i)[x]$. Supongamos que $p(x)$ tiene una raíz en el cuerpo*

$$\mathbb{Q}(\sqrt{23}i) = \{a + b\sqrt{23}i \,/\, a, b \in \mathbb{Q}\}.$$

Entonces, existen $a, b \in \mathbb{Q}$ *tal que* $a + b\sqrt{23}i$ *es una raíz de* $p(x)$. *Luego,*

$$a^3 - a - 69ab^2 - 1 + b(3a^2 - 1 - 23b^2)\sqrt{23}i,$$

de donde $a^3 - a - 69ab^2 - 1 = 0$ *y* $b(3a^2 - 1 - 23b^2) = 0$. *Así,* $b = 0$ *ó* $3a^2 - 1 - 23b^2 = 0$. *Si* $b = 0$, *entonces* $p(x)$ *tiene una raíz en* $\mathbb{Q}$, *lo que es una contradicción. Si* $3a^2 - 1 - 23b^2 = 0$, *entonces de* $a^3 - a - 69ab^2 - 1 = 0$ *obtenemos que* $8a^3 - 2a + 1 = 0$, *lo cual implica que el polinomio* $8x^3 - 2x + 1$ *tiene una raíz en* $\mathbb{Q}$. *Es fácil verificar que dicho polinomio no tiene raíces en* $\mathbb{Q}$. *Hemos demostrado que* $p(x)$ *es irreducible en* $\mathbb{Q}(\sqrt{23}i)[x]$. *Ahora,*

$$-4b^3 - 27c^2 = -4(-1)^3 - 27(-1)^2 = -23$$

es un cuadrado en $\mathbb{Q}(\sqrt{23}i)$. *Por lo tanto, el grupo de Galois de* $p(x)$ *es un grupo de orden* 3.

Ejercicios 5.6.

1. Determinar el grupo de Galois de los siguientes polinomios sobre $\mathbb{Q}$.
   a) $x^3 - 5x + 7$ *b)* $x^3 + 2x + 2$ *c)* $x^3 + 5$

2. Determinar el grupo de Galois de
   a) $x^3 - 10$ sobre $\mathbb{Q}(\sqrt{2})$ *b)* $x^3 - 10$ sobre $\mathbb{Q}(\sqrt{3}i)$
   c) $x^3 + 2$ sobre $\mathbb{Q}(\sqrt{3}i)$ *d)* $x^3 - 9$ sobre $\mathbb{Q}(\sqrt{3}i)$
   e) $x^3 + 3x^2 + x + 1$ sobre $\mathbb{Q}$.

5.6 El Grupo de Galois del Polinomio $x^n - 1$

Encontraremos resultados sobre la estructura que tiene el grupo de Galois del polinomio $f(x) = x^n - 1$ sobre $\mathbb{Q}$. Demostraremos que dicho grupo es Abeliano. En el caso que $n = p$ es un número primo, probaremos que es un grupo cíclico. Como una aplicación de estos resultados, demostraremos que un polígono regular de n lados es constructible, si y solo si, $\cos(\frac{2\pi}{n})$ es un real constructible.

Definición 5.6. *Un número complejo* ω *se dice que es una* ***raíz primitiva n-ésima de la unidad****, si* $\omega^n = 1$, *pero* $\omega^m \neq 1$ *para cualquier entero positivo* $m < n$.

Observación 5.3. *Si* ω *es una raíz primitiva n-ésima de la unidad, entonces* ω, $\omega^2, \ldots, \omega^{n-1}$, $\omega^n = 1$ *son todos distintos. En efecto, si suponemos que existen* p, $q \in \mathbb{Z}$ *tales que* $\omega^p = \omega^q$ *con* $1 \leq p < q \leq n$, *entonces* $\omega^{q-p} = 1$ *con* $1 \leq q - p < n$, *lo que es una contradicción. Por lo tanto,* $x^n - 1 = (x - 1)(x - \omega) \cdots (x - \omega^{n-1})$.

Observación 5.4. *En los cursos básicos de álgebra se estudia que* $\omega = \cos(\frac{2\pi}{n}) + isen(\frac{2\pi}{n})$ *es una raíz n-ésima primitiva de la unidad.*

Es fácil demostrar que el conjunto $\mathbb{C}_n = \{\alpha \in \mathbb{C} \ / \ \alpha^n = 1\}$ *es un grupo con el producto usual de* $\mathbb{C}$. *Además,* $\mathbb{C}_n$ *es un grupo cíclico dado que* $\omega = \cos(\frac{2\pi}{n}) + isen(\frac{2\pi}{n})$ *es un generador de* $\mathbb{C}_n$. *De la teoría de grupos, sabemos que si* m *es un entero primo*

relativo con n, entonces ω^m también es un generador del grupo $\mathbb{C}_n$. Además, $\mathbb{C}_n$ tiene $\varphi(n)$ generadores, siendo $\varphi : \mathbb{Z}^+ \to \mathbb{Z}^+$ la función definida por $\varphi(n) = s$, donde s es el número de enteros positivos menores o iguales a n y primos relativos con n. Dicha función es conocida como la función φ de Euler. Concluimos que existen $\varphi(n)$ raíces primitivas n-ésimas de la unidad.

De la observación anterior obtenemos que

Lema 5.5. *Si ω es una raíz primitiva n-ésima de la unidad, entonces se tiene que $\mathbb{Q}(1, \omega, \ldots, \omega^{n-1}) = \mathbb{Q}(\omega)$ es el cuerpo de descomposición del polinomio $f(x) = x^n - 1$ sobre $\mathbb{Q}$. Por lo tanto, $\mathbb{Q}(\omega)$ es una extensión de Galois de $\mathbb{Q}$.*

Definición 5.7. *El polinomio $\phi_n(x) = (x - \omega_1)(x - \omega_2)\cdots(x - \omega_{\varphi(n)})$, donde ω_1, $\omega_2, \ldots, \omega_{\varphi(n)}$ son las raíces primitivas n-ésimas de la unidad, se llama el n-ésimo* ***polinomio ciclotómico****.*

Si el lector desea conocer la demostración del resultado que sigue, puede consultar [11] de la bibliografía.

Teorema 5.9. *El n-ésimo polinomio ciclotómico $\phi_n(x)$ es un elemento en $\mathbb{Q}[x]$ e irreducible sobre $\mathbb{Q}$.*

Corolario 5.6. *El grupo de Galois del polinomio $f(x) = x^n - 1$ sobre $\mathbb{Q}$ tiene $\varphi(n)$ elementos.*

Demostración. Si ω es una raíz primitiva n-ésima de la unidad, del Lema 5.5, $K = \mathbb{Q}(\omega)$ es una extensión de Galois de $\mathbb{Q}$. De acuerdo al Teorema 5.9, $\phi_n(x)$ es el polinomio irreducible de ω sobre $\mathbb{Q}$. Por lo tanto, el grupo de Galois $G(K/\mathbb{Q})$ tiene $gr(\phi_n) = \varphi(n)$ elementos. □

Ejemplo 5.19. *Encontraremos el grupo de Galois del polinomio $f(x) = x^{12} - 1$ sobre $\mathbb{Q}$. De la observación 5.4, $\omega = \cos(\frac{\pi}{6}) + isen(\frac{\pi}{6}) = \frac{1}{2}\sqrt{3} + \frac{1}{2}i$ es un generador del grupo $\mathbb{C}_{12} = \{\alpha \in \mathbb{C} \ / \ \alpha^{12} = 1\}$. Además, $\omega^5 = -\frac{1}{2}\sqrt{3} + \frac{1}{2}i$, $\omega^7 = -\frac{1}{2}\sqrt{3} - \frac{1}{2}i$ y $\omega^{11} = \frac{1}{2}\sqrt{3} - \frac{1}{2}i$ son los otros generadores de $\mathbb{C}_{12}$. El cuerpo de descomposición de $f(x)$ es $\mathbb{Q}(\omega)$ y*

$$\phi_{12}(x) = (x - \omega)(x - \omega^5)(x - \omega^7)(x - \omega^{11}) = x^4 - x^2 + 1$$

es el polinomio irreducible de ω sobre $\mathbb{Q}$. El grupo de Galois del polinomio $f(x) = x^{12} - 1$ sobre $\mathbb{Q}$ es $G(\mathbb{Q}(\omega)/\mathbb{Q}) = \{\tau_1, \tau_2, \tau_3, \tau_4\}$, donde $\tau_1(\omega) = \omega$, $\tau_2(\omega) = \omega^{11}$, $\tau_3(\omega) = \omega^5$ y $\tau_4(\omega) = \omega^7$. Ahora,

$$\tau_2^2(\omega) = \tau_2(\tau_2(\omega)) = \tau_2(\omega^{11}) = (\tau_2(\omega))^{11} = (\omega^{11})^{11} = \omega^{121} = \omega^{120}\omega = \omega.$$

Así, $\tau_2^2 = \tau_1$. En forma similar se obtienen los otros productos obteniéndose la tabla

$\circ$	τ_1	τ_2	τ_3	τ_4
τ_1	τ_1	τ_2	τ_3	τ_4
τ_2	τ_2	τ_1	τ_4	τ_3
τ_3	τ_3	τ_4	τ_1	τ_2
τ_4	τ_4	τ_3	τ_2	τ_1

Ejercicios 5.7.

1. Encontrar el grupo de Galois del polinomio $f(x) = x^8 - 1$ sobre $\mathbb{Q}$.
2. Encontrar el grupo de Galois del polinomio $f(x) = x^7 - 1$ sobre $\mathbb{Q}$.
   Demostrar que dicho grupo de Galois es cíclico exhibiendo un generador.

El conjunto $U_n = \{\overline{k} \in \mathbb{Z}_n \ / \ (k, n) = 1\}$ con la multiplicación módulo n, es un grupo Abeliano con $\varphi(n)$ elementos. Este resultado de teoría de grupos será utilizado en la demostración del teorema que sigue.

Teorema 5.10. *El grupo de Galois del polinomio $f(x) = x^n - 1$ sobre $\mathbb{Q}$ es isomorfo a U_n. Luego, el grupo de Galois es Abeliano.*

Demostración. Sea ω una raíz primitiva de la unidad. Entonces, $K = \mathbb{Q}(\omega)$ es el cuerpo de descomposición de $f(x)$ y $[\mathbb{Q}(\omega) : \mathbb{Q}] = \varphi(n)$. Si σ es un elemento en el grupo de Galois $G(K/\mathbb{Q})$, entonces $\sigma(\omega)$ es una raíz del n-ésimo polinomio ciclotómico $\phi_n(x)$ y por lo tanto, existe un entero positivo k tal que $\sigma(\omega) = \omega^k$ con $(k, n) = 1$. Observemos que, si $k \equiv s \ (mód \ n)$, entonces existe $q \in \mathbb{Z}$ tal que $k = s + nq$. Luego, $\sigma(\omega) = \omega^k = \omega^{s+nq} = \omega^s(\omega^n)^q = \omega^s$.

Definamos una función $\Psi : G(K/\mathbb{Q}) \to U_n$ por $\Psi(\sigma) = \overline{k}$. Sean σ, τ elementos en $G(K/\mathbb{Q})$. Existen enteros k, r tales que $\sigma(\omega) = \omega^k$ y $\tau(\omega) = \omega^r$ con $(k, n) = 1$ y $(r, n) = 1$.

Demostraremos que Ψ es un homomorfismo de grupos. Como $\sigma\tau(\omega) = \sigma(\tau(\omega)) = \sigma(\omega^r) = \sigma(\omega)^r = (\omega^k)^r = \omega^{kr}$, entonces $\Psi(\sigma\tau) = \overline{k \cdot r} = \overline{k} \cdot \overline{r} = \Psi(\sigma)\Psi(\tau)$.

Demostraremos a continuación que Ψ es inyectiva. Si $\Psi(\sigma) = \overline{1}$, entonces $\sigma(\omega) = \omega$. Un elemento cualquiera β de $K = \mathbb{Q}(\omega)$ es de la forma $\beta = \sum_{i=0}^{\varphi(n)-1} a_i\omega^i$, donde $a_0, a_1, \ldots, a_{\varphi(n)-1}$ son elementos en $\mathbb{Q}$. Ahora,

$$\sigma(\beta) = \sum_{i=0}^{\varphi(n)-1} \sigma(a_i\omega^i) = \sum_{i=0}^{\varphi(n)-1} \sigma(a_i)\sigma(\omega^i) = \sum_{i=0}^{\varphi(n)-1} a_i\sigma(\omega)^i = \sum_{i=0}^{\varphi(n)-1} a_i\omega^i = \beta,$$

lo cual demuestra que $\sigma = I_K$ (I_K es la función identidad de K) y por lo tanto, Ψ es inyectiva. Como $G(K/\mathbb{Q})$ y U_n son grupos con $\varphi(n)$ elementos, entonces Ψ es sobreyectiva. □

Corolario 5.7. *Si p es un número primo, entonces el grupo de Galois del polinomio $f(x) = x^p - 1$ es cíclico con $p - 1$ elementos.*

Demostración. Por el teorema anterior, el grupo de Galois del polinomio $f(x) = x^p - 1$ sobre $\mathbb{Q}$ es isomorfo a U_p. Pero $U_p = \mathbb{Z}_p - \{\overline{0}\}$ y como $\mathbb{Z}_p$ es un cuerpo finito con p elementos, entonces $\mathbb{Z}_p - \{\overline{0}\}$ es un grupo cíclico con el producto de $\mathbb{Z}_p$ con $p-1$ elementos. □

5.7 Polígono Regular

Como una aplicación del Teorema Fundamental de la Teoría de Galois, demostraremos que: un polígono regular de n lados es constructible, si y solo si, $\varphi(n)$ es una potencia de 2, donde φ es la función de Euler.

Sea $\omega = \cos(\frac{2\pi}{n}) + isen(\frac{2\pi}{n})$ con $n \geq 3$. Consideremos un sistema coordenado cartesiano rectangular en el plano y una circunferencia de centro en el origen y radio 1. Las potencias de ω las podemos representar geométricamente como puntos de la circunferencia. Si $n = 3$, entonces estos puntos determinan un triángulo equilátero. Si $n = 4$, determinan un cuadrado y, en general, n puntos determinan un polígono regular de n lados.

Si $\cos(\frac{2\pi}{n})$ resulta ser un real constructible, entonces podemos construir el punto $(\cos(\frac{2\pi}{n}), 0)$ del plano. Si trazamos en el plano una recta perpendicular al eje x que pasa por el punto $(\cos(\frac{2\pi}{n}), 0)$, entonces dicha recta intersecta a la circunferencia en dos puntos, siendo uno de ellos $(\cos(\frac{2\pi}{n}), sen(\frac{2\pi}{n}))$ que es uno de los vértices de un polígono regular de n lados. Ahora podemos construir el segmento que determinan los puntos $(1, 0)$ y $(\cos(\frac{2\pi}{n}), sen(\frac{2\pi}{n}))$, es decir, uno de los lados del polígono. Es claro que con regla y compás podemos construir los vértices y lados restantes. De esta forma, para $n \geq 3$, obtenemos el siguiente resultado:

Lema 5.6. *Un polígono regular de n lados es constructible, si y solo si,* $\cos(\frac{2\pi}{n})$ *es un real constructible.*

En la demostración del Teorema 5.11, utilizaremos uno de los teoremas de Sylow: si p es un número primo y G es un grupo con p^n elementos, entonces existe una sucesión de subgrupos normales

$$\{1\} = G_0 \leq G_1 \leq \cdots \leq G_n = G \text{ tales que } \circ(G_i) = p^i \text{ para todo } i = 0, 1, \ldots, n.$$

Teorema 5.11. *Un polígono regular de n lados es constructible, si y solo si,* $\varphi(n)$ *es una potencia de* 2.

Demostración. Sea $\omega = \cos(\frac{2\pi}{n}) + isen(\frac{2\pi}{n})$ con $n \geq 3$. Como

$$(\cos(\tfrac{2\pi}{n}) + isen(\tfrac{2\pi}{n}))(\cos(\tfrac{2\pi}{n}) - isen(\tfrac{2\pi}{n})) = \cos^2(\tfrac{2\pi}{n}) + sen^2(\tfrac{2\pi}{n}) = 1,$$

entonces

$$\omega^{-1} = \frac{1}{\omega} = \cos(\frac{2\pi}{n}) - isen(\frac{2\pi}{n})$$

y luego, $\omega + \frac{1}{\omega} = 2\cos(\frac{2\pi}{n})$. $K = \mathbb{Q}(\omega)$ es el cuerpo de descomposición de $f(x) = x^n - 1$ sobre $\mathbb{Q}$ y $[K : \mathbb{Q}] = \varphi(n)$. Dado que $\omega + \frac{1}{\omega} \in K$, entonces K es una extensión de Galois de $\mathbb{Q}(\omega + \frac{1}{\omega}) = \mathbb{Q}(\cos(\frac{2\pi}{n}))$.

A continuación encontraremos los elementos del grupo de Galois $G(K/E) \leq G(K/\mathbb{Q})$, donde $E = \mathbb{Q}(\omega + \frac{1}{\omega})$. Si σ es un elemento en el grupo de Galois $G(K/\mathbb{Q})$, entonces existe un entero r tal que $\sigma(\omega) = \omega^r$ con $1 \leq r < n$ y $(r, n) = 1$. Ahora,

$$\begin{aligned}\sigma(2\cos(\frac{2\pi}{n})) &= \sigma(\omega + \frac{1}{\omega}) = \omega^r + \frac{1}{\omega^r} \\ &= (\cos(\frac{2\pi r}{n}) + isen(\frac{2\pi r}{n})) + (\cos(\frac{2\pi r}{n}) - isen(\frac{2\pi r}{n})) = 2\cos(\frac{2\pi r}{n}).\end{aligned}$$

Es decir, $\sigma(2\cos(\frac{2\pi}{n})) = 2\cos(\frac{2\pi r}{n})$. Tenemos que $2\cos(\frac{2\pi r}{n}) = 2\cos(\frac{2\pi}{n})$ solamente en los casos $r = 1$ y $r = n - 1$. Así, el elemento $\tau \in G(K/\mathbb{Q})$ tal que $\tau(\omega) = \omega^{n-1} = \frac{1}{\omega}$ y la identidad I son los únicos elementos del grupo $G(K/\mathbb{Q})$ que fijan el cuerpo $E = \mathbb{Q}(\omega + \frac{1}{\omega})$. Por lo tanto, $G(K/E) = \{I, \tau\}$.

De $[K : E] = \circ(G(K/E)) = 2$ y $[K : E][E : \mathbb{Q}] = [K : \mathbb{Q}] = \varphi(n)$, obtenemos que $[E : \mathbb{Q}] = \frac{1}{2}\varphi(n)$.

Si suponemos que un polígono regular de n lados es constructible, entonces del Lema 5.6, $2\cos(\frac{2\pi}{n}) = \omega + \frac{1}{\omega}$ es un real constructible y por el Teorema 4.4, $[E : \mathbb{Q}] = \frac{1}{2}\varphi(n)$ es una potencia de 2. En consecuencia, $\varphi(n)$ es una potencia de 2.

Supongamos ahora que $\varphi(n) = 2^k$. Entonces, $\circ(G(K/\mathbb{Q})) = 2^k$. Utilizando uno de los teoremas de Sylow, mencionado anteriormente, existe un sucesión de subgrupos $\{I\} = H_0 \leq H_1 \leq \cdots \leq H_k = G(K/\mathbb{Q})$ tales que $\circ(H_i) = 2^i$ para todo $i = 0, 1, \ldots, k$. De la correspondencia biyectiva, dada en el Teorema Fundamental de la Teoría de Galois, obtenemos que

$$\mathbb{Q} = K^{H_k} \leq K^{H_{k-1}} \leq \cdots \leq K^{H_1} = E = \mathbb{Q}(\omega + \frac{1}{\omega}) = \mathbb{Q}(\cos(\frac{2\pi}{n}))$$

con $[K^{H_{i-1}} : K^{H_i}] = 2$. Notemos que $\mathbb{Q}(\omega + \frac{1}{\omega})$ es un subcuerpo de $\mathbb{R}$. Del Teorema 4.3, $\mathbb{Q}(\omega + \frac{1}{\omega}) = \mathbb{Q}(\cos(\frac{2\pi}{n}))$ es un cuerpo constructible y luego, $\cos(\frac{2\pi}{n})$ es constructible. Del Lema 5.6, concluimos que un polígono regular de n lados es constructible. □

En el teorema anterior es natural preguntarse, ¿qué forma tienen los enteros $n \geq 3$ para los cuales $\varphi(n)$ es una potencia de 2?

i) Si $n \geq 3$ es una potencia de 2, entonces $\varphi(n)$ es una potencia de 2. En efecto, si $n = 2^k$ con $k \geq 2$, entonces $\varphi(n) = 2^{k-1}(2 - 1) = 2^{k-1}$ (Ver, [13]).

ii) Si $n \geq 3$ no es una potencia de 2, entonces podemos escribir n de la forma $n = 2^s p_1^{m_1} \cdots p_k^{m_k}$, donde $p_1, \ldots, p_k$ son primos impares distintos, $m_1, \ldots, m_k$ enteros positivos y $s \geq 0$. Como $\varphi(n) = \varphi(2^s)\varphi(p_1^{m_1}) \cdots \varphi(p_k^{m_k})$ (ver, [13]) y deseamos que $\varphi(n)$ sea una potencia de 2, entonces cada factor $\varphi(p_j^{m_j}) = p_j^{m_j - 1}(p_j - 1)$ debe ser una potencia de 2. Si $m_j - 1 > 0$, entonces $\varphi(p_j^{m_j})$ no es una potencia de 2, necesariamente $m_j = 1$ y $p_j - 1 = 2^m$ con $m \geq 1$. Es decir, $p_j = 2^m + 1$.

Demostraremos a continuación que m es una potencia de 2. Supongamos que existe un primo impar q que es un divisor de m. Entonces $m = qu$ con $u \geq 1$ y luego, $p_j = 2^{qu} + 1 = (2^u)^q + 1$.

Notemos que -1 es una raíz del polinomio $x^q + 1$, en consecuencia,

$$x + 1 \text{ es un divisor de } x^q + 1 \tag{1}$$

Reemplazando x por 2^u en (1), obtenemos que $2^u + 1$ es un divisor de $(2^u)^q + 1 = p_j$, lo que es una contradicción, dado que p_j es un primo. Concluimos que m es una potencia de 2, es decir, $m = 2^r$ con $r \geq 0$. Por lo tanto,

$$p_j = 2^{2^r} + 1 \text{ con } r \geq 0 \tag{2}$$

Así, $n = 2^s p_1 \cdots p_k$, donde $p_1, \ldots, p_k$ son primos impares distintos y $p_j = 2^{2^{r_j}} + 1$ con $r_j \geq 0$. Los números primos que tienen la forma (2), son llamados **primos de Fermat**. El lector puede verificar que, si $n = 2^s p_1 \cdots p_k$, donde $p_1, \ldots, p_k$ son primos impares distintos, $s \geq 0$ y $p_j = 2^{2^{r_j}} + 1$ con $r_j \geq 0$, entonces $\varphi(n)$ es una potencia de 2.

Del estudio anterior y del Teorema 5.11, obtenemos el siguiente teorema:

Teorema 5.12. *Un polígono regular de n lados es constructible, si y solo si,*

i) $n = 2^k$ con $k \geq 2$, o
ii) $n = 2^s p_1 \cdots p_k$, donde $p_1, \ldots, p_k$ son primos impares distintos $s \geq 0$ y $p_j = 2^{2^{r_j}} + 1$ con $r_j \geq 0$.

Observación 5.5. *Fermat conjeturó que cualquier entero de la forma* $2^{2^k} + 1$ *con* $k \geq 0$ *era un número primo. Euler demostró esta conjetura para los casos* $k = 0$, 1, 2, 3, 4. *Ha sido demostrado que cuando* $5 \leq k \leq 16$, *los números* $2^{2^k} + 1$ *no son primos. Lo que actualmente no se sabe es si los primos de Fermat son infinitos.*

Del Teorema 5.12, concluimos que los polígonos regulares de p lados (con p primo impar) constructibles, son aquellos para los cuales p es un primo de Fermat.

Leonhard Euler (1707-1783) fue un matemático y físico nacido en Basilea (Suiza). Considerado como uno de los más grandes matemáticos de todos los tiempos, realizó importantes aportes en áreas tan diversas como: el cálculo, teoría de grafos, análisis matemático, mecánica, óptica y astronomía.

Ejercicios 5.8.

1. Demostrar que el hexágono regular es constructible.
2. Demostrar que el pentadecágono (polígono regular de 15 lados) es constructible.
3. Demostrar que un eneágono (polígono regular de 9 lados) no es constructible.
4. ¿Es el polígono regular de 255 lados constructible?

5.8 Solubilidad por Radicales

Sea F un cuerpo. Diremos que un polinomio $f(x) \in F[x]$ es **soluble por radicales sobre** F, si las raíces de dicho polinomio se pueden obtener en términos de los coeficientes del polinomio, usando una sucesión finita de operaciones algebraicas (suma, resta, multiplicación, división) y la extracción de raíces (raíces cuadradas, cúbicas,

etc.). Es sabido que las raíces en $\mathbb{C}$ del polinomio $f(x) = ax^2 + bx + c \in \mathbb{R}[x]$ con $a \neq 0$ son $\frac{1}{2a}(-b \pm \sqrt{b^2 - 4ac})$. Por lo tanto, $f(x)$ es soluble por radicales sobre $\mathbb{R}$.

El Teorema Fundamental del Álgebra garantiza la existencia de las raíces de un polinomio con coeficientes complejos, pero su demostración no entrega un método para el cálculo de sus raíces. Existen fórmulas que permiten encontrar las raíces de un polinomio de grado 3 y grado 4, que fueron descubiertas por dos matemáticos italianos del Renacimiento, Tartaglia (1530) y Del Ferro (1545). Cardano también publicó fórmulas similares en su "*A*rs Magna", aparecida en 1545. En dicha obra también se incluye un método para la resolución de una ecuación de cuarto grado.

Los métodos encontrados para el cálculo de las raíces de un polinomio de grado 3 y grado 4 con coeficientes complejos nos permiten afirmar que, si $f(x)$ es un polinomio (de grado 3 ó grado 4) con coeficientes en un cuerpo F, entonces $f(x)$ es soluble por radicales sobre F.

A continuación exponemos el método descubierto por Cardano que permite explícitamente encontrar las raíces de un polinomio de grado 3.

Teorema 5.13. *Sea F un cuerpo y $f(x) = x^3 + ax^2 + bx + c \in F[x]$. Entonces $f(x)$ es soluble por radicales sobre F.*

Demostración. En la sección 5.5, se estudia que los polinomios $f(x) = x^3 + ax^2 + bx + c$ y $g(x) = x^3 + (b - \frac{1}{3}a^2)x + c - \frac{1}{3}ab + \frac{2}{27}a^3$ están relacionados por la siguiente propiedad: Si $\beta \in \mathbb{C}$ es una raíz de $f(x)$, entonces $\beta + \frac{1}{3}a$ es una raíz de $g(x)$ y si $\gamma \in \mathbb{C}$ es una raíz de $g(x)$, entonces $\gamma - \frac{1}{3}a$ es una raíz de $f(x)$. Por lo tanto, las raíces de $f(x)$ y $g(x)$ difieren en $\frac{1}{3}a$ y así, los cuerpos de descomposición de $f(x)$ y $g(x)$ son iguales. De esta forma, para encontrar las raíces de $f(x)$, basta con encontrar las raíces del polinomio

$$g(x) = x^3 + px + q, \tag{1}$$

donde $p = b - \frac{1}{3}a^2$ y $q = c - \frac{1}{3}ab + \frac{2}{27}a^3$. Si suponemos que $p = 0$, entonces las soluciones de $x^3 + q = 0$ serán las raíces cúbicas de $-q$. Ahora, si suponemos que $q = 0$, entonces las soluciones de $x^3 + px = x(x^2 + p) = 0$ serán 0 y las raíces cuadradas de $-p$. Podemos suponer que $pq \neq 0$. Consideremos la ecuación cuadrática

$$x^2 + qx - \frac{1}{27}p^3 = 0, \tag{2}$$

cuyas soluciones son no nulas. Como,

$$\frac{1}{2}(-q \pm \sqrt{q^2 + \frac{4}{27}p^3}) = -\frac{1}{2}q \pm \sqrt{\frac{1}{4}q^2 + \frac{1}{27}p^3}),$$

entonces las soluciones de (2) , son: $-\frac{1}{2}q+\delta$ y $-\frac{1}{2}q-\delta$, donde $\delta \in \mathbb{C}$ y $\delta^2 = \frac{1}{4}q^2+\frac{1}{27}p^3$. Sea $u \in \mathbb{C}$ tal que $u^3 = -\frac{1}{2}q+\delta$. Si $v = -\frac{p}{3u}$, entonces $v^3 = -\frac{1}{2}q-\delta$. En efecto,

$$\begin{aligned} v^3 &= -\frac{p^3}{27u^3} = -\frac{p^3}{27(-\frac{1}{2}q+\delta)} = -\frac{p^3(-\frac{1}{2}q-\delta)}{27(\frac{1}{4}q^2-\delta^2)} \\ &= -\frac{p^3(-\frac{1}{2}q-\delta)}{27(\frac{1}{4}q^2-\delta^2)} = \frac{p^3(-\frac{1}{2}q-\delta)}{p^3} = -\frac{1}{2}q-\delta. \end{aligned}$$

Ahora, sabemos que

$$u^3+v^3 = -q \quad \text{y} \quad 3uv+p = 0. \tag{3}$$

Utilizando (3) , obtenemos que

$$(u+v)^3+p(u+v)+q = u^3+v^3+(3uv+p)(u+v)+q = 0,$$

lo que demuestra que $u+v$ es una raíz de (1). Escribimos esta solución por

$$\sqrt[3]{-\frac{1}{2}q+\sqrt{\frac{1}{4}q^2+\frac{1}{27}p^3}}+\sqrt[3]{-\frac{1}{2}q-\sqrt{\frac{1}{4}q^2+\frac{1}{27}p^3}}.$$

Si $\omega \neq 1$ es una raíz cúbica primitiva de la unidad, es decir, si $\omega = -\frac{1}{2}+\frac{1}{2}\sqrt{3}i$ ó $\omega = -\frac{1}{2}-\frac{1}{2}\sqrt{3}i$, entonces el lector puede verificar que $u\omega+v\omega^2$ y $u\omega^2+v\omega$ también son raíces de $g(x)$. □

Ejemplo 5.20. *Utilizando el método dado en la demostración del Teorema 5.13, encontraremos todas las raíces en* $\mathbb{C}$ *del polinomio* $f(x) = x^3+3ix-1-i$.

Claramente, $p = 3i$ *y* $q = -1-i$. *La ecuación* (2) *es* $x^2-(1+i)\,x+i = 0$. *Una solución de esta ecuación es* $\delta = i$. *Una raíz cúbica de* i *es* $u = \frac{1}{2}\sqrt{3}+\frac{1}{2}i$. *Ahora,* $v = -\frac{3i}{3u} = -\frac{1}{2}-\frac{1}{2}\sqrt{3}i$. *Las soluciones de* $f(x)$ *son:*

$$\begin{aligned} u+v &= \frac{1}{2}\sqrt{3}-\frac{1}{2}+(\frac{1}{2}-\frac{1}{2}\sqrt{3})i, \\ u\omega+v\omega^2 &= u(-\frac{1}{2}+\frac{1}{2}\sqrt{3}i)+v(-\frac{1}{2}+\frac{1}{2}\sqrt{3}i)^2 = -\frac{1}{2}\sqrt{3}-\frac{1}{2}+(\frac{1}{2}+\frac{1}{2}\sqrt{3})i, \\ u\omega^2+v\omega &= u(-\frac{1}{2}+\frac{1}{2}\sqrt{3}i)^2+v(-\frac{1}{2}+\frac{1}{2}\sqrt{3}i) = 1-i. \end{aligned}$$

Ejercicios 5.9.

Encontrar todas las soluciones complejas de las siguientes ecuaciones:

a) $x^2+3-4i = 0$ *b)* $x^2+(1+2i)x-3+i = 0$

c) $x^3+(1+2i)x-1+i = 0$ *d)* $x^3+3iz^2-10i = 0$

A continuación exponemos un método que permite calcular las raíces de un polinomio de grado 4.

Teorema 5.14. *Sea* F *un cuerpo y* $f(x) = x^4+ax^3+bx^2+cx+d \in F[x]$. *Entonces* $f(x)$ *es soluble por radicales.*

Demostración. Reemplazando x por $y-\frac{1}{4}a$ en $f(x)$, obtenemos que $f(y-\frac{1}{4}a) = y^4+py^2+qy+r$, donde $p=b-\frac{3}{8}a^2$, $q=c-\frac{1}{2}ab+\frac{1}{8}a^3$ y $r=d-\frac{1}{4}ac-\frac{3}{256}a^4+\frac{1}{16}a^2b$. A continuación encontraremos β, γ, $\delta \in \mathbb{C}$ tales que

$$y^4+py^2+qy+r=(y^2+\beta y+\gamma)(y^2-\beta y+\delta)$$

Como

$$(y^2+\beta y+\gamma)(y^2-\beta y+\delta)=y^4+(\gamma+\delta-\beta^2)y^2+(\beta\delta-\beta\gamma)y+\gamma\delta,$$

entonces

$$\gamma+\delta-\beta^2=p,\ \beta\delta-\beta\gamma=q \text{ y } \gamma\delta=r. \tag{1}$$

Utilizando las relaciones anteriores, obtenemos que

$$\beta^6+2p\beta^4+(p^2-4r)\beta^2-q^2=\beta^6+2(\gamma+\delta-\beta^2)\beta^4+((\gamma+\delta-\beta^2)^2-4\gamma\delta)\beta^2-(\beta\delta-\beta\gamma)^2=0.$$

Por lo tanto, β^2 es una raíz de la ecuación $z^3+2pz^2+(p^2-4r)z-q^2=0$, que podemos calcular y así obtenemos β. De las relaciones (1), obtenemos γ y δ. Ahora, calculamos las soluciones de las ecuaciones $y^2+\beta y+\gamma=0$ e $y^2-\beta y+\delta=0$. Finalmente, reemplazando estas soluciones en $x=y-\frac{1}{4}a$, obtenemos las soluciones de $f(x)$. □

Definición 5.8. *Una extensión K de un cuerpo F se dice que es una* ***extensión radical*** *de F, si existen elementos $\alpha_1,\ldots,\alpha_r \in K$ y enteros positivos $n_1,\ldots,n_r$ tales que $K=F(\alpha_1,\ldots,\alpha_r)$, $\alpha_1^{n_1}\in F$ y $\alpha_i^{n_i}\in F(\alpha_1,\ldots,\alpha_{i-1})$ para $1<i\leq r$.*

Ejemplo 5.21. *Demostraremos que $\mathbb{Q}(\sqrt{1+\sqrt{2}})$ es una extensión radical de $\mathbb{Q}$.*

Dado que, $\left(\sqrt{1+\sqrt{2}}\right)^2=1+\sqrt{2}\in\mathbb{Q}(\sqrt{1+\sqrt{2}})$, entonces $\sqrt{2}\in\mathbb{Q}(\sqrt{1+\sqrt{2}})$. Por lo tanto, $\mathbb{Q}(\sqrt{1+\sqrt{2}})=\mathbb{Q}(\sqrt{2},\sqrt{1+\sqrt{2}})$. Ahora, $\mathbb{Q}(\sqrt{2},\sqrt{1+\sqrt{2}})$ es una extensión radical de $\mathbb{Q}$, dado que $\left(\sqrt{2}\right)^2\in\mathbb{Q}$ y $\left(\sqrt{1+\sqrt{2}}\right)^2\in\mathbb{Q}(\sqrt{2})$.

La definición en términos matemáticos del hecho que un polinomio sea soluble por radicales sobre un cuerpo, es la que sigue:

Definición 5.9. *Sean F un cuerpo, $f(x)\in F[x]$ y K el cuerpo de descomposición de $f(x)$ sobre F. Entonces, $f(x)$ es* ***soluble por radicales*** *sobre F, si existe una extensión radical E de F tal que $F\subset K\subset E$.*

Ejemplo 5.22. *Demostraremos que el polinomio $f(x)=x^5-3$ es soluble por radicales sobre $\mathbb{Q}$. El complejo $\omega=\cos(\frac{2\pi}{5})+isen(\frac{2\pi}{5})$ es una raíz quinta primitiva de la unidad y $\sqrt[5]{3}$ es una raíz de $f(x)$. Entonces, el cuerpo de descomposición de $f(x)$ sobre $\mathbb{Q}$ es $\mathbb{Q}(\sqrt[5]{3},\sqrt[5]{3}\omega,\ldots,\sqrt[5]{3}\omega^4)=\mathbb{Q}(\sqrt[5]{3},\omega)$. Como $\left(\sqrt[5]{3}\right)^5=3\in\mathbb{Q}$ y $\omega^5=1\in\mathbb{Q}(\sqrt[5]{3})$, de acuerdo a la definición 5.9, $f(x)=x^5-3$ es soluble por radicales sobre $\mathbb{Q}$.*

Ejemplo 5.23. *Demostraremos que el polinomio $f(x)=x^6+bx^3+c\in\mathbb{Q}[x]$ es soluble por radicales sobre $\mathbb{Q}$. Utilizando la fórmula que permite encontrar las raíces de un*

polinomio de grado 2, obtenemos que $x^3 = \frac{1}{2}(-b+\gamma)$ *ó* $x^3 = \frac{1}{2}(-b-\gamma)$, *donde* $\gamma \in \mathbb{C}$ *es una raíz cuadrada de* $b^2 - 4c$.

Sean α, β *en* $\mathbb{C}$ *raíces de los polinomios* $x^3 - \frac{1}{2}(-b+\gamma)$ *y* $x^3 - \frac{1}{2}(-b-\gamma)$, *respectivamente y* ω *una raíz cúbica primitiva de la unidad. Entonces* α, $\alpha\omega$, $\alpha\omega^2$ *son raíces de* $x^3 - \frac{1}{2}(-b+\gamma)$ *y* β, $\beta\omega$, $\beta\omega^2$ *son raíces de* $x^3 - \frac{1}{2}(-b-\gamma)$. *Por lo tanto, el cuerpo de descomposición de* $f(x)$ *es* $\mathbb{Q}(\alpha, \beta, \alpha\omega, \alpha\omega^2, \beta\omega, \beta\omega^2) = \mathbb{Q}(\omega, \alpha, \beta)$. *Dado que* $\alpha^3 = \frac{1}{2}(-b+\gamma) \in \mathbb{Q}(\omega, \alpha, \beta)$, *entonces* $\gamma \in \mathbb{Q}(\omega, \alpha, \beta)$ *y luego,* $\mathbb{Q}(\omega, \alpha, \beta) = \mathbb{Q}(\gamma, \omega, \alpha, \beta)$. *Como,* $\gamma^2 \in \mathbb{Q}$, $\omega^3 = 1 \in \mathbb{Q}(\gamma)$, $\alpha^3 \in \mathbb{Q}(\gamma, \omega)$ *y* $\beta^3 \in \mathbb{Q}(\gamma, \omega, \alpha)$, *entonces* $f(x) = x^6 + bx^3 + c \in \mathbb{Q}[x]$ *es soluble por radicales sobre* $\mathbb{Q}$.

Ejemplo 5.24. *Sea* F *un cuerpo y* $p(x) = x^3 + px + q \in F[x]$. *Utilizando la definición 5.9, demostraremos que* $p(x)$ *es soluble por radicales sobre* F.

Dejamos como ejercicio el caso $pq = 0$. *Supongamos que* $pq \neq 0$. *De la demostración del Teorema 5.12, sabemos* $u + v$, $u\omega + v\omega^2$ *y* $u\omega^2 + v\omega$ *son las raíces de* $p(x)$, *donde* $\omega \neq 1$ *es una raíz cúbica de la unidad,* $u^3 = -\frac{1}{2}q + \delta$, $v^3 = -\frac{1}{2}q - \delta$, *siendo* $\delta^2 = \frac{1}{4}q^2 + \frac{1}{27}p^3$. *Claramente*

$$F \leq F(u+v, \omega u + \omega^2 v, \omega^2 u + \omega v) \leq F(\omega, u, v) \leq F(\omega, \delta, u, v)$$

y además, $F(\omega, \delta, u, v)$ *es una extensión radical de* F. *En efecto,* $\omega^3 = 1 \in F$, $\delta^2 \in F(\omega)$, $u^3 \in F(\omega, \delta)$ *y* $v^3 \in F(\omega, \delta, u)$. *Por la definición 5.9, concluimos que* $p(x)$ *es soluble por radicales sobre* F.

El primer matemático en afirmar que existían ecuaciones de quinto grado que no eran solubles por radicales, fue Ruffini en 1799. El trabajo donde Ruffini incluía la demostración de la afirmación anterior no fue leída por Lagrange, a quien Ruffini envió para su aprobación.

En 1824 Abel dio la primera demostración aceptada de la no solubilidad por radicales de algunas ecuaciones de quinto grado. Pero fue Galois, en 1831, el primero en relacionar la solubilidad por radicales de una ecuación con la estructura del grupo de permutaciones de las raíces de dicha ecuación, hoy conocido como el grupo de Galois. Si el lector tiene interés en profundizar sobre este tema puede consultar los textos [5] , [6] , [17] de la bibliografía.

Finalizamos este capítulo enunciando un importante teorema demostrado por Abel.

Teorema 5.15. *Sea* F *un cuerpo. Si* $p(x) \in F[x]$ *es soluble por radicales sobre* F, *entonces el grupo de Galois de* $p(x)$ *sobre* F *es un grupo soluble.*

Que un grupo G sea soluble, significa que existen subgrupos $N_1, \ldots, N_r$ de G tales que $\{e\} = N_0 \subset N_1 \subset \cdots \subset N_r = G$, N_i es un subgrupo normal de N_{i+1} y N_{i+1}/N_i es abeliano.

Observación 5.6. *En esta monografía no incluimos un estudio sobre los posibles grupos de Galois de un polinomio de grado* 4 *e irreducible sobre un cuerpo* F. *Dichos grupos resultan ser isomorfos a subgrupos del grupo simétrico* S_4, *el cual es soluble.*

Si es posible encontrar un polinomio $p(x) \in \mathbb{Q}[x]$ tal que el grupo de Galois de $p(x)$ sobre $\mathbb{Q}$ no sea un grupo soluble, entonces (de acuerdo al Teorema 5.15) estaremos en presencia de un polinomio que no es soluble por radicales sobre $\mathbb{Q}$.

Existe un importante resultado que dice: si $f(x) \in \mathbb{Q}[x]$ es irreducible sobre $\mathbb{Q}$, de grado p con p primo y $f(x)$ tiene exactamente 2 raíces no reales, entonces el grupo de Galois de $f(x)$ sobre $\mathbb{Q}$ es isomorfo al grupo simétrico S_p.

Utilizando el criterio de Schöneman-Eisenstein, $f(x) = x^5 - 6x + 3 \in \mathbb{Q}[x]$ es irreducible sobre $\mathbb{Q}$. Utilizando los resultados estudiados en los primeros cursos de cálculo, el lector puede verificar que $f(x)$ tiene 3 raíces reales y 2 raíces no reales. En consecuencia, el grupo de Galois de $f(x)$ sobre $\mathbb{Q}$ es isomorfo al grupo simétrico S_5. Como S_5 no es un grupo soluble, entonces $f(x)$ no es soluble por radicales sobre $\mathbb{Q}$.

5.9 Ejercicios de Reforzamiento

1. Determinar si las siguientes afirmaciones son verdaderas o falsas.
   a) Sea K un subcuerpo de $\mathbb{C}$. Entonces, existe un homomorfismo inyectivo de anillos $\sigma : K \to \mathbb{C}$ y un elemento $\alpha \in \mathbb{Q}$ tal que $\sigma(\alpha) \neq \alpha$.
   b) Existe un cuerpo K tal que $\mathbb{R} \subset K \subset \mathbb{C}$ con $\mathbb{R} \neq K$ y $K \neq \mathbb{C}$.
   c) $\mathbb{Q}(\sqrt{7})$ es una extensión de Galois de $\mathbb{Q}$.
   d) $\tau : \mathbb{Q}(\sqrt{3}) \to \mathbb{Q}(\sqrt{3})$ definida por $\tau(a + b\sqrt{3}) = a - b\sqrt{3}$ para todo $a, b \in \mathbb{Q}$ es un elemento del grupo de Galois $G(\mathbb{Q}(\sqrt{3})/\mathbb{Q})$.
   e) Todo grupo de Galois es Abeliano.
   f) El polígono regular con 17 lados es constructible.
2. Encontrar el cuerpo de descomposición K del polinomio $f(x) = x^5 - 7$ sobre $\mathbb{Q}(\sqrt[5]{7})$. Encontrar el grupo de Galois $G(K/\mathbb{Q})$ de $f(x)$ y la correspondencia biyectiva entre los subgrupos de $G(K/\mathbb{Q})$ y los subcuerpos de K.
3. ¿Es $\mathbb{Q}(\sqrt{3}, \sqrt{7})$ una extensión de Galois de $\mathbb{Q}$? ¿Es $\mathbb{Q}(\sqrt[3]{5}, \sqrt{3}i)$ una extensión de Galois de $\mathbb{Q}(\sqrt[3]{5}(1 + \sqrt{3}i))$?
4. Sea $K = \mathbb{Q}(\sqrt[8]{2}, i)$.
   a) Demostrar que $K = \mathbb{Q}(\sqrt[8]{2}, i)$ es una extensión de Galois de $\mathbb{Q}$ y que $[K : \mathbb{Q}] = 16$.
   b) Demostrar que el grupo $G(K/\mathbb{Q}(i))$ es cíclico.
   c) Demostrar que el grupo $G(K/\mathbb{Q}(\sqrt{2}i))$ no es Abeliano.
5. Demostrar que $\mathbb{Q}(\sqrt[6]{2}, i)$ es una extensión de $\mathbb{Q}(\sqrt[3]{2})$.
   a) ¿Es $\mathbb{Q}(\sqrt[6]{2}, i)$ una extensión de Galois de $\mathbb{Q}(\sqrt[3]{2})$?
   b) ¿Es $\mathbb{Q}(\sqrt[6]{2}, i)$ una extensión de Galois de $\mathbb{Q}$?
6. Sea $f(x) = (x^{12} - 16)(x^2 - 3) \in \mathbb{Q}[x]$.
   a) Demostrar que $K = \mathbb{Q}(\sqrt[3]{2}, \sqrt{3}, i)$ es el cuerpo de descomposición de $f(x)$ sobre $\mathbb{Q}$.
   b) Demostrar que $[K : \mathbb{Q}] = 12$.
   c) Demostrar que existe una extensión de Galois E de $\mathbb{Q}$ con $\mathbb{Q} \leq E \leq K$ tal que $[E : \mathbb{Q}] = 6$.

Apéndice A: Códigos Lineales

Una importante aplicación de la teoría de cuerpos finitos es la Teoría de Códigos. Dicha teoría tiene su origen en un famoso teorema de Shannon (1948) que garantiza la existencia de códigos que pueden transmitir información a velocidad cercana a la capacidad de un canal de comunicación con una pequeña probabilidad de error.

Durante las dos últimas décadas más y más herramientas algebraicas como la teoría de cuerpos finitos y la teoría de polinomios sobre cuerpos finitos, han influenciado la teoría de códigos.

Códigos lineales: El problema de la comunicación de información, en particular codificar y decodificar la información para una trasmisión en un canal, es de gran importancia hoy día. Típicamente uno tiene que trasmitir un mensaje que consiste en una hilera finita de símbolos que son elementos de un alfabeto finito. Por ejemplo, si el alfabeto consiste sólo de 0 y 1, entonces el mensaje se puede describir como un número binario. Generalmente se asume que el alfabeto es un cuerpo finito.

La transmisión de hileras finitas de elementos del alfabeto, en un canal de comunicación, puede no ser perfecta en el sentido que cada pedazo de información se transmite inalterable sobre el canal. No hay canal ideal sin ruido, el receptor del mensaje puede obtener información distorsionada y puede cometer errores al interpretar la señal transmitida. Los métodos para mejorar la recepción de la transmisión dependen de propiedades de los cuerpos finitos.

Sea F_q un cuerpo finito con q elementos. Para cada $n > 0$, denotemos por F_q^n a su n-ésima potencia cartesiana dotada de su estructura usual de espacio vectorial sobre el cuerpo F_q.

Definición A.1. *Todo subespacio C de F_q^n de dimensión k es un código lineal (n, k) sobre el alfabeto F_q.*

Sea C un código lineal (n, k), $C \leq F_q^n$. Para el caso de $q = 2$, se habla de código binario. Codificar significa transformar un mensaje de símbolos $a_1 a_2 \cdots a_k$, $a_i \in F_q$, en una palabra codificada (code word) $c_1 c_2 \cdots c_n$ de n símbolos $c_j \in F_q$, donde $n > q$. Miramos las palabras codificadas como vectores fila $c \in F_q^n$ y $F : F_q^k \to F_q^n$ se llama **función de codificación.**

Ejemplo A.1. *Definamos la función de codificación $F : F_2^k \to F_2^{k+1}$ por $F(c) = cx$, donde x es* 0, *si el número de dígitos no nulos en c es par, y* 1, *si el número de dígitos no nulos en c es impar. Específicamente para $k = 3$ hay ocho palabras y la función de*

codificación F es:

000	001	010	100	011	101	110	111
0000	0011	0101	1001	0110	1010	1100	1111

Todo código lineal (n, k) tiene k símbolos de información y $n - k$ símbolos de revisión. Está conformado por q^k palabras codificadas.

Definición A.2. *Sea C un código lineal (n, k) y $C \leq F_q^n$. Se dice que una matriz $H \in M_{(n-k)\times n}(F_q)$ es de control de paridad para C, si para todo $y \in F_q^n$:*

$$y \in C \Longleftrightarrow Hy^t = 0.$$

Definición A.3. *Sea C un código lineal (n, k) y $C \leq F_q^n$. Si hay una matriz $G \in M_{k\times n}(F_q)$ definida por $G = \begin{pmatrix} I_k & -A^t \end{pmatrix}$, se la llama **matriz generadora** del código C con matriz de control de paridad $H = \begin{pmatrix} A & I_{n-k} \end{pmatrix}$.*

Para $A \in M_{(n-k)\times k}(F_q)$ se tiene de manera natural

$G = \begin{pmatrix} I_k & -A^t \end{pmatrix}$ generadora $\Longleftrightarrow H = \begin{pmatrix} A & I_{n-k} \end{pmatrix}$ de control de paridad.

Por lo tanto, se tiene que toda matriz de control de paridad posee rango $n - k$.

Ejemplo A.2. *Encontraremos la función de codificación $F : F_2^2 \to F_2^4$ de un código lineal cuya matriz generadora es $G = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix}$.*

Necesitamos conocer $F(00), F(01), F(10)$ y $F(11)$. Pero $F(x) = xG$ para todo $x \in F_2$. Luego, $F(00) = (00)G = (00)\begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix} = 0000$.

En forma similar, se obtienen $F(01) = 0101,\ F(10) = 1011,\ F(11) = 1110$.

Ejemplo A.3. *Sea $F : F_2^k \to F_2^n$ la función de codificación dada por $a_1 \cdots a_k \to b_1 \cdots b_{k+1}$, donde $b_i = a_i$ para todo $i \in \{1, \ldots, k\}$ y $b_{k+1} = \sum_{i=1}^{k} a_i$. Encontraremos la matriz de control de paridad H.*

Estamos trabajando en un código binario y, en consecuencia, la suma de los dígitos de cualquier palabra codificada $b_1 \cdots b_{k+1}$ es 0. Si la suma de los dígitos de una palabra transmitida es 1, entonces el recibidor sabe que un error de transmisión debe haber ocurrido. Sea $n = k + 1$, entonces este código es un código lineal binario $(n, n - 1)$ con matriz de control de paridad $H = (11 \cdots 1)$.

Ejemplo A.4. *Sea $H = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix} \in M_{3\times 7}(F_2)$ matriz de control de paridad de un código lineal C, que lleva un mensaje $a_1\ a_2\ a_3\ a_4$ a uno codificado $a_1\ a_2\ a_3\ a_4\ c_1\ c_2\ c_3$. Encontraremos c_i, la función de codificación $F : F_2^4 \to F_2^7$ de C y la matriz generadora de C.*

Resolviendo $Hc^t = 0$, *donde* $c = (a_1, a_2, a_3, a_4, c_1, c_2, c_3)$ *se tienen las siguientes ecuaciones:*

$$\begin{aligned} a_1 + a_3 + a_4 + c_1 &= 0 \\ a_1 + a_2 + a_4 + c_2 &= 0 \\ a_1 + a_2 + a_3 + c_3 &= 0, \end{aligned}$$

de donde

$$\begin{aligned} c_1 &= a_1 + a_3 + a_4 \\ c_2 &= a_1 + a_2 + a_4 \\ c_3 &= a_1 + a_2 + a_3. \end{aligned}$$

Por lo tanto,

$$F(a_1, a_2, a_3, a_4) = (a_1, a_2, a_3, a_4, a_1 + a_3 + a_4, a_1 + a_2 + a_4, a_1 + a_2 + a_3)$$

es la función de codificación del código. La matriz generadora de C *es*

$$A = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 \end{pmatrix} \in M_{4\times 7}(F_2).$$

Definición A.4. *Sean* x, y *dos palabras en* F_q^n.

a) Se define la distancia de Hamming entre las palabras x *e* y *como el número de coordenadas en que difieren* x *e* y. *Se denota por* $d(x, y)$.

b) Se define el peso de Hamming de la palabra y *como el número de coordenadas no nulas de* y. *Se anota* $w(y)$.

Observación A.1. *Si* x *es una palabra codificada e* y *es la palabra que se recibe después de una comunicación a través de un canal con ruido,* $d(x, y)$ *da el número de errores que se comete en la transmisión. Se tiene de inmediato que* $w(x) = d(x, 0)$ *y que* $d(x, y) = w(x - y)$.

Como un ejercicio para el lector dejamos el siguiente resultado:

Teorema A.1. *La distancia de Hamming es una métrica en* F_q^n, *es decir, para todo* x, $y \in F_q^n$ *se tiene:*

1. $d(x, y) = 0$, *si y solo si,* $x = y$.
2. $d(x, y) = d(y, x)$.
3. $d(x, z) \leq d(x, y) + d(y, z)$.

Para un código lineal (n, k), $C \leq F_q^n$, su **distancia mínima** es

$$d_C = min\{w(y) \mid y \in C - \{0\}\} = min\{d(u, v) \mid u, v \in C, u \neq v\}.$$

Observación A.2. *La distancia mínima* d_C *de un código lineal* (n, k), $C \leq F_q^n$, *queda acotada por*

$$d_C \leq n - k + 1.$$

Ejemplo A.5.

$$d(010101, 101000) = w(010101 - 101000) = w(010101 + 101000) = w(111101) = 5.$$

Teorema A.2. *Un código lineal C con distancia mínima d_C puede corregir hasta t errores, si $d_c \geq 2t + 1$.*

Demostración. Una bola $B_t(x)$ de radio t y centro $x \in F_q^n$ consiste de todos los vectores $y \in F_q^n$ tales que $d(x, y) \leq t$. Para corregir t errores, las bolas con palabras codificadas como centros no deben intersectarse. Si $u \in B_t(x)$ y $u \in B_t(y)$ con x, $y \in C$, $x \neq y$, entonces $d(x, y) \leq d(x, u) + d(u, y) \leq 2t$, lo que contradice $d_c \geq 2t + 1$. □

Ejemplo A.6. *Para el código C del ejemplo A.2, $d_c = 2$. Luego, este código no puede corregir errores.*

Ejemplo A.7. *Consideremos el código lineal cuya función de codificación $F : F_2^3 \to F_2^6$ es:*

000	001	010	100	011	101	110	111
000000	001110	010011	011101	100101	101011	110110	111000

Entonces $d_c = 3$. Por lo tanto, este código puede corregir un error.

Definición A.5. *Si $H \in M_{(n-k)\times n}(F_q)$ es la matriz de control de paridad de un código lineal (n, k), $C \leq F^n$, entonces la transformación lineal $S : F_q^n \to F_q^{n-k}$ definida por $S(y) = Hy^t$ se llama función de **síndrome.** El valor $S(y)$ es el síndrome de la palabra y.*

Así, tenemos que las palabras en el código son exactamente aquéllas con síndrome nulo. En otras palabras, el núcleo de la transformación de síndrome es el código mismo.

Al ser C un subespacio, el cuociente $F_q^n/C = \{y + C \mid y \in F_q^n\}$ es, a su vez, un espacio vectorial sobre F_q. Naturalmente, dos palabras cualesquiera y, $z \in F_q^n$ en una misma clase del cuociente F_q^n/C, es decir, tales que $z - y \in C$, han de poseer el mismo síndrome, o sea, $S(z) = S(y)$.

También, si al transmitir una palabra en el código, digamos $y \in C$, se recibiera la palabra $z \in F_q^n$, entonces, para el error $e = z - y$ se habría de tener $S(e) = S(z)$. Así, el síndrome del error ha de coincidir con el síndrome de la palabra recibida, lo que, por lo anterior, equivale a que la palabra recibida z y el error cometido e necesariamente han de estar en una misma clase lateral de F_q^n/C.

Definición A.6. *Para cada clase $z + C \in F_q^n/C$, **un representante principal o líder de la clase lateral** es un vector $e \in z + C$ de peso de Hamming mínimo.*

Por el teorema fundamental de homomorfismos se tiene que $B : F_q^n \,/\, C \to Img(B)$ es un isomorfismo. Así, para cada posible valor de síndrome $s \in Img(B) \leq F_q^{n-k}$existe una única clase lateral $z_s + C \in F_q^n/C$ tal que $B(z_s + C) = s$. Sea e_s un representante principal de la clase $z_s + C$. Resulta, entonces, un procedimiento de decodificación.

Supongamos que al transmitir una palabra $y \in C$ se recibe la palabra $z \in F_q^n$, cometiéndose el error $e = z - y$, entonces se calcula el síndrome $s = Bz$ y considerando el representante principal e_s se recupera la palabra transmitida, tomando $z - e_s$. Este procedimiento, es claramente correcto, toda vez que $e = e_s$.

Ejemplo A.8. *Sea C código lineal binario (4,2) con matriz generadora G y matriz de control de paridad H, donde $G = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 \end{pmatrix}$ y $H = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}$. Encontraremos las palabras codificadas, los representantes principales y los respectivos síndromes.*

Sea $F : F_2^2 \to F_2^4$ función de codificación del código C. Necesitamos conocer $F(00)$, $F(01)$, $F(10)$ y $F(11)$. Pero $F(x) = xG$ para todo $x \in F_2$. Luego, $F(10) = (10)G = (10)\begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 \end{pmatrix} = 1010$.

De manera similar se prueba que $F(00) = 0000$, $F(01) = 0111$ y $F(11) = 1101$. Por lo tanto, las palabras codificadas son 0000, 1010, 0111 y 1101. Como están en el código, todas tienen síndrome $(00)^t$. Calculemos ahora los síndromes de 1000, 0010, 1111 y 0101.

$$S(1000) = H(1000)^t = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}(1000)^t = (10)^t.$$

$$S(0010) = H(0010)^t = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}(0010)^t = (10)^t.$$

$$S(1111) = H(1111)^t = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}(1111)^t = (10)^t.$$

$$S(0101) = H(0101)^t = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}(0101)^t = (10)^t.$$

El representante principal es 1000, pues su peso de Hamming es $w(1000) = 1$ que es mínimo. En forma similar se calculan todos los otros representantes y sus respectivos síndromes. En lo que sigue vemos una tabla mostrando todo lo que pide el problema.

mensaje	00	10	01	11	
palabra codificada	0000	1010	0111	1101	$(00)^t$
	1000	0010	1111	0101	$(10)^t$
otros representantes	0100	1110	0011	1001	$(11)t$
	0001	1011	0110	1100	$(01)^t$
	representantes principales				síndromes

Si se recibe la palabra $y = 1001$ se puede ver en qué lugar está, pero si el arreglo es muy grande, entonces se calcula $S(y)$ y se ve cuál es el representante principal. Para $y = 1001$, $S(y) = Hy^t = (11)^t$. La palabra codificada es, entonces, parecida a 1101 y el mensaje original era 11.

Ejemplo A.9. *Consideremos la función de codificación* $F : F_2^3 \to F_2^6$*:*

000	001	010	100	011	101	110	111
000000	001110	010011	011101	100101	101011	110110	111000

y la matriz generadora $G = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \end{pmatrix}$*. Encontraremos los síndromes y los representantes principales de cada clase lateral. Como* $A \in M_{(n-k)\times k}(F_q)$*,*

$G = \begin{pmatrix} I_k & -A^t \end{pmatrix}$ *generadora* $\iff H = \begin{pmatrix} A & I_{n-k} \end{pmatrix}$ *de control de paridad.*

Se tiene que $H = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$

síndromes	representante principal
$(000)^t$	000000
$(001)^t$	000001
$(010)^t$	000010
$(100)^t$	000100
$(110)^t$	001000
$(011)^t$	010000
$(101)^t$	100000
$(111)^t$	100010

Ejemplo A.10. *Usaremos el ejercicio anterior para enviar un mensaje codificado y si hay error en la transmición, corregiremos ese error.*

Supongamos que el mensaje se ha codificado, usando la siguiente equivalencia:

000	A	001	C	010	E	011	N
100	O	101	R	110	S	111	T

y que ha sido enviado después de aplicar la función de codificación F. Supongamos que el mensaje recibido es

101110 100001 101011 111011 010011 011110 111000

Si no intentamos corregir este mensaje y simplemente leemos los tres primeros dígitos de cada palabra, obtenemos

101 100 101 111 010 011 111

que según lo traducido, queda una palabra sin sentido

$RORTENT$

Pero hemos cometido errores en la trasmisión, pues algunas de las palabras recibidas no son palabras codificadas, luego aplicaremos el proceso de corrección. Los síndromes

de las palabras recibidas se calculan formando los productos Hy^t, donde y recorre las 7 palabras recibidas. Son

$$101 \quad 100 \quad 000 \quad 011 \quad 000 \quad 011 \quad 000$$

Los correspondientes representantes principales son

$$100000 \quad 000100 \quad 000000 \quad 010000 \quad 000000 \quad 010000 \quad 000000$$

El mensaje corregido, obtenido sumando los representantes principales a las correspondientes palabras recibidas es

$$001110 \quad 100101 \quad 101011 \quad 101011 \quad 010011 \quad 01110 \quad 111000$$

Extrayendo los tres dígitos iniciales de cada palabra tenemos

$$001 \quad 100 \quad 101 \quad 101 \quad 010 \quad 001 \quad 111$$

Haciendo la conversión tenemos que el mensaje original era

$$CORRECT$$

Observación A.3. *La corrección de errores se introdujo en el año 1940 a fin de proteger la transmisión de los mensajes.*

Bibliografía

[1] Andrews, G. E. *Number Theory*, Dover Pub, Company, Nueva York, 1971.
[2] Babini, J. *Historia de las Ideas Modernas en Matemática*, OEA Washington, D.C., 1967.
[3] Birkhoff G., MacLane S. *Álgebra Moderna*, Editorial Vicens - Vives, Barcelona, 1963.
[4] Eekhoff, E. T. *Constructibility of Regular Polygons*, Iowa University, Math 599, http://orion.math.iastate.edu/dept/thesisarchive/MSM/EekhoffMSMSS07.pdf
[5] Fraleigh, J. B. *A first course in Abstract Algebra*, Addison Wesley Pub. Company, 1971.
[6] Herstein, I. N. *Álgebra Moderna*, Editorial F. Trillas, S. A. México, 1970.
[7] Humphreys, J. F., Prest M. I. *Numbers, Groups and Codes*, Cambridge University Press, 2004.
[8] Iranzo M.J., Pérez F. *Lecciones Sobre Estructuras Algebraicas*, Departamento de Álgebra, Universidad de Valencia, www.uv.es/iranzo/Estructuras_algebraicas.pdf
[9] Klein, F. *Famous problems of elementary Geometry*, Dover Pub. Company, Nueva York, 1956.
[10] Kleiner, I. *A History of Abstract Algebra*, Birkhäuser Boston, 2007.
[11] Lang, S. *Algebra*, Addison Wesley Pub. Company, 1965.
[12] Lang, S. *Algebraic Structures*, Addison Wesley Pub. Company, 1968.
[13] Lewin, R. A. *Introducción al Álgebra*, J.C. Sáez Editor, Santiago, 2011.
[14] Lidl R., Niederreiter, H. *Introduction to finite fields and their applications*, Cambridge University Press, 1986. Revised Edition, 1994.
[15] Merklen, H. A. *Estructuras Algebraicas V (Teoría de Cuerpos)*, OEA Washington, D.C., 1979.
[16] Pan Collantes, A. J. *Acta de Mathematicas*, Vulgata Vol. 1., Dpto. Mat. Universidad de Cádiz, 2005.
[17] Stewart, I. *Galois Theory*, Chapman and Hall Ltd, Nueva York, 1973.
[18] Van der Waerden, B. L. *Modern Algebra*, Vol. I, Frederick Ungar Pub. Co., Nueva York, 1966.
[19] Weintraub, S. T. *Galois Theory*, Universitex, Springer Science, 2006.

Índice de Términos