

INTRODUCCIÓN AL ÁLGEBRA ABSTRACTA

Juan Francisco Escamilla Castillo

DEPARTAMENTO DE MATEMÁTICAS, CENTRO DE INVESTIGACIONES EN MATEMÁTICAS Y CIENCIAS
NATURALES AFINES, CIMACIEN, GUATEMALA

E-mail address: jescamilla@cimacien.org.gt

URL: www.cimacien.org.gt

A mis hijos Juanito y Fabiola y a mi esposa la Señor Amparo

Mis agradecimientos a mis profesores Artibano Micali y Philippe Revoy, de la universidad de Montpellier, Francia y a los profesores Mario Fiorentini y Antonio Tognoli de la universidad de Ferrara, Italia, quienes me motivaron a profundizar el estudio del álgebra. Van mis agradecimientos también a mi esposa Amparo González y a mis Hijos Fabiola y Juan por su paciencia mostrada durante la elaboración de este libro. En particular quiero agradecer al Lic. William Gutiérrez por su apoyo en la corrección de algunos errores tipográficos, así como a sus observaciones para mejorar la presentación del libro.

Índice general

Índice de figuras	v
PRÓLOGO	vii
INTRODUCCIÓN	1
NOMENCLATURA	6
Capítulo 1. NOCIONES ELEMENTALES DE LA TEORÍA DE CONJUNTOS	7
1.1. Conjuntos y Subconjuntos	7
1.2. Relaciones y Aplicaciones	8
1.3. Familias Indizadas	9
1.4. Ejercicios y Complementos	15
Capítulo 2. ESTRUCTURAS ALGEBRAICAS	17
2.1. Operaciones binarias	17
2.2. Homomorfismos de Estructuras Algebraicas Simples	19
2.3. Estructuras Algebraicas Con Dos Operaciones Binarias	21
2.4. Ω_σ^μ -Estructuras Algebraicas	25
Capítulo 3. NÚMEROS NATURALES, ENTEROS Y RACIONALES	27
3.1. Los Números Naturales	27
3.2. Los Números Enteros	34
3.3. Los Números Racionales	43
Capítulo 4. INTRODUCCIÓN A LA TEORÍA DE GRUPOS	49
4.1. Reseña Histórica	49
4.2. Definición y Propiedades Generales	51
4.3. Homomorfismos de Grupos	65
Capítulo 5. GRUPOS DE PERMUTACIONES Y SIMETRÍA	77
5.1. Aplicaciones a la Geometría y Teoría Musical	93
Capítulo 6. TEOREMAS DE SYLOW, p -GRUPOS y GRUPOS SOLUBLES	101
6.1. Teoremas de Sylow	101
6.2. Grupos Solubles	112
6.3. Sucesiones Normales y Series de Composición	115
Capítulo 7. CLASIFICACIÓN DE LOS GRUPOS ABELIANOS FINITAMENTE GENERADOS	117
7.1. Producto Directo de Subgrupos	117
7.2. Grupos Abelianos Finitamente Generados	119

Capítulo 8. PRODUCTO Y SUMA DIRECTA DE FAMILIA DE GRUPOS. GRUPOS LIBRES	127
8.1. Producto Directo y Suma Directa Sobre Una Familia de Grupos	127
8.2. Grupos Libres	132
Capítulo 9. INTRODUCCIÓN A LA TEORÍA DE ANILLOS E IDEALES	145
9.1. Anillos	145
9.2. Ideales, Homomorfismos, Anillos Cociente y Teorema de Isomorfía	149
9.3. Ideales Primos e Ideales Maximales	157
9.4. Anillos Principales, Noetherianos, de Factorización Única y Euclídeanos	168
Capítulo 10. MÓDULOS Y ÁLGEBRAS	179
10.1. Módulos	179
10.2. Álgebras	187
Capítulo 11. ANILLO Y ÁLGEBRA DE POLINOMIOS	191
11.1. Conceptos y Propiedades Generales	191
11.2. Anillo de Polinomios sobre un Campo	196
11.3. Raíces de Polinomios	209
11.4. Conjuntos Algebraicos y Topología de Zariski	227
Capítulo 12. EXTENSIÓN DE CAMPOS Y TEORÍA DE GALOIS	233
12.1. Extensión de Campos	233
12.2. Teoría de Galois	258
12.3. Construcción con Regla y Compás	291
Bibliografía	305
Índice alfabético	307

Índice de figuras

0.1. Al Jwarizmi	1
0.2. Omar Khayyam	3
0.3. Alejandro de Pisa (Fibonacci)	4
0.4. Nicolo Fontana (Tartaglia)	4
0.5. Girolamo Cardano	5
0.6. Fran�ois Vi�te	5
1.1. Georg Cantor	7
1.2.	14
1.3.	14
3.1. Leopold Kronecker	27
3.2. Giuseppe Peano	28
4.1. Joseph Lagrange	49
4.2. Paolo Ruffini	50
4.3. Camille Jordan	50
4.4. Felix Klein	51
4.5. Niels Abel	51
5.1. Plano xy	94
5.2. Sistema 3-dimensional	95
5.3. Tri�ngulo equil�tero	95
5.4. Cuadrado	96
5.5. Tetraedro Regular	98
5.6. Pent�gono Regular	98
5.7. Hex�gono Regular	99
5.8. Octaedro Regular	99
6.1. Peter Ludwig Mejdell Sylow	101
9.1. Emie Noether	145
11.1Circunferencia	209
11.2Cilindro Circular	209

11.3 $V \subseteq \mathbb{R}^2$	211
11.4 Φ_P	214
11.5 $X^3 - Y^2 = 0$	230
11.6 $Y^2 - X^3 + X = 0$	230
11.7 $X^2 - Y^2 - Z = 0$	231
11.8 $X^4 + (Y^2 - X^2Z^2) = 0$	231
12.1 Évariste Galois	259
12.2 Paralela a recta (AB)	293
12.3 Perpendicular por punto C sobre g	294
12.4 Perpendicular por punto $C \notin g$	294
12.5 Conjugado	295
12.6 $z := re^{i\psi}$	295
12.7 $A := z - w$	296
12.8 Cociente $\frac{z}{w}$	297
12.9 $C := e^{i(\phi-\psi)}$	297
12.10 Raíz cuadrada	298
12.11 $\mathbb{C} := e^{i\frac{\phi}{2}}$	298

PRÓLOGO

En 1980 se inició en la Universidad de San Carlos la carrera de licenciatura en matemática aplicada. Considerando la dificultad que existe en Guatemala de conseguir textos de literatura especializados en temas avanzados de matemáticas y de la escasa existencia de éstos en castellano, me propuse la tarea de escribir un texto introductorio de *álgebra abstracta*. Mi propósito es iniciar al estudiante al estudio de esta interesante y bella rama de las matemáticas, empezando con ejemplos muy sencillos y acrecentando de forma progresiva el grado de dificultad. Una gran variedad de ejercicios y ejemplos geométricos se han incluido, los cuales contribuirán a una mejor comprensión de la teoría. También se incluyen algunos complementos a la teoría en forma de ejercicios para que el estudiante se habitúe a investigar por su cuenta algunos temas.

El primer capítulo es un resumen de los elementos de la teoría de conjuntos necesarios para entender este texto y puede ser obviado si el lector considera tener dichos conocimientos.

En el segundo capítulo trataremos, de forma general, lo que son las estructuras algebraicas. Se introduce la noción de operación binaria y de estructura algebraica simple, la cual consta de un conjunto sobre el cual se ha definido una operación binaria interna cerrada, entre las que se encuentran los *semigrupos*, *monoides* y *grupos*. Se definen también estructuras algebraicas con más de una operación binaria interna y cerrada, de las cuales las más importantes son los *anillos* y *campos*, que son estructuras algebraicas con dos operaciones binarias internas y cerradas que satisfacen ciertas propiedades de *distributividad* entre ellas. Trataremos muy brevemente algunos ejemplos de estructuras algebraicas con más de dos operaciones e incluso con operaciones n -arias. En los capítulos siguientes desarrollaremos los elementos básicos de la teoría de grupos, anillos y extensión de campos.

La primera parte estará dedicada al desarrollo de la teoría de grupos y su clasificación y, particularmente, daremos una clasificación exhaustiva de los grupos abelianos finitamente generados. Terminaremos esta primera parte con una introducción a lo que son los productos directos y amalgamados y las sumas directas y amalgamadas de grupos, así como la construcción de los llamados grupos libres, tanto en el caso abeliano como no abeliano.

En la segunda parte se estudia la teoría de anillos, en particular de anillos conmutativos, campos, extensiones de campos y sus aplicaciones al proceso de radicación para encontrar las raíces de polinomios con coeficientes en un campo dado, culminando con la teoría de Galois, la cual hace uso de la teoría de grupos y relaciona la posibilidad de encontrar las raíces de un polinomio, usando un proceso de radicación, con la solubilidad de un cierto grupo asociado al polinomio, llamado el *grupo de Galois*.

En la tercera parte daremos una breve introducción a lo que es la teoría de categorías y funtores, así como de las llamadas álgebras universales: álgebra tensorial, álgebra de Grassmann, álgebra simétrica y sus propiedades fundamentales.

Los apuntes están diseñados para un curso de dos semestres (las dos primeras partes) para estudiantes de licenciatura en matemática que ya hayan cursado o tengan conocimientos básicos del álgebra superior y de álgebra lineal. La tercera parte está pensada como complemento y materia de estudio para aquellos estudiantes que deseen profundizar más en el estudio del álgebra y de la topología o geometría algebraicas.

Si este texto logra despertar en el estudiante el interés por el estudio del álgebra, en cualquiera de sus especializaciones, habré alcanzado mi objetivo.

Dr. Juan Francisco Escamilla Castillo
Guatemala, 2008

INTRODUCCIÓN



FIGURA 0.1. Al Jwarizmi

El álgebra constituye una de las principales ramas de las matemáticas. En su forma elemental nos enseña el formalismo y las reglas de las operaciones elementales con números y su enseñanza forma parte del currículum básico de la educación secundaria en todos los países. Su campo de aplicación se extiende a todas las ciencias, así como a la vida diaria.

La palabra álgebra deriva de la palabra árabe *al-yebr*, que quiere decir *la reducción* y que aparece en el tratado escrito por el matemático persa *Muhammad ibn Musa al-Jwarizmi*, por el año 820 de nuestra era, titulado *Al-Kitab al-yebr wa-l-Muqabala*, que significa *Compendio de cálculo por el método de reducción y balanceo*, el cual proporcionaba operaciones simbólicas para la solución de ecuaciones lineales y cuadráticas. El nombre de *al-Jwarizmi* ha dado origen a la palabra *algoritmo*, empleado en matemáticas para indicar un método de cálculo específico, como por ejemplo el famoso *algoritmo euclídeano* de la división elemental.

Sin embargo los orígenes del álgebra se remontan, según los historiadores de la matemática, hasta los antiguos babilonios, quienes ya lograron desarrollar un avanzado sistema aritmético con el cual eran capaces de realizar cálculos de tipo algebraico para encontrar soluciones a ecuaciones lineales y cuadráticas. Mientras que los egipcios, indios, chinos y griegos del primer milenio antes de Cristo, usaban más métodos geométricos, tal y como se describen en algunos papiros egipcios, en el *Sulba Sutras* de la India, en *Los Elementos de Euclides* y *Los Nueve capítulos sobre el Arte Matemático* de los chinos.

Sin embargo más tarde los matemáticos indios llegaron a desarrollar métodos algebraicos bastante sofisticados, entre los que destaca *Brahmagupta*, (628 DC.), quien fuera el primero en resolver ecuaciones usando métodos generales, en contraste con los matemáticos griegos como *Diophanto*, (200 DC.), quien en su famosa *Arithmetica* utilizaba

métodos específicos para cada caso, para solucionar ecuaciones con números enteros, conocidas como *ecuaciones diofantinas*. Una de las más famosas de estas ecuaciones es la ecuación $x^n + y^n = z^n$, la cual dió origen a la famosa *conjetura de Fermat*, cuya corroboración llevó a los matemáticos varios siglos y la implementación de métodos algebraicos y geométricos sofisticadísimos.

Tanto Diophanto como Al-Jwarizmi son considerados los padres del álgebra.

A continuación damos un resumen sobre el desarrollo del álgebra desde la antigüedad hasta Galois (1832). [26]

- Alrededor de 1800 AC: *Las Viejas Tablas Babilonias de Strassburg* buscan soluciones de *ecuaciones cuadráticas elípticas*.
- Alrededor de 1600 AC: Las tablas *Plimpton 322* dan una tabla de *tripletas pitagóricas* en escritura cuneiforme babilónica
- Alrededor de 800 AC: El matemático indio *Baudhayana*, en su *Baudhayana Sulba Sjutra*, descubre *tripletas pitagóricas* algebraicamente, encuentra soluciones de ecuaciones lineales y cuadráticas de las formas $ax^2 = c$ y $ax^2 + bx = c$ y encuentra dos conjuntos de posibles soluciones enteras a un conjunto de ecuaciones diofantinas simultáneas.
- Alrededor de 600 AC: El matemático indio *Apastamba*, en su *Apastamba Sulba Sutra*, resuelve la ecuación lineal general y usa sistemas simultáneos de ecuaciones diofantinas hasta de 5 incógnitas.
- Alrededor de 300 AC: en su segundo libro de *Elementos*, *Euclides* da una construcción, usando herramientas euclidianas, (es decir construcciones con regla y compás), de la solución de la ecuación cuadrática con raíces positivas reales. La construcción es debida a la *Escuela Pitagórica de Geometría*. En este período se buscan también construir soluciones para el problema de la duplicación del cubo y ya es conocido el hecho que, en general, dicho problema no puede ser resuelto por métodos euclidianos.
- Alrededor de 100 AC: Ecuaciones algebraicas son tratadas en el libro chino de *Jiuzhang Suanshu* (*Los Nueve Capítulos del Arte Matemático*), se dan soluciones geométricas a la ecuación de segundo grado y soluciones matriciales de sistemas simultáneos de ecuaciones. En este período, también en la antigua India, en el manuscrito conocido por *Bakhshali Manuscript*, ya se usa una notación algebraica que utiliza letras del alfabeto y otros símbolos. También se incluyen soluciones a ecuaciones cúbicas y cuárticas, soluciones algebraicas a sistemas de ecuaciones lineales hasta de cinco incógnitas y la solución general de la ecuación cuadrática.
- Alrededor de 150 DC: *Herón de Alejandría* trata las ecuaciones algebraicas en sus tres volúmenes matemáticos.
- Alrededor de 200 DC: *Diophanto*, considerado uno de los padres del álgebra y que vivió en Egipto, escribe su famosa *Arithmetica*, en el cual da soluciones de ecuaciones algebraicas y trata problemas de la teoría de números.
- Alrededor de 499 DC: El matemático indio *Aryabhata* en su tratado *Aryabhatiya*, obtiene soluciones enteras a ecuaciones lineales, utilizando métodos similares a los actuales.
- Alrededor de 625 DC: El matemático chino *Wang Xiatong*, encuentra soluciones numéricas de la ecuación cúbica.
- Alrededor de 628 DC: El matemático Indio *Brahmagupta*, en su tratado *Brahma Sputa Siddhanta*, inventa el método de la *Chakravala* para resolver ecuaciones

cuadráticas indeterminadas y da algunas reglas para la solución de ecuaciones lineales y cuadráticas.

- Alrededor de 820 DC: El matemático persa *Muhammad ibn Musa al-Jwarizmi*, escribe su famoso tratado *Al-Kitab al-yabr wa-l-Muqabala*, en el cual trata soluciones de ecuaciones lineales y cuadráticas.
- Alrededor de 850 DC: El matemático persa *Al-Mahani* concive la idea de reducir problemas de tipo geométrico, como la duplicación del cubo, a problemas de tipo algebraico. En este período también el matemático indio *Mahavira* resuelve varias ecuaciones cuadráticas, cúbicas, cuárticas, y de grados superiores.
- Alrededor de 990 DC: El matemático persa *Abu Bakr Al-Karaji* en su tratado *Al-Fajri*, continúa desarrollando el álgebra extendiendo los métodos de Al-Jwarizmi a ecuaciones con potencias y raíces enteras de las incógnitas. Reemplaza operaciones de tipo geométrico, utilizadas hasta entonces en el álgebra, por operaciones aritméticas modernas y define las expresiones monomiales x, x^2, \dots , y $\frac{1}{x}, \frac{1}{x^2}, \dots$ y da reglas para el producto de éstos.
- Alrededor de 1050 DC: El matemático chino *Jia Xian* encuentra soluciones numéricas de ecuaciones polinomiales.
- Alrededor de 1072 DC: El matemático persa *Omar Khayyam* desarrolla la geometría algebraica y, en el *Tratado sobre demostración de Problemas de Álgebra*, da una completa clasificación de la ecuación cúbica con solución general geométrica, encontrada por medio de intersección de cónicas.



FIGURA 0.2. Omar Khayyam

- Alrededor de 1114 DC: El matemático indio *Bhaskara*, en su *Bijaganita* (Álgebra), reconoce que todo número positivo posee tanto una raíz cuadrada positiva como una negativa y resuelva varios tipos de ecuaciones cúbicas, cuárticas y de grado superior.
- Alrededor de 1202 DC: *Leonardo de Pisa*, más conocido como *Fibonacci*, introduce en Europa el álgebra, en su trabajo *Liber Abaci*.
- Alrededor de 1300 DC: El matemático chino *Zhu Shijie* trata con álgebra polinomial, resuelve ecuaciones cuadráticas, sistemas de ecuaciones simultáneas hasta de cuatro incógnitas y da soluciones numéricas a algunas ecuaciones de grado cuarto, quinto y de grado superior.



FIGURA 0.3. Alejandro de Pisa (Fibonacci)

- Alrededor de 1400 DC: El matemático indio *Madhava de Sangamagramma* encuentra métodos iterativos para la aproximación de soluciones de ecuaciones no lineales.
- Alrededor de 1450 DC: El matemático árabe *Abu Al-Hasan ibn Ali Al-Qalasadi* toma los primeros pasos hacia la introducción del simbolismo algebraico, representando símbolos matemáticos usando caracteres del alfabeto árabe.
- Alrededor de 1535 DC: *Nicolo Fontana (Tartaglia)* y otros matemáticos italianos, de forma independiente resuelven la ecuación general cúbica.



FIGURA 0.4. Nicolo Fontana (Tartaglia)

- Alrededor de 1545 DC: *Girolamo Cardano* publica en su *Ars Magna (El Gran Arte)* la solución de Tartaglia para la ecuación general de cuarto grado.
- Alrededor de 1572 DC: *Rafael Bombelli* reconoce las raíces complejas de la ecuación cúbica e introduce la actual notación.
- Alrededor de 1591 DC: *François Viète* desarrolla, en su *In Artem Analyticiam Isagogae*, una notación simbólica utilizando vocales para las incógnitas y consonantes para las constantes.
- Alrededor de 1631 DC: *Thomas Harriot*, en una obra póstuma, usa ya la notación exponencial e introduce los símbolos para *menor que* y *mayor que*
- Alrededor de 1682 DC: *Gottfried Wilhelm Leibniz* desarrolla su noción de *manipulación simbólica* con reglas formales que él llama *characteristica generalis*.



FIGURA 0.5. Girolamo Cardano



FIGURA 0.6. François Viète

- Alrededor de 1680 DC: El matemático japonés *Kowa Seki*, en su *Método para Resolver el Problema Disimulado*, descubre el *determinante* y los *números de Bernoulli*.
- Alrededor de 1750 DC: *Gabriel Cramer*, en su tratado *Introducción al Análisis de Curvas Algebraicas*, formula la famosa *fórmula de Cramer* y estudia curvas algebraicas, matrices y determinantes.
- Alrededor de 1824 DC: *Niels Henrik Abel* muestra la insolubilidad, por *radicación*, de la ecuación general de quinto grado.
- Alrededor de 1832 DC: *Évariste Galois* en su trabajo sobre *Álgebra Abstracta*, desarrolla la famosa *Teoría de Galois*

Hasta mediados del siglo XIX los matemáticos se ocupaban de estructuras algebraicas particulares, que involucraban entes concretos, como números, figuras geométricas, permutaciones y funciones y fueron descubriendo, que algunas de las operaciones que se realizaban con estos entes satisfacían ciertas condiciones, como la *cerradura*, *asociatividad*, existencia de *elementos neutros* e *inversos*. Con el surgimiento de la teoría de conjuntos de Cantor y la posibilidad de trabajar con conjuntos cuyos elementos podían ser de cualquier índole bien definida, surge la idea de considerar conjuntos sobre los cuales están definidas una serie de operaciones que se suponen satisfacen ciertas condiciones, las cuales son dadas de forma axiomática y deducir, a partir de los axiomas dados, sus propiedades generales. Así surge la idea de *estructura algebraica* y su estudio es el núcleo de lo que

hoy conocemos como *álgebra abstracta*. Particular interés despertó el estudio de las estructuras algebraicas como los grupos, anillos, campos, módulos y espacios vectoriales y la estructura de álgebra sobre un campo o anillo.

Durante el siglo XX el álgebra abstracta alcanza un gran desarrollo y una gran gama de aplicaciones a diferentes campos de la matemática y de la física teórica, surgiendo nuevas ramas, entre las cuales podemos citar: El *álgebra commutativa*, que estudia las propiedades de los anillos commutativos y constituye la base de la geometría algebraica moderna. El *álgebra homológica* que constituye la herramienta principal de la topología y geometría algebraicas. El *álgebra de Lie*, que estudia estructuras algebraicas definidas sobre variedades diferenciables y exige que todas las operaciones sean diferenciables, de gran aplicación en la geometría y topología diferencial, así como en la física teórica. La mayor abstracción en el estudio de estructuras algebraicas y no algebraicas es alcanzada en la llamada *teoría de categorías*, en la cual se definen los llamados *objetos*, *morfismos* entre objetos y ciertas reglas de composición de morfismos y se estudian las propiedades generales. Así, por ejemplo, la teoría de grupos estudia la categoría cuyos objetos son los *grupos* y sus morfismos los *homomorfismos* de grupos.

Para más información sobre historia de las matemáticas referimos al lector a las siguientes obras [23], [22], [19], [26]

NOMENCLATURA

Los conjuntos los denotaremos por letras mayúsculas A, B, \dots, X, Y, Z . Si X es un conjunto, denotaremos por $\mathcal{P}(X)$ a su *conjunto potencia o boreliano*. Una familia de conjuntos la denotaremos por $\mathcal{A}, \mathcal{B}, \dots, \mathcal{X}, \mathcal{Y}, \mathcal{Z}$. Por $\mathbb{R}, \mathbb{Q}, \mathbb{Z}, \mathbb{N}, \mathbb{C}$ denotaremos los conjuntos de los números reales, racionales, enteros, naturales y complejos respectivamente. La contencción (propia o impropia) la denotaremos por \subseteq y la contención propia por \subset . $A := \dots$ indica que A está siendo definido por \dots . \wedge, \vee , indican la conjunción lógica ‘y’ y la disyunción lógica ‘o’, respectivamente. Por el símbolo $A \approx B$ indicaremos una biyección entre dos conjuntos o bien un isomorfismo entre dos estructuras algebraicas. En cuanto a las referencias de ejercicios o ejemplos, los primeros números indican la serie de ejercicios o ejemplos correspondiente y el último número el número del ejercicio o ejemplo en esa serie. Así, por ejemplo, 7.2.2,3), se refiere al ejercicio 3) de la serie de ejercicios 7.2.2.

CAPÍTULO 1

NOCIONES ELEMENTALES DE LA TEORÍA DE CONJUNTOS



FIGURA 1.1. Georg Cantor

1.1. Conjuntos y Subconjuntos

OBSERVACIÓN. En este capítulo emplearemos el concepto *naive* de conjunto, ya que en este tratado todos los conjuntos son tales que sus objetos están bien definidos y que siempre es posible decir, sin ambigüedad, si un elemento está o no en dicho conjunto.

DEFINICIÓN 1.1. Llamaremos *conjunto* a una colección S de objetos bien definidos, llamados *puntos*.

Si x es un elemento de S , escribiremos $x \in S$, y $x \notin S$ si x no está en S . Por U designaremos al conjunto *universo*, al cual pertenecen los puntos en cuestión. Si P es una proposición, $S := \{x \in U \mid P(x)\}$ es el conjunto de todos los elementos de U para los cuales la proposición P es verdadera.

DEFINICIÓN 1.2. Por \emptyset denotaremos al *conjunto vacío* que no posee ningún elemento, lógicamente se puede poner $\emptyset := \{x \in U \mid x \neq x\}$.

DEFINICIÓN 1.3. Dados dos conjuntos A y B , decimos que:

1. A es un *subconjunto* de B , ($A \subseteq B$) Ssi: $x \in A \Rightarrow x \in B$, $\forall x \in A$
2. $A = B$ Ssi: $A \subseteq B$, y $B \subseteq A$
3. A es *subconjunto propio* de B , ($A \subset B$) Ssi A es subconjunto de B y $A \neq B$

DEFINICIÓN 1.4. Dados dos conjuntos A y B

1. Al conjunto $A \cup B := \{x \mid x \in A \vee x \in B\}$ lo llamamos la *unión* del conjunto A con el conjunto B .

2. Al conjunto $A \cap B := \{x \mid x \in A \wedge x \in B\}$ lo llamamos la *intersección* del conjunto A con el conjunto B .
3. Al conjunto de pares ordenados $A \times B := \{(a, b) \mid a \in A \wedge b \in B\}$ lo llamamos el *producto cartesiano* del conjunto A con el conjunto B .
4. Al conjunto $A \setminus B := \{x \mid x \in A \wedge x \notin B\}$ lo llamamos la *diferencia* del conjunto A con el conjunto B o *complemento relativo* de B respecto de A .
5. Al conjunto $A \Delta B := (A \setminus B) \cup (B \setminus A)$ lo llamamos la *diferencia simétrica* del conjunto A con el conjunto B .

DEFINICIÓN 1.5. Sea A subconjunto de un conjunto universo U

1. Al conjunto $A^c := \{x \in U \mid x \notin A\}$ lo llamamos el *complemento* del conjunto A .
2. El conjunto $\mathcal{P}(U) := \{A \mid A \subseteq U\}$ se llama el *conjunto potencia* o *boreleano* de U .
3. A un subconjunto $\mathcal{A} \subseteq \mathcal{P}(U)$ lo llamamos una *familia de conjuntos*.

Leyes de de Morgan.

TEOREMA 1.1. *Dados dos conjuntos A y B entonces vale:*

1. $(A \cup B)^c = A^c \cap B^c$
2. $(A \cap B)^c = A^c \cup B^c$

1.2. Relaciones y Aplicaciones

Por lo que sigue supondremos que todo conjunto es subconjunto de un universo U .

DEFINICIÓN 1.6. Sean A y B dos conjuntos

1. Un subconjunto $\mathcal{R} \subseteq A \times B$ se llama una *relación* de A en B . Si $\forall a \in A \exists! b \in B$ tal que $(a, b) \in \mathcal{R}$ entonces se dice que A es el *dominio* de la relación \mathcal{R} y el conjunto $\{b \in B \mid (a, b) \in \mathcal{R}\}$ el *contradominio* o *rango* de \mathcal{R} y lo denotamos por $\text{Rang}(\mathcal{R})$.
2. \mathcal{R} es una relación *sobre* B si $\text{Rang}(\mathcal{R}) = B$.
3. Si \mathcal{R} es una relación de A en B , entonces $\mathcal{R}^{-1} := \{(b, a) \in B \times A \mid (a, b) \in \mathcal{R}\}$ es una relación de B en A , llamada la *inversa* de \mathcal{R} .

DEFINICIÓN 1.7. Dados dos conjuntos A y B

1. Decimos que una relación f de A en B es una *aplicación* de A en B , $f : A \rightarrow B$, si $\forall a \in A \exists! b \in B$ tal que $(a, b) \in f$ ($\exists!$ denota existe un único). Entonces decimos que b es la *imagen* de a y escribimos $f(a) := b$ al rango de f lo denotaremos por $f[A]$ y lo llamaremos la *imagen* de A .
2. Se dice que la aplicación $f : A \rightarrow B$ es *sobreyectiva* si $f[A] = B$. Si $f(a) = f(b) \Rightarrow a = b$ entonces se dice que f es *inyectiva* o una *inyección*. Si f es inyectiva y sobreyectiva entonces se dice que f es *biyectiva* o una *biyección*.
3. Si $f : A \rightarrow B$ es una aplicación y $C \subseteq A$ entonces la *restricción* de f a C , $f|_C : C \rightarrow B$ está definida por $f|_C(x) := f(x)$, $\forall x \in C$.
4. Si $f : A \rightarrow B$ es una aplicación y $C \subseteq A$, entonces al conjunto $f^{-1}[C] := \{x \in A \mid f(x) \in C\}$ lo llamamos la *contraimagen* o *imagen inversa* de C bajo f .

DEFINICIÓN 1.8. Sean A , B , C conjuntos y $f : A \rightarrow B$, $g : B \rightarrow C$ aplicaciones, entonces la *composición* $g \circ f : A \rightarrow C$ es la aplicación definida por $g \circ f(x) := g(f(x))$, $\forall x \in A$.

El siguiente teorema, cuya demostración se deja al lector como ejercicio nos resume las principales propiedades de las aplicaciones:

TEOREMA 1.2. *Dadas las aplicaciones $f : X \rightarrow Y$, $g : Y \rightarrow Z$, entonces:*

- a) $f[A \cap B] \subseteq f[A] \cap f[B]$. $\forall A, B \subseteq X$
- b) $f[A \cup B] = f[A] \cup f[B]$
- c) $f^{-1}[U \cap V] = f^{-1}[U] \cap f^{-1}[V]$, $\forall U, V \subseteq Y$
- d) $f^{-1}[U \cup V] = f^{-1}[U] \cup f^{-1}[V]$, $\forall U, V \subseteq Y$
- e) $f^{-1}[U \setminus V] = f^{-1}[U] \setminus f^{-1}[V]$, $\forall U, V \subseteq Y$
- f) $A \subseteq f^{-1}[f[A]]$, $\forall A \subseteq X$. Si f inyectiva, entonces $f^{-1}[f[A]] = A$
- g) $f[f^{-1}[U]] \subseteq U$, $\forall U \subseteq Y$. Si f sobreyectiva, entonces $f[f^{-1}[U]] = U$
- h) $(g \circ f)^{-1}[W] = f^{-1}[g^{-1}[W]]$, $\forall W \subseteq Z$

1.3. Familias Indizadas

DEFINICIÓN 1.9. Sean I un conjunto no vacío, $\mathcal{A} \subseteq \mathcal{P}(U)$ una familia. A una aplicación $\varphi : I \rightarrow \mathcal{A}$ la llamamos una *indización* de \mathcal{A} por I . El conjunto I se denomina el *conjunto de índices*. Para $i \in I$ escribiremos $\varphi(i) = A_i \in \mathcal{A}$. Entonces a la familia $\{A_i\}_{i \in I}$ la llamaremos una *familia indizada* por I .

EJEMPLO 1.1. Sean $I := \{1, 2, 3, 4, 5\}$, $\mathcal{A} := \{\{a, b\}, \{c, d\}, \{1, 2\}, \{3, 4\}, \{5, 6\}\}$, $\varphi : I \rightarrow \mathcal{A}$, dada por

- $\varphi(1) = A_1 := \{a, b\}$
- $\varphi(2) = A_2 := \{c, d\}$
- $\varphi(3) = A_3 := \{1, 2\}$
- $\varphi(4) = A_4 := \{3, 4\}$
- $\varphi(5) = A_5 := \{5, 6\}$

$$\{A_i\}_{i \in I} = \{A_1, A_2, A_3, A_4, A_5\}$$

La familia \mathcal{A} puede también ser indizada por ella misma en una forma natural: $\varphi(A) := A$, $\forall A \in \mathcal{A}$, llamada la *indización natural*.

1.3.1. Unión e Intersección de Familias Indizadas. Dada una familia indizada $\{A_i\}_{i \in I}$, entonces definimos:

$$\begin{aligned} \bigcup_{i \in I} A_i &:= \{x \mid \exists i \in I, x \in A_i\} \\ \bigcap_{i \in I} A_i &:= \{x \mid x \in A_i, \forall i \in I\}. \end{aligned}$$

El siguiente teorema nos generaliza las leyes de Morgan enunciadas en teorema 1.1:

TEOREMA 1.3. *Dada una familia indizada $\{A_i\}_{i \in I}$, entonces se tiene:*

1. $(\bigcup_{i \in I} A_i)^c = \bigcap_{i \in I} A_i^c$
2. $(\bigcap_{i \in I} A_i)^c = \bigcup_{i \in I} A_i^c$

DEMOSTRACIÓN. Demostraremos 1. y dejaremos al lector la demostración de 2. como ejercicio.

$$\begin{aligned} 1. \quad x \in (\bigcup_{i \in I} A_i)^c &\Leftrightarrow x \notin \bigcup_{i \in I} A_i \\ &\Leftrightarrow x \notin A_i, \forall i \in I \Leftrightarrow x \in \bigcap_{i \in I} A_i^c \\ &\text{por consiguiente } (\bigcup_{i \in I} A_i)^c = \bigcap_{i \in I} A_i^c \end{aligned}$$

□

1.3.2. Conjuntos Finitos e Infinitos.

DEFINICIÓN 1.10. Dado un conjunto S , entonces se tiene:

1. S es un conjunto *finito* si existe $n \in \mathbb{N}$ y una biyección $f : \{1, \dots, n\} \rightarrow S$
2. S es un conjunto *infinito* si existe una biyección entre S y un subconjunto propio de S
3. S es un conjunto *denumerable* si existe una biyección entre \mathbb{N} y S .
4. Se dice que dos conjuntos son *equipotentes* o que poseen la misma *cardinalidad* si existe una biyección entre ellos.
5. Un conjunto es *contable* si es finito o denumerable.

EJEMPLOS 1.2.

1. El conjunto \mathbb{N} de los números naturales es infinito, ya que $f(n) := 2n$ es una biyección entre \mathbb{N} y el subconjunto propio de los números pares. \mathbb{N} es obviamente denumerable. La cardinalidad de cualquier conjunto denumerable se denota por \aleph_0 , (alef sub 0, primera letra del alfabeto hebreo)
2. $f : \mathbb{N} \rightarrow \mathbb{Z}$ definida por

$$f(n) := \begin{cases} \frac{n}{2} & \text{si } n \text{ par} \\ \frac{-(n+1)}{2} & \text{si } n \text{ es impar} \end{cases}$$

es una biyección entre \mathbb{N} y \mathbb{Z} . Por lo que \mathbb{Z} es contable.

3. El conjunto \mathbb{R} de los números reales es “no contable”. Para demostrar esto basta con mostrar que el intervalo $I := [0, 1]$ no es contable. En efecto, supongamos que I fuera contable, entonces $I = \{x_1, x_2, \dots, x_n, \dots\}$, donde cada uno de los x_n posee una expansión decimal única no finita: $x_n = 0.a_{n1} \dots, a_{nn}, \dots$ consideremos el número $y := 0.a_{11} \dots a_{nn} \dots$ y formemos $z := 0.b_1 \dots b_n$, $b_n \neq 0$, $b_n \neq a_{nn}$, $\forall n \in \mathbb{N}$, entonces $z \neq x_n$, $\forall n \in \mathbb{N}$, $z \in I$, pero z no aparece en el conteo. Por lo tanto I no es contable y por consiguiente tampoco \mathbb{R} .

Se puede demostrar que la cardinalidad de \mathbb{R} es la misma que la del intervalo I . La cardinalidad de \mathbb{R} se suele denotar por c o por \aleph_1 y se llama la *cardinalidad del continuo*.. Así mismo se puede demostrar que \mathbb{R} y $\mathcal{P}(\mathbb{N})$ poseen la misma cardinalidad. Uno de los resultados de la teoría de conjuntos es que la cardinalidad de un conjunto S es siempre estrictamente menor que la cardinalidad de su conjunto potencia. Para un conjunto finito de n elementos se ve fácilmente que la cardinalidad de su conjunto potencia es 2^n , así se define entonces $\aleph_n := 2^{\aleph_{n-1}}$, $n = 1, 2, \dots$. Durante mucho tiempo se planteó el problema de demostrar que no existe ninguna cardinalidad entre \aleph_0 y \aleph_1 , la llamada *hipótesis del continuo*. No fue sino hasta hace algunos años que P.J. Cohen [6] demostró que la validez o invalidez de dicha hipótesis no es demostrable con los axiomas de la teoría de conjuntos..

1.3.3. Producto Cartesiano Sobre una Familia Indizada.

DEFINICIÓN 1.11. Sea $\{A_i\}$ una familia indizada. Llamamos *producto cartesiano sobre I* al conjunto: $\prod_{i \in I} A_i := \{x | x : I \rightarrow \bigcup_{i \in I} A_i, \text{ con } x(i) \in A_i, \forall i \in I\}$. En lugar de escribir $x(i) \in A_i$ se suele escribir $x_i \in A_i$. Si $x \in \prod_{i \in I} A_i$, entonces escribiremos $x := (x_i)$. A la aplicación $p_k : \prod_{i \in I} A_i \rightarrow A_k$, $k \in I$ definida por $p_k(x) := x_k \in A_k$, la llamamos la *k-proyección* sobre A_k , $k \in I$.

En el caso en que I es un conjunto finito de índices esta definición coincide con la definición dada en 1.4.

EJEMPLO 1.3. Sea $I = \{1, 2\}$ y consideremos la familia indizada $\{A_1, A_2\}$, entonces $A_1 \times A_2 = \{x|x : \{1, 2\} \rightarrow A_1 \cup A_2, x_1 \in A_1, x_2 \in A_2\}$, por lo que podemos identificar x con el par ordenado (x_1, x_2) .

La existencia del producto cartesiano está garantizada por el llamado *axioma de selección de Zermelo*.

AXIOMA (Axioma de Selección). *Sea $\{A_i\}$ una familia de conjuntos no vacíos. Entonces existe una aplicación $\varphi : I \rightarrow \bigcup_{i \in I} A_i$, tal que $\varphi(i) \in A_i, \forall i \in I$. La aplicación φ se llama una aplicación de selección. Esto quiere decir que podemos formar un conjunto que esté formado por un elemento de cada uno de los A_i .*

Cohen demostró que este axioma es independiente de los demás axiomas de la teoría de conjuntos de Zermelo-Fraenkel y además que dicho axioma, el teorema del buen ordenamiento y el lema de Zorn (ver teoremas 1.6 y 1.7) son equivalentes.

1.3.4. Relaciones de Equivalencia y de Orden.

DEFINICIÓN 1.12. Sea A un conjunto no vacío, $A \times A$ el producto cartesiano de A consigo mismo y sea $\mathcal{R} \subseteq A \times A$ una relación de A en A .

1. Al subconjunto $\Delta := \{(x, x) | x \in A\}$ lo llamamos la *diagonal* de $A \times A$.
2. Decimos que \mathcal{R} es *reflexiva* si $\Delta \subseteq \mathcal{R}$
3. \mathcal{R} es *transitiva* si $(x, y) \wedge (y, z) \in \mathcal{R} \Rightarrow (x, z) \in \mathcal{R}$
4. \mathcal{R} es *simétrica* si $(x, y) \in \mathcal{R} \Rightarrow (y, x) \in \mathcal{R}$.
5. \mathcal{R} es *antisimétrica* si $(x, y) \wedge (y, x) \in \mathcal{R} \Rightarrow x = y$.

DEFINICIÓN 1.13. Sea $\mathcal{R} \subseteq A \times A$ una relación de A en A .

1. Decimos que \mathcal{R} es una *relación de equivalencia* sobre A si \mathcal{R} es reflexiva, simétrica y transitiva.
2. Si $x \in A$, al conjunto $[x] := \{y \in A | (x, y) \in \mathcal{R}\}$ lo llamamos la *\mathcal{R} -clase de equivalencia* de x .

DEFINICIÓN 1.14. Decimos que una familia $\mathcal{P} \subseteq \mathcal{P}(A)$ es una *partición* del conjunto A si:

- a) $\bigcup_{P \in \mathcal{P}} P = A$
- b) Si $P, Q \in \mathcal{P}$, entonces $P \cap Q = \emptyset$, o $P = Q$.

TEOREMA 1.4. Si \mathcal{R} es una relación de equivalencia sobre el conjunto A y $P_x := [x]$, entonces la familia $\mathcal{P} := \{P_x\}_{x \in A}$ es una partición de A

DEMOSTRACIÓN. Como $\Delta \subseteq \mathcal{R}$, $\forall x \in A$ $x \in P_x$, por consiguiente $\bigcup_{x \in A} P_x = A$. Por otra parte si $z \in P_x \cap P_y$, entonces $(x, z) \wedge (y, z) \in \mathcal{R}$, como \mathcal{R} simétrica $(z, y) \in \mathcal{R}$ y por la transitividad de \mathcal{R} resulta que $(x, y) \in \mathcal{R}$, por lo tanto $P_x = P_y$. \square

DEFINICIÓN 1.15. Sea \mathcal{R} una relación de equivalencia sobre el conjunto A

1. Al conjunto $A/\mathcal{R} := \{[x] | x \in A\}$ lo llamamos el *conjunto cociente* de A sobre \mathcal{R} .

2. La aplicación $\pi : A \rightarrow A/\mathcal{R}$, definida por $\pi(x) := [x]$ se llama la *proyección canónica* o *aplicación de identificación*, la cual identifica a todos los elementos que son equivalentes entre sí a un único elemento en A/\mathcal{R} y es obviamente sobreyectiva.

EJEMPLO 1.4. Sea \mathbb{Z} el conjunto de los números enteros, para $p \in \mathbb{Z}$, $p\mathbb{Z} := \{px | x \in \mathbb{Z}\}$, dados $n, m \in \mathbb{Z}$ decimos que n es *congruente* con m $(\text{mód } p)$ ($m \equiv n \pmod{p}$), si $(n - m) \in p\mathbb{Z}$. Entonces la relación definida por $\mathcal{R} := \{(m, n) | m \equiv n \pmod{p}\}$ es una relación de equivalencia sobre \mathbb{Z} . Sólo existen p clases distintas: $[0], [1], \dots, [p - 1]$, llamadas *clases de congruencia* $(\text{mód } p)$. Entonces $\mathbb{Z}/\mathcal{R} := \{[0], [1], \dots, [p - 1]\}$ es el conjunto cociente.

DEFINICIÓN 1.16. Sean X, Y, Z tres conjuntos y $f : X \rightarrow Z$, $g : Z \rightarrow Y$, $h : X \rightarrow Y$ aplicaciones, decimos que el diagrama

$$\begin{array}{ccc} X & \xrightarrow{h} & Y \\ f \downarrow & \nearrow g & \\ Z & & \end{array}$$

es *comutativo* si $h = g \circ f$.

En forma análoga se dice que el diagrama de aplicaciones entre conjuntos

$$\begin{array}{ccc} X & \xrightarrow{f} & Y \\ g \downarrow & & \downarrow h \\ Z & \xrightarrow{j} & W \end{array}$$

es *comutativo* si $h \circ f = j \circ g$

OBSERVACIÓN 1.1. El estudio de los diagramas comutativos es de suma importancia en el álgebra moderna y la topología y geometría algebraicas. En particular son el tema de estudio en la llamada *teoría de categorías*.

El teorema que daremos ahora es muy importante en el álgebra y recibe el nombre de *teorema de factorización*.

TEOREMA 1.5 (Teorema de factorización). *Sea $f : X \rightarrow Y$ una aplicación y sea $\mathcal{R}_f := \{(x, y) \in X \times X | f(x) = f(y)\}$, entonces*

- a) \mathcal{R}_f es una relación de equivalencia sobre X .
- b) Existe una única aplicación $\bar{f} : X/\mathcal{R}_f \rightarrow Y$, tal que el diagrama

$$\begin{array}{ccc} X & \xrightarrow{f} & Y \\ \pi \downarrow & \nearrow \bar{f} & \\ X/\mathcal{R}_f & & \end{array}$$

es comutativo. Además \bar{f} es inyectiva y si f es sobreyectiva, entonces \bar{f} es una biyección.

DEMOSTRACIÓN. Demostraremos únicamente el inciso b), dejando al lector la demostración de a).

En efecto, la aplicación $\bar{f} : X/\mathcal{R}_f \rightarrow Y$, definida por $\bar{f}([x]) := f(x)$ hace commutar al diagrama. Para mostrar que \bar{f} está bien definida, debemos mostrar que \bar{f} no depende del

representante escogido. En efecto, para $y \in [x]$, $[y] = [x]$, $\bar{f}([y]) = f(y) = f(x) = \bar{f}([x])$, por lo que \bar{f} está bien definida y es la única que hace commutar al diagrama. \bar{f} es inyectiva, ya que $[x] \neq [y] \Rightarrow \bar{f}([x]) = f(x) \neq f(y) = \bar{f}([y])$. Si f es sobreyectiva también lo es \bar{f} , ya que $\forall z \in Y \exists x \in X$, tal que $f(x) = z$, por lo tanto $\bar{f}([x]) = z$. \square

1.3.5. Relaciones de Orden y Conjuntos Ordenados.

DEFINICIÓN 1.17. Sea A un conjunto no vacío y $\leq \subseteq A \times A$ una relación sobre A . Decimos que \leq es una *relación de orden parcial* sobre A si \leq es reflexiva, transitiva y antisimétrica. Al par (A, \leq) , donde \leq es una relación de orden parcial, lo llamamos un conjunto parcialmente ordenado. Si $(x, y) \in \leq$ escribiremos $x \leq y$. Si $\forall x, y \in A$, $x \leq y$ o $y \leq x$ entonces se dice que \leq es una *relación de orden total* y que (A, \leq) es un *conjunto totalmente ordenado*.

DEFINICIÓN 1.18. Sea (A, \leq) un conjunto parcialmente ordenado y $B \subseteq A$

1. $t \in A$ es una *cota superior* de B , si $x \leq t$, $\forall x \in B$
2. $m \in B$ es un elemento *maximal* o *máximo* de B , si $\forall x \in B$, $m \leq x \Rightarrow m = x$
3. $g \in B$ es el *elemento más grande* de B , si $x \leq g$, $\forall x \in B$.
4. Decimos que una cota superior s de B es el *supremo* de B , si para cualquier otra cota superior r de B , $s \leq r$. Entonces escribiremos $\sup B := s$

En forma análoga, invirtiendo la relación, se definen los conceptos de *cota inferior*, *elemento minimal* o *mínimo*, *elemento más pequeño* e *ínfimo* ($\inf B$ de un conjunto B).

Es de notar que elementos maximales (minimales), si existen, pueden haber varios, mientras que un elemento más grande (más pequeño), si existe, es único. El elemento más grande (más pequeño) es a su vez un elemento maximal (minimal), pero no al revés.

EJEMPLO 1.5. $A := \{a, b, c, d\}$, $\leq := \{(a, b), (b, c), (a, c)\} \cup \Delta$. El lector verificará fácilmente que ésta es una relación de orden parcial sobre A . Sean $B := \{a, b, d\}$, $D := \{a, b, c\}$, entonces b, d son elementos maximales de B , pero B no posee elemento más grande ni elemento más pequeño. En cambio D si posee elemento más grande que es c y elemento más pequeño que es a .

DEFINICIÓN 1.19.

1. Decimos que (A, \leq) está *bien ordenado* si cada subconjunto no vacío de A posee un elemento más pequeño.
2. Decimos que (A, \leq) está *inductivamente ordenado*, si cada subconjunto no vacío de A totalmente ordenado posee una cota superior.

OBSERVACIÓN 1.2. En un conjunto totalmente ordenado coincide el elemento maximal (minimal), en caso de que exista, con el elemento más grande (más pequeño).

A continuación enunciaremos, sin demostración, dos teoremas de suma importancia en la teoría de conjuntos y en la matemática moderna: el *lema de Zorn* y el *teorema del buen ordenamiento*. Ver, por ejemplo, [11], [24].

TEOREMA 1.6 (Lema de Zorn). *Todo conjunto no vacío inductivamente ordenado posee un elemento maximal (minimal).*

TEOREMA 1.7 (Teorema del buen ordenamiento). *Todo conjunto puede ser bien ordenado.*

Si (A, \leq) es un conjunto finito parcialmente ordenado, \leq se suele representar por medio de un “grafo”, donde los puntos que están relacionados aparecen unidos por una flecha.

EJEMPLO 1.6. Sea $A := \{a, b, c, d, e\}$, entonces la relación $\leq := \{(d, c), (c, a), (d, a), (e, c), (c, b), (e, b), (e, a)\} \cup \Delta$ se puede representar por el grafo:

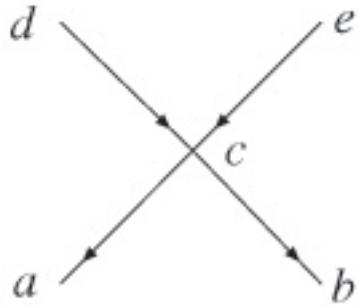


FIGURA 1.2

DEFINICIÓN 1.20. Un conjunto parcialmente ordenado (L, \leq) es una *red*, si $\forall a, b \in L$, $\{a, b\}$ posee un ínfimo $a \cdot b \in L$ y un supremo $(a + b) \in L$.

EJEMPLO 1.7. Sea $L := \{a, b, c, d, e\}$, \leq sea la relación dada por el grafo:

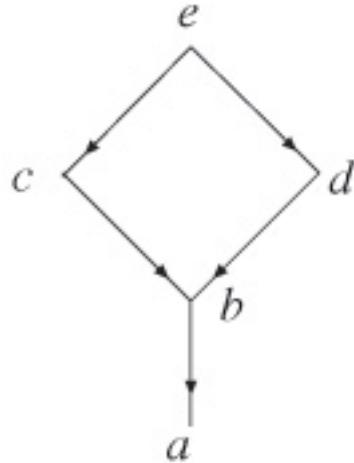


FIGURA 1.3

Entonces (L, \leq) es una red, mientras que (A, \leq) en el ejemplo precedente no es una red.

DEFINICIÓN 1.21. Sea (S, \leq) un conjunto parcialmente ordenado, $A \subseteq S$ un subconjunto no vacío

1. $\leq|_A := \leq \cap A \times A$ es el *orden inducido por* \leq sobre A .
2. $(A, \leq|_A)$ es una *cadena* en S , si $(A, \leq|_A)$ es totalmente ordenado.

DEFINICIÓN 1.22. Sea (L, \leq) una red con elemento más pequeño que denotaremos por 0 y elemento más grande que denotaremos por 1.

1. Se dice que (L, \leq) es *complementada* si $\forall a \in L, \exists x \in L$, tal que $a + x = 1 \wedge a \cdot x = 0$, x se llama el *complemento* de a .
2. Se dice que la red (L, \leq) es *distributiva* si $(a + b) \cdot c = a \cdot c + b \cdot c$, $\forall a, b, c \in L$.
3. Una red (L, \leq) distributiva y complementada se denomina un *álgebra de Boole o booleana*.

1.4. Ejercicios y Complementos

1. Demostrar las leyes de Morgan enunciadas en los teoremas 1.1, y 1.3.
2. Probar que la relación definida sobre \mathbb{Z} en el ejemplo 1.4 es una relación de equivalencia.
3. Definir sobre $A := \{a, b, c, d, e\}$ una relación de equivalencia \mathcal{R} y dar las clases de equivalencia para cada $x \in A$, así como el conjunto cociente A/\mathcal{R} .
4. Sea A un conjunto no vacío y \mathcal{P} una partición de A . Mostrar que la relación \sim , definida por $x \sim y \Leftrightarrow \exists P \in \mathcal{P}$, tal que $x, y \in P$, es una relación de equivalencia sobre A y su conjunto cociente es precisamente \mathcal{P} .
5. Sean $n, m \in \mathbb{Z}^+$, donde \mathbb{Z}^+ es el conjunto de los enteros positivos mayores que 0, decimos que $n \mid m$ (n divide a m) si existe $q \in \mathbb{Z}^+$, tal que $m = qn$. Mostrar que $\leq := \{(n, m) \in \mathbb{Z}^+ \times \mathbb{Z}^+ \mid n \mid m\}$ es una relación de orden sobre \mathbb{Z}^+ . Investigar además si (\mathbb{Z}^+, \leq) es totalmente ordenado, bien ordenado o inductivamente ordenado.
6. Se dice que un conjunto \mathcal{U} es *universal*, si:
 - a) Si $X \in \mathcal{U} \Rightarrow X \subseteq \mathcal{U}$.
 - b) Si $X \in \mathcal{U} \Rightarrow \mathcal{P}(X) \in \mathcal{U}$
 - c) Si $X, Y \in \mathcal{U} \Rightarrow \{X, Y\} \in \mathcal{U}$
 - d) Si $\mathcal{F} := \{F_i\}_{i \in I}$, $F_i \in \mathcal{U}$, $I \in \mathcal{U}$, entonces $\bigcup_{i \in I} F_i \in \mathcal{U}$.

Sea \mathcal{U} un conjunto universal, con $\emptyset \in \mathcal{U}$. Decimos que $\mathcal{N} \subseteq \mathcal{U}$ es un *numeral*, si $\emptyset \in \mathcal{N}$ y si $X \in \mathcal{N} \Rightarrow X \cup \{X\} \in \mathcal{N}$, mostrar que \mathcal{U} es un numeral.

7. Sea \mathcal{U} un conjunto universal con $\emptyset \in \mathcal{U}$. Si \mathbb{N} es la intersección de todos los subconjuntos numerales de \mathcal{U} , entonces \mathbb{N} es también un subconjunto numeral y se llama el *conjunto de los números naturales*.
8. Si $x \in \mathbb{N}$, $x' := x \cup \{x\}$ se llama el *sucesor* de x . Demostrar que \mathbb{N} posee las siguientes propiedades:
 - a) $\emptyset \in \mathbb{N}$
 - b) Si $x \in \mathbb{N} \Rightarrow x' \in \mathbb{N}$
 - c) Cualquier subconjunto de \mathbb{N} que satisface a) y b), coincide con \mathbb{N} (principio de inducción).
 - d) Si $x \in \mathbb{N}$, $x' \neq \emptyset$, además $x \in y \Rightarrow x \subseteq y$
 - e) $x' \subseteq y' \Rightarrow x \subseteq y$
 - f) $x' = y' \Rightarrow x = y$

Las propiedades a)-f) caracterizan totalmente a \mathbb{N} y reciben el nombre de *axiomas de Peano*. Algunos textos introducen al conjunto de los naturales utilizando estos axiomas. Un número natural es entonces un elemento de \mathbb{N} y lo designamos de la siguiente forma:

$$0 := \emptyset, 1 := 0' = \{\emptyset\}, 2 := 1' = \{\emptyset, \{\emptyset\}\}, 3 := 2' = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}, \dots$$

9. Dados dos conjuntos A, B , y una aplicación $f : A \rightarrow B$, demostrar que la relación \mathcal{R}_f , definida en el teorema 1.5, es una relación de equivalencia.
10. Definir los conceptos de mínimo, elemento más pequeño, cota inferior e ínfimo en un conjunto parcialmente ordenado (ver definición 1.18).

11. Mostrar que $\leq|_A$, definida en definición 1.21-1) es una relación de orden sobre A .
12. Sea $S \neq \emptyset$ y $(\mathcal{P}(S), \leq)$, donde $\leq := \{(A, B) \in \mathcal{P}(S) \times \mathcal{P}(S) | A \subseteq B\}$
 - a) Desmostrar que \leq es una relación de orden sobre $\mathcal{P}(S)$
 - b) Si $A, B \in \mathcal{P}(S)$, $A \cdot B := A \cap B$, $A + B := A \cup B$, mostrar que $(\mathcal{P}(S), \leq)$ es un álgebra de Boole.
13. Sea \mathcal{P} el conjunto de todas las proposiciones decidibles, es decir que son verdaderas o falsas en sentido exclusivo. Definimos: $p \leq q$ Ssi $p \Rightarrow q$,
 $p \cdot q := p \wedge q$, $p + q := p \vee q$, $\forall p, q \in \mathcal{P}$. Mostrar que (\mathcal{P}, \leq) es una red distributiva. (\mathcal{P}, \leq) es además isomorfa a un álgebra de Boole de dos elementos $\{0, 1\}$, por eso recibe el nombre de lógica bivalente.
14. Sea (A, \leq) un conjunto parcialmente ordenado. Se dice que (A, \leq) satisface la *condición del mínimo* si todo subconjunto no vacío de A posee un elemento minimal. Mostrar que si (A, \leq) posee la propiedad del mínimo y si B es un subconjunto de A que tiene la propiedad de que cualquier elemento $a \in A$ está en B siempre que B contiene a todos los elementos $x \in A$, $x < a$, entonces $B = A$. (Ayuda: hacer ver que B^c no posee ningún elemento minimal y por consiguiente debe ser \emptyset) Este resultado es conocido como el *principio de inducción Noetheriana*. Si (A, \leq) está además bien ordenado, este principio se conoce con el nombre de *inducción transfinita*.

CAPÍTULO 2

ESTRUCTURAS ALGEBRAICAS

En este capítulo estudiaremos el concepto general de estructura algebraica. Empezaremos definiendo el concepto de operación binaria y de estructuras algebraicas con dicho tipo de operaciones y luego extenderemos el concepto de operación binaria a operaciones n -arias y daremos algunos ejemplos de dichas estructuras.

2.1. Operaciones binarias

DEFINICIÓN 2.1. Dados tres conjuntos A , B , y C , a una aplicación $* : A \times B \rightarrow C$, tal que $*(a, b) := a * b \in C$, $\forall (a, b) \in A \times B$, la llamaremos una *operación binaria* de elementos de A con elementos de B en C .

EJEMPLO 2.1. Consideremos los conjuntos \mathbb{Z} , \mathbb{R} y \mathbb{C} de los números enteros, reales y complejos respectivamente y la operación $* : \mathbb{Z} \times \mathbb{R} \rightarrow \mathbb{C}$, definida por $n * r := nr + inr \in \mathbb{C}$, $\forall (n, r) \in \mathbb{Z} \times \mathbb{R}$.

En el caso particular en que $A = B$ diremos que $* : A \times A \rightarrow C$ es una *operación binaria interna* y si $A = B = C$, entonces diremos que $* : A \times A \rightarrow A$ es una *operación binaria interna cerrada*.

EJEMPLOS 2.2.

1. El producto interno sobre el \mathbb{R}^2 , definido por $\cdot : \mathbb{R}^2 \times \mathbb{R}^2 \rightarrow \mathbb{R}$, $(a, b) \cdot (c, d) := ac + bd \in \mathbb{R}$, $\forall (a, b), (c, d) \in \mathbb{R}^2$, es una operación binaria interna
2. La suma usual de enteros: $+ : \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}$, es una operación binaria interna y cerrada.

DEFINICIÓN 2.2. Llamamos *estructura algebraica binaria simple* a un par ordenado $(A, *)$, donde A es un conjunto no vacío y $*$ es una operación binaria interna y cerrada.

Consideremos una estructura algebraica binaria simple $(A, *)$:

- a) Decimos que la operación $*$ es *asociativa* si $a * (b * c) = (a * b) * c$, $\forall a, b, c \in A$.
- b) Decimos que A posee un *elemento neutro* respecto de $*$, si $\exists e \in A$, tal que $e * a = a * e = a$, $\forall a \in A$.
- c) Decimos que $a \in A$ posee un *elemento simétrico o inverso* a^{-1} respecto de $*$, si $a * a^{-1} = a^{-1} * a = e$, donde e es elemento neutro.
- d) Decimos que la operación $*$ es *comutativa*, si $a * b = b * a$, $\forall a, b \in A$.

Una estructura algebraica binaria $(A, *)$ que no cumple con ninguna de las condiciones a)-d) se llama un *magma* o *grupoido* y constituye la estructura algebraica más sencilla y, por lo general, carente de interés en el álgebra. Si $*$ es comutativa, diremos que $(A, *)$ es un *magma comunitativo* o *abeliano*¹.

¹En honor del matemático Noruego Niels Henrik Abel

Una estructura algebraica binaria $(A, *)$, donde $*$ es asociativa se llama un *semigrupo*. Si $*$ es commutativa diremos que es un *semigrupo commutativo o abeliano*.

Una estructura algebraica binaria $(A, *)$, donde $*$ es asociativa y posee elemento neutro respecto de $*$, se llama un *monoide*. Si $*$ es commutativa diremos que es un *monoide commutativo o abeliano*.

Una estructura algebraica binaria $(A, *)$, donde $*$ es asociativa, posee elemento neutro respecto de $*$ y todo elemento de A posee un simétrico respecto de $*$ se llama un *grupo*. Si $*$ es commutativa entonces diremos que es un *grupo commutativo o abeliano*.

EJEMPLOS 2.3.

1. Sea P el subconjunto de los números enteros pares · el producto usual de enteros, entonces (P, \cdot) es un semigrupo abeliano
2. $(\mathbb{N}, +)$, donde $+$ es la suma usual de números naturales es un monoide abeliano. Ningún $n \in \mathbb{N}$, salvo el 0, posee un simétrico respecto de $+$. (Ver 3.3)
3. $(\mathbb{Z}, +)$, donde $+$ es la suma usual de números enteros es un grupo abeliano. Dado $n \in \mathbb{Z}$, $-n \in \mathbb{Z}$ es su simétrico.
4. Si \mathcal{M}_n es el conjunto de matrices cuadradas con términos reales $n \times n$ y · el producto usual de matrices, entonces (\mathcal{M}_n, \cdot) es un monoide no commutativo.
5. (\mathbb{R}^3, \times) , donde \times es el producto vectorial sobre \mathbb{R}^3 , es un magma.
6. Sea $GL(n)$ el conjunto de matrices invertibles con términos reales $n \times n$, entonces $(GL(n), \cdot)$, donde \cdot es el producto usual de matrices, es un grupo (no commutativo), llamado el *grupo lineal*.

En el caso en que A es un conjunto finito, la operación $*$ se suele definir por medio de una tabla, como en los siguientes ejemplos:

EJEMPLOS 2.4.

1. Sea $A := \{a, b, c\}$ y $*$ definida por la siguiente tabla:

$*$	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

(2.1)

De la tabla se deduce facilmente que a es el elemento neutro de $*$. Si el lector traza una diagonal principal sobre la tabla, notará que existe simetría, respecto de la diagonal, en la distribución, en la tabla, de los elementos de A , lo cual indica que $*$ es commutativa. Dejamos al lector la inquietud de determinar si existe un simétrico para cada elemento de A y si la operación es asociativa.

2. Sea $\Omega_3 := \{\omega_1, \omega_2, \omega_3\}$ las tres raíces cúbicas complejas de 1, donde $\omega_1 := 1$, $\omega_2 := -\frac{1}{2} + \frac{1}{2}\sqrt{3}i$, $\omega_3 := -\frac{1}{2} - \frac{1}{2}\sqrt{3}i$. Si · es el producto usual de números complejos, se obtiene la siguiente tabla:

\cdot	ω_1	ω_2	ω_3
ω_1	ω_1	ω_2	ω_3
ω_2	ω_2	ω_3	ω_1
ω_3	ω_3	ω_1	ω_2

(2.2)

De la tabla se deduce que el conjunto Ω_3 es cerrado respecto del producto de números complejos. El lector verificará fácilmente que (Ω_3, \cdot) es un grupo abeliano. Nótese la similitud formal entre la tabla (2.1) y la tabla (2.2).

2.1.1. Ejercicios y Complementos.

1. Consideremos la estructura algebraica $(\mathbb{Z}, *)$, donde $a * b := a + b - a \cdot b$, $\forall a, b \in \mathbb{Z}$.
+ y · designan la suma y producto usuales de números enteros.
 - a) Comprobar si existe un elemento neutro en \mathbb{Z} respecto de *.
 - b) ¿Qué elementos poseen un simétrico respecto de *?
 - c) ¿Es * asociativa?
 - d) ¿Qué tipo de estructura posee $(\mathbb{Z}, *)$?
2. Analizar qué tipo de estructura poseen las siguientes estructuras algebraicas:
 - a) $(S, +)$, donde $S := \{x \mid x \in \mathbb{Z}, x < 0\}$ y + la suma de números enteros.
 - b) $(S, +)$, donde $S := \{5x \mid x \in \mathbb{Z}\}$ y + la suma de números enteros.
 - c) (S, \cdot) , donde $S := \{x \mid x \in \mathbb{Z}, x \text{ es impar}\}$ y · el producto de números enteros.
 - d) El conjunto Ω_n , de las n -raíces complejas de 1, con ·, el producto usual de complejos.
 - e) (S, \cdot) , donde $S := \{-2, -1, 1, 2\}$ y · el producto usual de números enteros.
 - f) (S, \cdot) , donde $S := \{1, -1, i, -i\}$ y · el producto usual de números complejos.
 - g) (S, \cdot) , donde $S := \{z \mid z \in \mathbb{C}, |z| = 1\}$
3. Dadas las matrices complejas
 $\mathbf{1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $\mathbf{i} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, $\mathbf{j} = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$, $\mathbf{k} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$, agregando sus respectivos elementos negativos, construir una tabla de sus productos, usando el producto usual de matrices. Determinar si (\mathcal{Q}, \cdot) , donde \mathcal{Q} es el conjunto de dichas matrices con sus negativos, forma un grupo y si éste es commutativo.
4. Mostrar que en una estructura algebraica $(A, *)$ el elemento neutro, si existe, es único. Si además * es asociativa, entonces el simétrico de un elemento, si existe, es único.
5. Sea \mathcal{P} el conjunto de matrices de la forma
 $\mathbf{1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $\mathbf{i} = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$, $\mathbf{h} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, $\mathbf{s} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$
 llamadas las *matrices de Pauli* y sus negativos correspondientes. ¿Es \mathcal{P} cerrado respecto del producto de matrices? Las matrices de Pauli son utilizadas en la mecánica cuántica

2.2. Homomorfismos de Estructuras Algebraicas Simples

DEFINICIÓN 2.3. Sean $(A, *)$, (B, \oplus) dos estructuras algebraicas. Decimos que la aplicación $\varphi : A \rightarrow B$ es un *homomorfismo* de estructuras algebraicas, entre $(A, *)$ y (B, \oplus) , si $\varphi(x * y) = \varphi(x) \oplus \varphi(y)$, $\forall x, y \in A$.

Si φ es inyectiva, sobreinyectiva o biyectiva, diremos que φ es un *monomorfismo*, *epimorfismo* o *isomorfismo* respectivamente. Si φ es un homomorfismo cuyo dominio y contradominio es la misma estructura, entonces se dice que φ es un *endomorfismo*. Un endomorfismo biyectivo se llama un *automorfismo*.

Si las estructuras son semigrupos, monoides o grupos, diremos que φ es un homomorfismo de semigrupos, monoides o grupos.

EJEMPLOS 2.5.

1. Sea $(\mathbb{Z}, +)$ el grupo de los números enteros con la suma usual, $\varphi : \mathbb{Z} \rightarrow \mathbb{Z}$ la aplicación definida por $\varphi(n) := 2n$, $\forall n \in \mathbb{Z}$. φ es un homomorfismo entre $(\mathbb{Z}, +)$ y $(\mathbb{Z}, +)$, ya que $\varphi(m+n) = 2(m+n) = 2m+2n$, $\forall m, n \in \mathbb{Z}$. φ es un endomorfismo inyectivo, sin embargo no es automorfismo, ya que no es sobreyectivo.
2. $\psi : \mathbb{Z} \rightarrow \mathbb{Z}$, definida por $\psi(m) := m + 5$, $\forall m \in \mathbb{Z}$ no es un homomorfismo, ya que $\psi(m+n) = (m+n) + 5$, mientras que $\psi(m) + \psi(n) = m + 5 + n + 5 = m + n + 10$
3. Consideremos las estructuras algebraicas $(A, *)$, y (Ω_3, \cdot) , donde $A := \{a, b, c\}$, Ω_3 el conjunto de las raíces cúbicas complejas de 1, $*$ la operación binaria definida por la tabla (2.1), página 18 y \cdot la operación binaria definida por la tabla (2.2), página 18 y φ la aplicación $\varphi : A \rightarrow \Omega_3$, definida por $\varphi(a) := \omega_1$, $\varphi(b) := \omega_2$, $\varphi(c) := \omega_3$, entonces $\varphi(a * a) = \varphi(a) = 1 = \varphi(a) \cdot \varphi(a)$, $\varphi(a * b) = \varphi(b) = \omega_2 = 1 \cdot \omega_2 = \varphi(a) \cdot \varphi(b)$, $\varphi(a * c) = \varphi(c) = \omega_3 = 1 \cdot \omega_3 = \varphi(a) \cdot \varphi(c)$, $\varphi(b * b) = \varphi(c) = \omega_3 = \omega_2 \cdot \omega_2 = \varphi(b) \cdot \varphi(b)$, $\varphi(c * c) = \varphi(b) = \omega_2 = \omega_3 \cdot \omega_3 = \varphi(c) \cdot \varphi(c)$, $\varphi(c * b) = \varphi(a) = \omega_1 = \omega_3 \cdot \omega_2 = \varphi(c) \cdot \varphi(b)$, por lo que φ es un homomorfismo. Por tratarse de estructuras abelianas ya no es necesario examinar $b * c$ y $c * a$.

DEFINICIÓN 2.4. Sean $(A, *)$, (B, \oplus) dos estructuras algebraicas con elementos neutros $e \in A$ y $f \in B$, $\varphi : A \rightarrow B$ un homomorfismo. Al conjunto $\ker \varphi := \{x \in A \mid \varphi(x) = f\}$ lo llamamos el *núcleo* o *kernel* de φ .

EJEMPLOS 2.6.

1. Así en los ejemplos 2.5 números 1) y 3) el $\ker \varphi$ es $\{0\}$ y $\{a\}$ respectivamente.
2. Sean $(\mathbb{Z}, +)$, (A, \oplus) , donde $A := \{0, 1\}$ y \oplus la operación binaria definida por la tabla

	0	1
0	0	1
1	1	0

y $\varphi : \mathbb{Z} \rightarrow A$ la aplicación definida por

$$\varphi(n) := \begin{cases} 0 & \text{si } n \text{ par} \\ 1 & \text{si } n \text{ es impar} \end{cases}$$

El lector verificará fácilmente que φ es un homomorfismo y que $\ker \varphi = 2\mathbb{Z} := \{x \in \mathbb{Z} \mid x \text{ par}\}$.

3. Consideremos las estructuras algebraicas $(\mathbb{R}, +)$ y (\mathbb{S}^1, \cdot) , donde $\mathbb{S}^1 := \{z \in \mathbb{C} \mid |z| = 1\}$ (geométricamente \mathbb{S}^1 es el círculo de radio 1 con centro en el origen), $\varphi : \mathbb{R} \rightarrow \mathbb{S}^1$ la aplicación definida por $\varphi(x) := e^{2\pi xi}$, $\forall x \in \mathbb{R}$. φ es un homomorfismo, ya que $\varphi(x+y) = e^{2\pi(x+y)i} = e^{2\pi xi} \cdot e^{2\pi yi} = \varphi(x) \cdot \varphi(y)$. El elemento neutro en $(\mathbb{R}, +)$ es el 0 y en (\mathbb{S}^1, \cdot) es el 1 que es igual a $e^{2\pi ni}$, $\forall n \in \mathbb{Z}$. Por lo que $\ker \varphi = \mathbb{Z}$.

2.2.1. Ejercicios y complementos.

1. Sean $(\mathbb{Z}, +)$, (A, \oplus) , donde $A := \{0, 1, 2\}$, $+$, \oplus son la suma usual de enteros, \oplus , la operación definida por la tabla:

\oplus	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

y sea $\varphi : \mathbb{Z} \rightarrow A$ la aplicación definida por:

$$(2.5) \quad \varphi(n) := \begin{cases} 0 & \text{si } n = 3m, m \in \mathbb{Z} \\ 1 & \text{si } n = 3m + 1, m \in \mathbb{Z} \\ 2 & \text{si } n = 3m + 2, m \in \mathbb{Z} \end{cases}$$

Mostrar que φ es un homomorfismo y dar $\ker \varphi$.

2. Sean $(\mathbb{R}^3, +)$, $(\mathbb{R}^2, +)$, donde $+$ es la suma usual en \mathbb{R}^3 y \mathbb{R}^2 , respectivamente. Si $\varphi : \mathbb{R}^3 \rightarrow \mathbb{R}^2$ definida por $\varphi(x, y, z) := (x, y)$, $\forall (x, y, z) \in \mathbb{R}^3$. Mostrar que φ es un homomorfismo y dar $\ker \varphi$.
3. Sean $(A, *)$, (Ω_3, \cdot) , donde $A := \{a, b, c\}$, $\Omega_3 := \{\omega_1, \omega_2, \omega_3\}$ el conjunto de las raíces cúbicas complejas de 1, ver ejemplos 2.4 1) y 2), $*$, \cdot definidas en las tablas (2.1), (2.2) respectivamente. Si $\varphi : A \rightarrow \Omega_3$ es la aplicación definida por $\varphi(a) := 1$, $\varphi(b) := \omega_2$, $\varphi(c) := \omega_3$, mostrar que φ es un isomorfismo y $\ker \varphi = a$.
4. Sean (B, \oplus) , (Ω_3, \cdot) , donde $B := \{0, 1, 2\}$, \oplus definida en la tabla (2.4), (Ω_3, \cdot) , como en el ejercicio precedente y $\psi : \Omega_3 \rightarrow B$ la aplicación definida por $\psi(\omega_1) := 0$, $\psi(\omega_2) = 1$, $\psi(\omega_3) := 2$. Mostrar que ψ es un isomorfismo, cuyo núcleo es $\ker \psi = \{\omega_1\}$ y que la composición $\psi \circ \varphi$, donde φ es la aplicación definida en el ejercicio precedente, es también un isomorfismo.
5. Si ψ es un isomorfismo entre dos estructuras algebraicas cualesquiera $(A, *)$, (B, \odot) , mostrar que entonces las dos poseen el mismo tipo de estructura. (Es decir que si $(A, *)$ es grupo, también lo será (B, \odot) , etc.).

2.3. Estructuras Algebraicas Con Dos Operaciones Binarias

Del álgebra elemental es conocido que en los conjuntos de números enteros, racionales, reales y complejos se tienen definidas dos operaciones binarias cerradas, la suma y el producto usuales, las cuales son asociativas y que entre éstas dos operaciones subsiste la siguiente *ley de distributividad*:

$$(2.6) \quad a \cdot (b + c) = a \cdot b + a \cdot c, \text{ y } (a + b) \cdot c = a \cdot c + b \cdot c, \quad \forall a, b, c$$

en cualquiera de los conjuntos arriba mencionados.

DEFINICIÓN 2.5. Una tríada ordenada $(A, *, \odot)$, donde A es un conjunto no vacío, $*$, \odot operaciones binarias cerradas e internas sobre A , se llama una *estructura algebraica con dos operaciones binarias*.

Naturalmente en el álgebra se está interesado en que dichas operaciones cumplan ciertas condiciones interesantes y ciertas relaciones entre ellas.

Inspirados en las propiedades que subsisten en los conjuntos de los números enteros, racionales, reales y complejos definimos la siguiente estructura:

DEFINICIÓN 2.6. Decimos que la estructura algebraica con dos operaciones binarias $(A, *, \odot)$ es un *anillo*, si $(A, *)$ es un grupo abeliano, (A, \odot) un semigrupo y se cumplen las relaciones de distributividad siguientes:

$$(2.7) \quad a \odot (b * c) = a \odot b * a \odot c, \text{ y } (a * b) \odot c = a \odot c * b \odot c, \quad \forall a, b, c \in A$$

Si además (A, \odot) es un monoide, entonces se dice que $(A, *, \odot)$ es un anillo con *unidad*, y si \odot es conmutativa, entonces se dice que es un *anillo conmutativo*.

EJEMPLOS 2.7.

1. $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$ son anillos conmutativos con unidad.
2. $(\mathcal{M}_n, +, \cdot)$, donde \mathcal{M}_n es el conjunto de matrices reales o complejas, y $+$, \cdot la suma y producto usual de matrices, es un anillo no conmutativo con unidad.
3. $(A, *, \odot)$, donde $A := \{0, 1, 2\}$, $*$ la operación definida en la tabla (2.1), y \odot la operación definida por la tabla:

\odot	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

es un anillo conmutativo con unidad. (¡verificarlo!)

Si en un anillo $(A, *, \odot)$ se cumple además que (A^*, \odot) es un grupo, donde $A^* := A \setminus \{e\}$, e el elemento neutro de $*$, entonces se dice que $(A, *, \odot)$ es un *cuerpo*. Si (A^*, \odot) es grupo abeliano, entonces se dice que $(A, *, \odot)$ es un *campo*.

OBSERVACIÓN. En la literatura alemana, francesa y alguna española, se utiliza cuerpo y cuerpo conmutativo, para lo que nosotros llamamos campo.

La palabra *cuerpo* es la traducción de la palabra alemana *Körper*, utilizada, por primera vez, por el matemático alemán Richard Dedekind.

EJEMPLOS 2.8.

1. $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$ son campos, mientras que $(\mathbb{Z}, +, \cdot)$ no es ni campo ni cuerpo, ya que $(\mathbb{Z} \setminus \{0\}, \cdot)$ no es grupo, pues sus elementos, salvo $\{1, -1\}$, no son invertibles respecto de \cdot .
2. $(\mathcal{M}_n, +, \cdot)$ tampoco es un cuerpo, pues no toda matriz cuadrada es invertible respecto del producto.
3. $(A, *, \odot)$ del ejemplo 2.7, 3), es un campo, como el lector comprobará fácilmente.

DEFINICIÓN 2.7. Sean $(A, *, \odot)$, (B, \oplus, \circ) , dos anillos (cuerpos o campos). Decimos que la aplicación $\psi : A \rightarrow B$ es un *homomorfismo de anillos* (cuerpos o campos), si ψ es homomorfismo de grupos abelianos entre $(A, *)$ y (B, \oplus) y homomorfismo de semigrupos (monoídes) entre (A, \odot) y (B, \circ) .

El núcleo o ker de un homomorfismo de anillos ψ , entre $(A, *, \odot)$ y (B, \oplus, \circ) es el núcleo de ψ en tanto que homomorfismo de grupos abelianos entre $(A, *)$ y (B, \oplus) .

OBSERVACIÓN. En un anillo es de suma importancia el orden en el cual se dan las operaciones. Así por ejemplo, $(\mathbb{Z}, +, \cdot)$ es un anillo, mientras que $(\mathbb{Z}, \cdot, +)$ no lo es, ya que (\mathbb{Z}, \cdot) no es grupo.

2.3.1. Estructuras mixtas relacionadas con anillos y campos. Existen estructuras algebraicas, que además de poseer una operación binaria interna y cerrada, poseen una operación externa cerrada, de un anillo o campo fijo, que opera sobre ella. Tal es el caso de los llamados *módulos* y *espacios vectoriales*.

DEFINICIÓN 2.8. Sea $(A, *, \odot)$ un anillo con unidad. Un *A-módulo* por la izquierda es una estructura algebraica (M, \dagger, \circ) , donde (M, \dagger) es un grupo abeliano, \circ es una operación binaria externa $\circ : A \times M \rightarrow M$ y se satisfacen las condiciones siguientes:

1. $\lambda \circ (x \dagger y) = \lambda \circ x \dagger \lambda \circ y, \forall x, y \in M, \forall \lambda \in A.$
2. $(\lambda * \alpha) \circ x = \lambda \circ x \dagger \alpha \circ x, \forall x \in M, \forall \lambda, \alpha \in A.$
3. $(\lambda \odot \alpha) \circ x = \lambda \circ (\alpha \circ x), \forall x \in M, \forall \lambda, \alpha \in A.$
4. Si u es la unidad en $(A, *, \odot)$, entonces $u \circ x = x, \forall x \in M.$

Si \circ es una operación binaria externa $\circ : M \times A \rightarrow M$ y se cumplen las condiciones:

1. $(x \dagger y) \circ \lambda = x \circ \lambda \dagger y \circ \lambda, \forall x, y \in M, \forall \lambda \in A.$
2. $x \circ (\lambda * \alpha) = x \circ \lambda \dagger x \circ \alpha, \forall x \in M, \forall \lambda, \alpha \in A.$
3. $x \circ (\lambda \odot \alpha) = (x \circ \lambda) \circ \alpha, \forall x \in M, \forall \lambda, \alpha \in A.$
4. Si u es la unidad en $(A, *, \odot)$, entonces $x \circ u = x, \forall x \in M.$

Entonces se dice que (M, \dagger, \circ) es un *A-módulo* por la derecha.

Un *A-módulo* (M, \dagger, \circ) sobre un campo $(A, *, \odot)$ se llama un *A-espacio vectorial*. Los elementos de M se denominan *vectores* y los del campo A *escalares* y se dice que A es el *campo de escalares* del espacio vectorial (M, \dagger, \circ) . A la operación \circ la llamamos el *producto con escalares*.

EJEMPLOS 2.9.

1. Sea $(\mathbb{Z}, +, \cdot)$ el anillo de los números enteros con la suma y producto usuales. Entonces $(\mathbb{Z}^2, \dagger, \circ)$ donde \dagger está definida por

$$(x, y) \dagger (u, v) := (x + u, y + v), \forall (x, y), (u, v) \in \mathbb{Z}^2$$

y \circ definida por

$$\lambda \circ (x, y) := (\lambda \cdot x, \lambda \cdot y), \forall (x, y) \in \mathbb{Z}^2, \forall \lambda \in \mathbb{Z},$$

es un \mathbb{Z} -módulo.

2. Del álgebra lineal son bien conocidos los \mathbb{R} -espacios vectoriales $(\mathbb{R}^n, +, \cdot)$, donde $+$ y \cdot son la suma en el \mathbb{R}^n y el producto con escalares respectivamente.
3. $(\mathcal{M}_n, +, \cdot)$, donde \mathcal{M}_n es el conjunto de las matrices reales $n \times n$, $+$ la suma usual de matrices y \cdot el producto definido por $\lambda \cdot \mathbf{A} := (\lambda \cdot a_{ij})$, donde $\mathbf{A} := (a_{ij})$, es un \mathbb{R} -espacio vectorial.

Los homomorfismos entre *A-módulos* o *A-espacios vectoriales* se llaman *aplicaciones lineales*. Dados dos *A-módulos* (M, \dagger, \circ) , (N, \ddagger, \bullet) , decimos que la aplicación $\psi : M \rightarrow N$ es *lineal* si satisface las condiciones siguientes:

1. $\psi(x \dagger y) = \psi(x) \ddagger \psi(y), \forall x, y \in M$
2. $\psi(\lambda \circ x) = \lambda \bullet \psi(x), \forall x \in M, \forall \lambda \in A$

Algunos módulos poseen una operación interna y cerrada adicional, que satisface ciertas relaciones de distributividad respecto de las operaciones del módulo,

DEFINICIÓN 2.9. Sea $(A, *, \odot)$ un anillo con unidad. Un *A-álgebra* por la izquierda (por la derecha) es una estructura algebraica $((M, \dagger, \circ), \star)$, donde (M, \dagger, \circ) es un *A-módulo* por la izquierda (por la derecha) y \star es una operación binaria cerrada $\star : M \times M \rightarrow M$ que satisface las siguientes condiciones de distributividad:

1. $(x \dagger y) \star z = (x \star z) \dagger (y \star z), \forall x, y, z \in M.$
2. $x \star (y \dagger z) = (x \star y) \dagger (x \star z), \forall x, y, z \in M.$
3. $(\lambda \circ x) \star y = x \star (\lambda \circ y) = \lambda \circ (x \star y), \forall x, y \in M, \forall \lambda \in A.$

$$(3a). (x \circ \lambda) \star y = x \star (y \circ \lambda) = (x \star y) \circ \lambda, \forall x, y \in M, \forall \lambda \in A.$$

Si \star es conmutativa $((M, \dagger, \circ), \star)$ es un A -álgebra conmutativa. Si \star es asociativa, entonces se dice que $((M, \dagger, \circ), \star)$ es un A -álgebra asociativa.

Dadas dos A -álgebras $((M, \dagger, \circ), \star), ((N, \ddagger, \bullet), \diamond)$. Decimos que la aplicación $\psi : M \rightarrow N$ es un *homomorfismo de A -álgebras*, si ψ es lineal y satisface además $\psi(x \star y) = \psi(x) \diamond \psi(y), \forall x, y \in M$.

EJEMPLOS 2.10.

1. Todo anillo o campo $(A, *, \odot)$ es un A -álgebra.
2. El espacio vectorial $(\mathbb{R}^2, +, \cdot)$ puede ser dotado de una estructura de \mathbb{R} -álgebra asociativa y conmutativa, por medio de la operación $\star : \mathbb{R}^2 \times \mathbb{R}^2 \rightarrow \mathbb{R}^2$, definida de la siguiente manera: $\forall \mathbf{x} := (x_1, x_2), \mathbf{y} := (y_1, y_2) \in \mathbb{R}^2, (\mathbf{x}) \star (\mathbf{y}) := (x_1 \cdot y_1 - x_2 \cdot y_2, x_1 \cdot y_2 + x_2 \cdot y_1)$.
3. El espacio vectorial de las matrices reales $n \times n$ $(\mathcal{M}_n, +, \cdot)$ con el producto usual de matrices, es una \mathbb{R} -álgebra no conmutativa.

OBSERVACIÓN 2.1. Por abuso de lenguaje y de simbología y para no perdernos en formalismos, en el futuro designaremos las operaciones de un anillo (campo) por $+$ y \cdot , salvo casos particulares, y las llamaremos la suma y el producto respectivamente. Denotaremos por 0 y 1 a los elementos neutros de $+$ y \cdot . Por el anillo (campo) A nos referiremos al anillo $(A, +, \cdot)$. De forma análoga procederemos con los módulos (espacios vectoriales), representaremos por $+$ y por \cdot la operación interna y el producto con escalares y por M al módulo $(M, +, \cdot)$. Al elemento neutro de $+$ en M lo representaremos por $\mathbf{0}$. Los elementos de un módulo o espacio vectorial, en general, los escribiremos en letras negrillas, para diferenciarlos de los elementos del anillo o campo correspondiente. También, por facilidad, obviaremos escribir la operación \cdot y escribiremos $\lambda\alpha$ por $\lambda \cdot \alpha, \forall \lambda, \alpha \in A$ y $\lambda\mathbf{x}$ por $\lambda \cdot \mathbf{x}, \forall \mathbf{x} \in M$. Igualmente, en el caso de las A -álgebras, representaremos por \cdot la operación binaria interna y cerrada y escribiremos también \mathbf{xy} por $\mathbf{x} \cdot \mathbf{y}$. En general no hay confusión ya que cada operación se aplica en elementos de índole diferente.

En algunos espacios vectoriales reales se puede definir también una operación binaria interna, cuyo resultado es un elemento del campo \mathbb{R} y que cumple con determinadas condiciones, como es el llamado producto escalar o interno.

DEFINICIÓN 2.10. Sea V un \mathbb{R} -espacio vectorial. Una operación binaria interna $\langle \cdot, \cdot \rangle : V \times V \rightarrow \mathbb{R}$ se llama un *producto escalar* o *producto interno*, si satisface las siguientes condiciones:

1. $\langle \mathbf{u}, \mathbf{v} \rangle = \langle \mathbf{v}, \mathbf{u} \rangle, \forall \mathbf{u}, \mathbf{v} \in V$ (Axioma de simetría)
2. $\langle \mathbf{u}, \mathbf{u} \rangle \geq 0, \forall \mathbf{u} \in V \quad \langle \mathbf{u}, \mathbf{u} \rangle = 0 \text{ Ssi } \mathbf{u} = 0$ (Axioma de positividad)
3. $\langle \mathbf{u} + \mathbf{w}, \mathbf{v} \rangle = \langle \mathbf{u}, \mathbf{v} \rangle + \langle \mathbf{w}, \mathbf{v} \rangle, \forall \mathbf{u}, \mathbf{v}, \mathbf{w} \in V$ (Axioma de aditividad)
4. $\langle \lambda\mathbf{u}, \mathbf{v} \rangle = \lambda\langle \mathbf{u}, \mathbf{v} \rangle, \forall \mathbf{u}, \mathbf{v} \in V, \forall \lambda \in \mathbb{R}$. (Axioma de homogeneidad)

Una estructura $(V, \langle \cdot, \cdot \rangle)$, donde V es un espacio vectorial y $\langle \cdot, \cdot \rangle$ es un producto interno, se llama un *espacio vectorial euclídeano*.

Del álgebra lineal es bien conocido el producto escalar en el \mathbb{R}^n , definido de la siguiente forma: Dados $\mathbf{x} := (x_1, \dots, x_n), \mathbf{y} := (y_1, \dots, y_n) \in \mathbb{R}^n, \langle \mathbf{x}, \mathbf{y} \rangle := \sum_{i=1}^n x_i y_i$. Llamado el producto escalar *estándar*.

2.3.2. Ejercicios y Complementos.

1. Determinar si $(\mathbb{Q}, \cdot, +)$ y $(\mathbb{R}, \cdot, +)$ son anillos

2. Sea S un conjunto cualquiera no vacío, $\mathcal{P}(S)$ su conjunto potencia. Determinar si $(\mathcal{P}(S), \cap, \cup)$ y $(\mathcal{P}(S), \cup, \cap)$ son anillos. ¿Existen elementos neutros de \cup y \cap ?
3. Sea S como en el ejercicio anterior, mostrar que $(\mathcal{P}(S), \oplus, \cap)$, donde $A \oplus B := A \cup B \setminus A \cap B$, $\forall A, B \in \mathcal{P}(S)$, es un anillo conmutativo con unidad.
4. Sea $(\mathbb{Q}^4, +, \cdot)$, donde $+$ es la suma usual en \mathbb{Q}^4 y \cdot el producto definido de la siguiente forma: dados $\mathbf{x} := (x_1, x_2, x_3, x_4)$, $\mathbf{y} := (y_1, y_2, y_3, y_4) \in \mathbb{Q}^4$, $\mathbf{x} \cdot \mathbf{y} := (x_1y_1 + x_2y_3, x_1y_2 + x_2y_4, x_3y_1 + x_4y_3, x_3y_2 + x_4y_4)$. Mostrar que $(\mathbb{Q}^4, +, \cdot)$ es un anillo. ¿Es un anillo conmutativo?
5. Mostrar que el anillo del ejemplo 2.7, 3) es un campo.
6. Mostrar que el álgebra definida en el ejemplo 2.10, 2), es isomorfa al álgebra de los números complejos.
7. Sean $\mathbf{e}_1 := (1, 0, 0, 0)$, $\mathbf{e}_2 := (0, 1, 0, 0)$, $\mathbf{e}_3 := (0, 0, 1, 0)$, $\mathbf{e}_4 := (0, 0, 0, 1) \in \mathbb{R}^4$, la base usual del espacio vectorial \mathbb{R}^4 y un producto definido por la siguiente tabla:

.	\mathbf{e}_1	\mathbf{e}_2	\mathbf{e}_3	\mathbf{e}_4
\mathbf{e}_1	\mathbf{e}_1	\mathbf{e}_2	\mathbf{e}_3	\mathbf{e}_4
\mathbf{e}_2	\mathbf{e}_2	$-\mathbf{e}_1$	$-\mathbf{e}_4$	\mathbf{e}_3
\mathbf{e}_3	\mathbf{e}_3	\mathbf{e}_4	$-\mathbf{e}_1$	$-\mathbf{e}_2$
\mathbf{e}_4	\mathbf{e}_4	$-\mathbf{e}_3$	\mathbf{e}_2	$-\mathbf{e}_1$

Considerando que todo elemento del \mathbb{R}^4 se escribe de la forma $\mathbf{x} := \sum_{i=1}^4 x_i \mathbf{e}_i$ y que el producto debe ser distributivo respecto de la suma, generalizar, a cualquier elemento del \mathbb{R}^4 , el producto definido en la tabla (2.9), para los elementos de la base. Mostrar que con éste producto el espacio vectorial \mathbb{R}^4 es una \mathbb{R} -álgebra anticonmutativa, es decir $\mathbf{x} \cdot \mathbf{y} = -\mathbf{y} \cdot \mathbf{x}$, llamada el álgebra de *cuaterniones* o *Hamiltonianos* (en honor a su descubridor Hamilton).

8. Utilizar las matrices $\mathbf{1}, \mathbf{i}, \mathbf{j}, \mathbf{k}$ definidas en la sección de ejercicios 2.1.1, 3) como base de un \mathbb{R} -espacio vectorial. Mostrar que este espacio vectorial, con el producto de matrices, forma una \mathbb{R} -álgebra anticonmutativa, isomorfa al álgebra de cuaterniones del ejercicio precedente.
9. Si $(V, \langle \cdot, \cdot \rangle)$ es un espacio vectorial con producto escalar, mostrar que también valen las siguientes propiedades:
 - i) $\langle \mathbf{u}, \mathbf{0} \rangle = \langle \mathbf{0}, \mathbf{u} \rangle = 0$, $\forall \mathbf{u} \in V$.
 - ii) $\langle \mathbf{u}, \mathbf{v} + \mathbf{w} \rangle = \langle \mathbf{u}, \mathbf{v} \rangle + \langle \mathbf{u}, \mathbf{w} \rangle$ $\forall \mathbf{u}, \mathbf{v}, \mathbf{w} \in V$.
 - iii) $\langle \mathbf{u}, \lambda \mathbf{v} \rangle = \lambda \langle \mathbf{u}, \mathbf{v} \rangle$, $\forall \mathbf{u}, \mathbf{v} \in V$, $\forall \lambda \in \mathbb{R}$.
10. Mostrar que los siguientes productos son productos escalares en \mathbb{R}^2 :
 - a) $\langle \mathbf{u}, \mathbf{v} \rangle := 6u_1v_1 + 2u_2v_2$
 - b) $\langle \mathbf{u}, \mathbf{v} \rangle := 2u_1v_1 + u_2v_1 + u_1v_2 + 2u_2v_2$.
11. Sea \mathcal{M}_2 el espacio vectorial de las matrices reales 2×2 . Dadas las matrices

$$U := \begin{pmatrix} u_1 & u_2 \\ u_3 & u_4 \end{pmatrix} \text{ y } V := \begin{pmatrix} v_1 & v_2 \\ v_3 & v_4 \end{pmatrix}.$$

Mostrar que $\langle U, V \rangle := u_1v_1 + u_2v_2 + u_3v_3 + u_4v_4$ es un producto escalar en \mathcal{M}_2 .

2.4. Ω_σ^μ -ESTRUCTURAS ALGEBRAICAS

En esta sección generalizaremos el concepto de estructura algebraica, considerando estructuras con varias operaciones de diferentes tipos de *ariedad*.

DEFINICIÓN 2.11. Sea A un conjunto no vacío. Una aplicación $* : \underbrace{A \times \cdots \times A}_n \rightarrow A$ se llama una operación n -aria, interna y cerrada sobre A . $*((a_1, \dots, a_n))$ se denota por $a_1 * \cdots * a_n, \forall a_1, \dots, a_n \in A$.

Un ejemplo clásico de una operación $(n - 1)$ -aria, para $n > 2$ es el *producto vectorial* o *producto cruz* sobre el espacio vectorial \mathbb{R}^n . Dados $n - 1$ vectores fijos $\mathbf{v}_1, \dots, \mathbf{v}_{n-1} \in \mathbb{R}^n$, definimos una aplicación lineal $\psi : \mathbb{R}^n \rightarrow \mathbb{R}$, de la forma siguiente:

$$\psi(\mathbf{u}) := \det \begin{pmatrix} \mathbf{v}_1 \\ \vdots \\ \mathbf{v}_{n-1} \\ \mathbf{u} \end{pmatrix}$$

Por el teorema de representación existe un único vector $\mathbf{w} \in \mathbb{R}^n$, tal que $\langle \mathbf{u}, \mathbf{w} \rangle = \psi(\mathbf{u})$. Al vector \mathbf{w} lo llamamos el *producto cruz* o *vectorial* de los vectores $\mathbf{v}_1, \dots, \mathbf{v}_{n-1} \in \mathbb{R}^n$ y lo representaremos por $\mathbf{v}_1 \times \cdots \times \mathbf{v}_{n-1} \times : \underbrace{\mathbb{R}^n \times \cdots \times \mathbb{R}^n}_{n-1} \rightarrow \mathbb{R}^n$ es una operación $(n - 1)$ -aria.

En \mathbb{R}^3 el producto vectorial es una operación binaria, tal y como la conocemos del álgebra elemental de vectores.

Denotemos por $\Omega := \{\omega_1, \dots, \omega_m\}$ un conjunto finito de operaciones internas y cerradas de diferente ariedad definidas sobre un conjunto A . La aplicación $v : \Omega \rightarrow \mathbb{N}$, definida por $v(\omega_j) := n_j$ Ssi ω_j es una operación n_j -aria, se llama la *aplicación de ariedad* de Ω .

Sea σ una permutación sobre Ω . Al par (A, Ω_σ^μ) , $1 \leq \mu \leq m$, donde $\Omega_\sigma^\mu := (\omega_{\sigma(1)}, \dots, \omega_{\sigma(\mu)})$ lo llamamos una Ω_σ^μ -estructura algebraica., al número μ lo llamaremos el *tipo* de la estructura. Los elementos de Ω pueden cumplir con ciertas propiedades de asociatividad, distributividad, existencia de elementos neutros o simétricos.

En particular, un grupo es una Ω_σ^1 -estructura algebraica de tipo 1 en la cual $\Omega_\sigma^1 := \{\omega_{\sigma(1)}\}$ y $v(\omega_{\sigma(1)}) = 2$, $\omega_{\sigma(1)}$ es asociativa, posee elemento neutro y cada elemento de A posee un simétrico respecto de $\omega_{\sigma(1)}$. Un anillo es una estructura Ω_σ^2 , de tipo 2, donde $\Omega_\sigma^2 := (\omega_{\sigma(1)}, \omega_{\sigma(2)})$, $v(\omega_{\sigma(1)}) = v(\omega_{\sigma(2)}) = 2$, $\omega_{\sigma(1)}$ es asociativa, posee elemento neutro y cada elemento posee un simétrico respecto de $\omega_{\sigma(1)}$, $\omega_{\sigma(2)}$ es asociativa y distributiva respecto de $\omega_{\sigma(1)}$.

En este libro nos limitaremos al estudio de los grupos, anillos y campos, es decir de estructuras Ω_σ^1 y Ω_σ^2 . Para el estudio de estructuras de órdenes mayores referimos al lector a [5].

2.4.1. Ejercicios y Complementos.

1. Mostrar que $\mathbf{v}_1 \times \cdots \times \mathbf{v}_{n-1}$ es ortogonal a cada \mathbf{v}_i , $1 \leq i \leq n - 1$, es decir $\langle \mathbf{v}_1 \times \cdots \times \mathbf{v}_{n-1}, \mathbf{v}_i \rangle = 0$, $\forall i$, $1 \leq i \leq n - 1$.
2. Calcular $\mathbf{v}_1 \times \mathbf{v}_2 \times \mathbf{v}_3$ en \mathbb{R}^4 .

CAPÍTULO 3

NÚMEROS NATURALES, ENTEROS Y RACIONALES



FIGURA 3.1. Leopold Kronecker

Dios creó los números naturales, lo demás es obra del hombre. L. Kronecker.

En este capítulo daremos una pequeña introducción a la construcción formal de los números naturales, enteros y racionales y demostraremos algunas de sus propiedades más importantes y que nos servirán en el desarrollo de algunos temas. Omitiremos la construcción de los números reales por considerar que su construcción corresponde más a un curso de análisis real que al álgebra.

3.1. Los Números Naturales

3.1.1. Propiedades Generales y Operaciones Algebraicas. En la serie de ejercicios 1.4, 7) se introdujeron los números naturales como el conjunto \mathbb{N} , intersección de todos los conjuntos numerales, el cual tenía las siguientes propiedades fundamentales:

- a) $\emptyset \in \mathbb{N}$
- b) Si $x \in \mathbb{N} \Rightarrow x' \in \mathbb{N}$
- c) Cualquier subconjunto de \mathbb{N} que satisface a) y b), coincide con \mathbb{N} (principio de inducción).
- d) Si $x \in \mathbb{N}$, $x' \neq \emptyset$, además $x \in y \Rightarrow x \subseteq y$
- e) $x' \subseteq y' \Rightarrow x \subseteq y$
- f) $x' = y' \Rightarrow x = y$

Las propiedades a)-f) caracterizan totalmente a \mathbb{N} y reciben el nombre de *axiomas de Peano*. Algunos textos introducen al conjunto de los naturales utilizando estos axiomas. Un número natural es entonces un elemento de \mathbb{N} y lo designamos de la siguiente forma:
 $0 := \emptyset$, $1 := 0' = \{\emptyset\}$, $2 := 1' = \{\emptyset, \{\emptyset\}\}$, $3 := 2' = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}$, \dots .



FIGURA 3.2. Giuseppe Peano

OBSERVACIÓN. En nuestra definición de \mathbb{N} se incluye el 0 como número natural y por la definición de 0 y de sucesor, es el único número natural que no es sucesor de otro, como se deduce del inciso d). Algunos autores no lo incluyen y comienzan con el número 1. Desde un punto de vista teórico es irrelevante dónde comiencen los números naturales.

TEOREMA 3.1. *Para todo $n \in \mathbb{N}$, $n' \neq n$.*

DEMOSTRACIÓN. Consideremos el conjunto $N := \{x \in \mathbb{N} \mid x' \neq x\}$, entonces $0 \in N$, ya que 0 no es sucesor de ningún número entero. Sea $n \in N$, entonces vale $n' \neq n$, si $(n')' = n'$, entonces, por el inciso f), tendríamos que $n' = n$ en contradicción a que $n \in N$. Por consiguiente $n' \in N$ y por el principio de inducción $N = \mathbb{N}$. \square

Consideremos sobre \mathbb{N} la siguiente operación, definida por:

$$(3.1) \quad n + 0 := n, \forall n \in \mathbb{N}$$

$$(3.2) \quad n + m' := (n + m)', \forall n, m \in \mathbb{N}$$

Entonces $+ : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$, ya que $\forall n \in \mathbb{N}, \forall m \in \mathbb{N} \setminus \{0\}$, $n + m = n + m'_1 = (n + m_1)' \in \mathbb{N}$, donde $m'_1 := m$. Si $m = 0$ es obvio que $n + 0 = n \in \mathbb{N}$. Es decir que $+$ es una operación binaria cerrada sobre \mathbb{N} que llamaremos *suma de naturales*.

Como una consecuencia inmediata de (3.1) y (3.2) se tiene:

$$(3.3) \quad n + 1 = n + 0' = (n + 0)' = n', \forall n \in \mathbb{N}$$

TEOREMA 3.2. *$+$: $\mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$ posee las siguientes propiedades:*

1. *$+$ es asociativa, es decir:*

$$(3.4) \quad n + (m + k) = (n + m) + k, \forall n, m, k \in \mathbb{N}$$

2. *$+$ es commutativa, es decir:*

$$(3.5) \quad n + m = m + n, \forall n, m \in \mathbb{N}$$

DEMOSTRACIÓN. Para mostrar tanto la asociatividad como la commutatividad haremos uso del *principio de inducción*.

1. Consideremos el conjunto $\mathbf{N} := \{x \in \mathbb{N} \mid n + (m + x) = (n + m) + x, \forall m, n \in \mathbb{N}\}$

Vamos a mostrar que $\mathbf{N} = \mathbb{N}$. En efecto, por (3.1) $(n + m) + 0 = (n + m) = n + m = n + (m + 0)$, por lo que $0 \in \mathbf{N}$.

Por (3.2) y (3.3) $n + (m + 1) = n + m' = (n + m)' = (n + m) + 1$, por lo que $1 \in \mathbf{N}$. Vamos a mostrar ahora que $k \in \mathbf{N} \Rightarrow k' \in \mathbf{N}$. En efecto, para $k \in \mathbf{N}$ vale la ecuación: $n + (m + k) = (n + m) + k$, entonces $n + (m + k') = n + (m + k)' = n + (m + k) + 1 = (n + m) + k + 1 = (n + m) + k'$, por consiguiente $k' \in \mathbf{N}$ y por el principio de inducción $\mathbf{N} = \mathbb{N}$.

2. Para mostrar la comutatividad consideremos primeramente el conjunto $\mathbf{M} := \{x \in \mathbb{N} \mid x + 0 = 0 + x\}$, del cual mostraremos, usando el principio de inducción, que es igual a \mathbb{N} . En efecto $0 + 0 = 0 + 0$, por lo que $0 \in \mathbf{M}$, también $0 + 1 = 0 + 0' = (0 + 0)' = 0' = 1 = 1 + 0$, por consiguiente $1 \in \mathbf{M}$. Mostremos ahora que $m \in \mathbf{M} \Rightarrow m' \in \mathbf{M}$. Sea entonces $m \in \mathbf{M}$, entonces $0 + m' = (0 + m)' = m' = m' + 0$ y por el principio de inducción $\mathbf{M} = \mathbb{N}$. Consideremos ahora el conjunto $\mathbf{U} := \{x \in \mathbb{N} \mid 1 + x = x + 1\}$, obviamente $0, 1 \in \mathbf{U}$. Si $n \in \mathbf{U}$, entonces $1 + n' = (1 + n)' = (n + 1)' = (n + 1) + 1 = n' + 1$ y nuevamente por el principio de inducción $\mathbf{U} = \mathbb{N}$.

Finalmente consideremos el conjunto $\mathcal{N} := \{x \in \mathbb{N} \mid x + n = n + x, \forall n \in \mathbb{N}\}$, entonces, por lo anteriormente expuesto $0, 1 \in \mathcal{N}$. Sea ahora $m \in \mathcal{N}$, entonces $n + m' = (n + m)' = (m + n)' = (m + n) + 1 = m + (n + 1) = m + (1 + n) = (m + 1) + n = m' + n$. Por el principio de inducción vale entonces que $\mathcal{N} = \mathbb{N}$.

□

De lo anteriormente expuesto se obtiene el siguiente

COROLARIO 3.3. $(\mathbb{N}, +)$ es un monoide conmutativo con $e = 0$ como elemento neutro y 0 es el único elemento neutro respecto de $+$.

DEMOSTRACIÓN. Sólo nos falta mostrar la unicidad del elemento neutro. En efecto, consideremos el conjunto $M := \{x \in \mathbb{N} \mid x + p \neq x, \forall p \in \mathbb{N}, p \neq 0\}$. Por definición de $+$ tenemos que $0 + p = p \neq 0$, por lo que $0 \in M$. Por otra parte, sea $n \in M$, entonces $n + p \neq n$. Supongamos que $n' + p = (n + p)' = n'$, entonces por inciso f) de las propiedades de \mathbb{N} , tendríamos $n + p = n$, en contradicción a que $n \in M$, por consiguiente $n' + p \neq n'$ y $n' \in M$. Entonces por el principio de inducción $M = \mathbb{N}$. □

Sobre \mathbb{N} también podemos definir otra operación binaria, que llamaremos *producto de naturales*, de la siguiente forma:

$$(3.6) \quad n \cdot 0 := 0, \forall n \in \mathbb{N}$$

$$(3.7) \quad n \cdot m' := n \cdot m + n$$

Como una consecuencia inmediata de (3.6) y (3.7) se obtiene:

$$(3.8) \quad n \cdot 1 = n \cdot 0' = n \cdot 0 + n = n, \forall n \in \mathbb{N}$$

De la definición resulta que $\cdot : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$, es decir \cdot es una operación binaria cerrada sobre \mathbb{N} .

TEOREMA 3.4. $\cdot : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$ posee las siguientes propiedades:

1. \cdot es distributiva respecto de $+$, es decir:

$$(3.9) \quad n \cdot (m + k) = n \cdot m + n \cdot k, \forall n, m, k \in \mathbb{N}$$

y

$$(3.10) \quad (n + m) \cdot k = n \cdot k + m \cdot k, \forall n, m, k \in \mathbb{N}$$

2. \cdot es asociativa, es decir:

$$(3.11) \quad n \cdot (m \cdot k) = (n \cdot m) \cdot k, \forall n, m, k \in \mathbb{N}$$

3. \cdot es conmutativa, es decir:

$$(3.12) \quad n \cdot m = m \cdot n, \forall n, m \in \mathbb{N}$$

DEMOSTRACIÓN. Al igual que en el teorema precedente usaremos el principio de inducción para mostrar estas propiedades.

1. Consideremos los conjuntos $A := \{x \in \mathbb{N} \mid n \cdot (m + x) = n \cdot m + n \cdot x, \forall n, m \in \mathbb{N}\}$ y $B := \{x \in \mathbb{N} \mid (n+m) \cdot x = n \cdot x + m \cdot x, \forall n, m \in \mathbb{N}\}$. El lector comprobará facilmente que $0, 1 \in A$ y $0, 1 \in B$. Sea $k \in A$, entonces $n \cdot (m + k) = n \cdot m + n \cdot k$. $n \cdot (n+k') = n \cdot (n+k)' = n \cdot (m+k) + n = (n \cdot m + n \cdot k) + n = n \cdot m + (n \cdot k + n) = n \cdot m + n \cdot k'$, esto muestra que $k \in A \Rightarrow k' \in A$ y por el principio de inducción $A = \mathbb{N}$. Por otra parte si $k \in B$, entonces $(n+m) \cdot k = n \cdot k + m \cdot k$ y tendremos $(n+m) \cdot k' = (n+m) \cdot k + (n+m) = (n \cdot k + m \cdot k) + (n+m) = n \cdot k + (m \cdot k + (n+m)) = n \cdot k + (m \cdot k + (m+n)) = n \cdot k + ((m \cdot k + m) + n) = n \cdot k + (m \cdot k' + n) = n \cdot k + (n+m \cdot k') = (n \cdot k + n) + m \cdot k' = n \cdot k' + m \cdot k'$, lo que muestra que $k \in B \Rightarrow k' \in B$ y por el principio de inducción $B = \mathbb{N}$.
2. Consideremos $N := \{x \in \mathbb{N} \mid n \cdot (m \cdot x) = (n \cdot m) \cdot x, \forall n, m \in \mathbb{N}\}$, obviamente $0, 1 \in N$. Sea $k \in N$, entonces $n \cdot (m \cdot k) = (n \cdot m) \cdot k$ y tendremos $n \cdot (m \cdot k') = n \cdot (m \cdot k + m) = n \cdot (m \cdot k) + n \cdot m = (n \cdot m) \cdot k + n \cdot m = (n \cdot m) \cdot k'$, lo que muestra que $k \in N \Rightarrow k' \in N$ y por el principio de inducción $N = \mathbb{N}$.
3. Consideremos los siguientes conjuntos $O := \{x \in \mathbb{N} \mid 0 \cdot x = x \cdot 0\}$, $U := \{x \in \mathbb{N} \mid 1 \cdot x = x \cdot 1\}$ y $C := \{x \in \mathbb{N} \mid n \cdot x = x \cdot n, \forall n \in \mathbb{N}\}$, vamos a mostrar, por el principio de inducción, que cada uno de ellos es igual a \mathbb{N} .

En efecto $0 \in O$, por otra parte también $1 \in O$, ya que $0 \cdot 1 = 0 \cdot 0' = 0 \cdot 0 + 0 = 0 = 1 \cdot 0$. Si $n \in O$, entonces $n \cdot 0 = 0 \cdot n$. Entonces obtenemos $0 \cdot n' = 0 \cdot n + 0 = 0 = n' \cdot 0$, lo que muestra que $n \in O \Rightarrow n' \in O$ y por el principio de inducción $O = \mathbb{N}$.

De forma análoga se tiene que $0, 1 \in U$ y si $n \in U$, entonces $n = n \cdot 1 = 1 \cdot n$ y se tiene $1 \cdot n' = 1 \cdot n + 1 = n + 1 = n' = n' \cdot 1 = n'$ y de nuevo, por el principio de inducción $U = \mathbb{N}$.

Finalmente mostremos que $C = \mathbb{N}$. En efecto, es obvio que $0, 1 \in C$. Si $m \in C$, entonces $n \cdot m = m \cdot n$ y se tiene $n \cdot m' = n \cdot m + n = m \cdot n + n = m \cdot n + 1 \cdot n = (m + 1) \cdot n = m' \cdot n$. Por consiguiente $C = \mathbb{N}$.

□

Del teorema precedente se infiere, de forma inmediata, el siguiente

COROLARIO 3.5. (\mathbb{N}, \cdot) es un monoide conmutativo, cuyo único elemento neutro es $e = 1$.

DEMOSTRACIÓN. Sólo nos queda mostrar la unicidad de e . Vamos a mostrar primero que $m \cdot n = 0 \Rightarrow m = 0$ o $n = 0$. En efecto, supongamos que para n, m , $m \neq 0 \neq n$, $m \cdot n = 0$, entonces ambos son sucesores de un $n_1 \in \mathbb{N}$ y un $m_1 \in \mathbb{N}$ respectivamente. $0 = n \cdot m = n \cdot m'_1 = n \cdot m_1 + n = n \cdot m_1 + n_1 = (n \cdot m_1 + n_1)',$ en contradicción a que 0 no es sucesor de ningún elemento de \mathbb{N} . Por consiguiente $n = 0$ o $m = 0$. Por otra parte, supongamos que

existe $m \in \mathbb{N}$, $m \neq 1$, $m \neq 0$, tal que $m \cdot n = n$, $\forall n \in \mathbb{N}$, $n \neq 0$, y sea $m_1 \in \mathbb{N}$, $m'_1 = m$, entonces $n = m \cdot n = m'_1 \cdot n = n \cdot m_1 + n$, entonces, por corolario 3.3, $n \cdot m_1 = 0$ y, por lo anteriormente expuesto, dado que $n \neq 0$, $m_1 = 0$ y, por consiguiente $m = 1$. \square

3.1.2. Relación de Orden.

DEFINICIÓN 3.1. Sobre \mathbb{N} vamos a definir una relación \leq de la siguiente forma:

$$(3.13) \quad n \leq m : \Leftrightarrow \exists p \in \mathbb{N} \text{ tal que } m = n + p$$

Si $n \leq m$ diremos que n es *menor o igual* que m .

Diremos que n es *mayor o igual* que m , denotado: $n \geq m$, Ssi $m \leq n$.

TEOREMA 3.6. \leq es una relación de orden sobre \mathbb{N}

DEMOSTRACIÓN.

1. \leq es reflexiva. En efecto $n \leq n$, $\forall n \in \mathbb{N}$, ya que $n = n + 0$, $0 \in \mathbb{N}$
2. \leq es antisimétrica. En efecto, si $n \leq m$ y $m \leq n$, entonces existen $p, q \in \mathbb{N}$, tales que

$$(3.14) \quad m = n + p$$

$$(3.15) \quad n = m + q$$

de (3.14) y (3.15) resulta, substituyendo:

$$(3.16) \quad m = m + p + q = m + r, \text{ donde } r := (p + q) \in \mathbb{N}$$

entonces, por corolario 3.3, $r = 0$. Si p o q fueran distintos de 0, supongamos $p \neq 0$, entonces existe $p_1 \in \mathbb{N}$, tal que $p = p'_1$ y $0 = p + q = p'_1 + q = (p_1 + q)'$, en contradicción a que 0 no es sucesor de ningún número natural. Lo mismo se deduce si asumimos que $q \neq 0$, por consiguiente $p = q = 0$ y $n = m$

3. \leq es transitiva. Si $n \leq m$ y $m \leq s$, entonces existen $p, q \in \mathbb{N}$, tales que

$$(3.17) \quad m = n + p$$

y

$$(3.18) \quad s = m + q$$

de (3.17) y (3.18) se obtiene

$$(3.19) \quad s = n + (p + q) = n + r, \text{ donde } r := (p + q) \in \mathbb{N}$$

por consiguiente $n \leq s$. \square

DEFINICIÓN 3.2. Decimos que $n < m$ Ssi existe $p \in \mathbb{N} \setminus \{0\}$, tal que $m = n + p$.

El lector comprobará que $<$ es una relación que solamente es transitiva. No es simétrica ni reflexiva, ver ejercicios 3.1.4, 10) y 3.1.4, 11). $\forall n, m \in \mathbb{N}$, si $m < n$ no puede valer $n < m$ ni $n < n$. $<$ es lo que se llama entonces una *relación de orden estricto*. Si $m < n$ entonces diremos que m es *estrictamente menor* que n . Diremos que m es *estrictamente mayor* que n , denotado: $m > n$, Ssi $n < m$.

TEOREMA 3.7 (Ley de Tricotomía). *Para cada $n, m \in \mathbb{N}$ una y sólamente una de las siguientes relaciones es verdadera*

$$(3.20) \quad m = n$$

$$(3.21) \quad m < n$$

$$(3.22) \quad m > n$$

DEMOSTRACIÓN. Dado $m \in \mathbb{N}$, construimos los siguientes conjuntos:

$$M_1 := \{m\}, \quad M_2 := \{x \in \mathbb{N} \mid x < m\}, \quad M_3 := \{x \in \mathbb{N} \mid x > m\}$$

Vamos a probar que $\mathcal{M} := \{M_1, M_2, M_3\}$ es una partición de \mathbb{N} , $\forall m \in \mathbb{N}$. En efecto, si $m = 0$, $0 \in M_1$, $M_2 = \emptyset$, $M_3 = \mathbb{N} \setminus \{0\}$, entonces

$$\bigcup_{i=1}^n M_i = \mathbb{N}$$

y $M_1 \cap M_2 = M_1 \cap M_3 = M_2 \cap M_3 = \emptyset$. Sea ahora $m \neq 0$ y consideremos el conjunto

$$M := \bigcup_{i=1}^n M_i$$

$0 \in M_1$, por consiguiente $0 \in M$. Sea ahora $n \in \mathbb{N} \setminus \{0\}$ y $n \in M$. Entonces tenemos tres casos posibles:

- a) $n \in M_1$, entonces $n = m$ y $n' < m$, por lo que $n' \in M_3$ y por consiguiente $n' \in M$
- b) $n \in M_2$, entonces $n' \leq m$, si $n' = m$, resulta que $n' = m \in M_1$ y $n' \in M$. Si $n' < m$, entonces $n' \in M_2$ y $n' \in M$.
- c) $n \in M_3$, entonces $m < n < n'$ y $n' \in M$

En cualquiera de los casos resulta, por el principio de inducción que $M = \mathbb{N}$. Los M_j , $j = 1, 2, 3$, son disjuntos entre sí por la antisimetría y no reflexividad de $<$, ver 3.1.4, 10) y 3.1.4, 11). Por consiguiente \mathcal{M} es una partición de \mathbb{N} y cada número natural $n \in \mathbb{N}$ está en uno y sólo uno de los conjuntos M_j , $j = 1, 2, 3$. \square

3.1.3. Algoritmo Euclídeo de la División. Una herramienta muy útil en el álgebra de números naturales y enteros y en el álgebra en general, es el algoritmo euclídeo.

TEOREMA 3.8. *Dados dos números naturales $m \in \mathbb{N}$, $n \in \mathbb{N} \setminus \{0\}$, $\exists q, r \in \mathbb{N}$, $0 \leq r < n$, tales que*

$$(3.23) \quad m = q \cdot n + r$$

DEMOSTRACIÓN. Sea $n \in \mathbb{N} \setminus \{0\}$ un número natural cualquiera distino de 0 y considéremos el conjunto $N_n := \{x \in \mathbb{N} \mid \exists q, r \in \mathbb{N}, 0 \leq r < n, x = q \cdot n + r\}$. Vamos a mostrar que $N_n = \mathbb{N}$, $\forall n \in \mathbb{N} \setminus \{0\}$. En efecto $0 \in N_n$, pues $q = 0 = r$ satisfacen lo deseado. $1 \in N_n$, pues si $n = 1$ entonces $q = 1, r = 0$ satisfacen lo deseado. Si $1 < n$ y $q = 0, r = 1$ satisfacen lo deseado. Supongamos ahora que $m \in N_n$ y que $m = q \cdot n + r$, $0 \leq r < n$, entonces $m' = m + 1 = q \cdot n + r + 1 = q \cdot n + r'$. Como $r < n$, entonces $r' \leq n$. Si $r = n$, entonces $m' = q \cdot n + n = (q + 1) \cdot n$ y $q', r = 0$ satisfacen lo deseado. Si $r' < n$, entonces q, r' satisfacen lo deseado y $m' \in N_n$. Entonces, por el principio de inducción $N_n = \mathbb{N}$. \square

Al número q en 3.23 lo llamamos el *cociente de m respecto de n* , y a r el *resto*.

Decimos que n divide a m , denotado $n \mid m$ si en (3.23) $r = 0$. En tal caso decimos que n es un divisor de m . Si n es un divisor de m y $n \neq m$, entonces diremos que n es un divisor propio de m . Si en (3.23) $r \neq 0$, diremos que n no divide a m , denotado $n \nmid m$.

Decimos que un número natural $p \in \mathbb{N}$ es primo, si $p \neq 1$ y sus únicos divisores son p y 1, es decir, si su único divisor propio es 1.

Decimos que un número natural $n \in \mathbb{N}$ es producto de números primos, si n es primo o si existen números primos, no necesariamente distintos, p_1, \dots, p_r , tales que

$$n = p_1 \cdot p_2 \cdot \dots \cdot p_r.$$

TEOREMA 3.9. *Todo número natural mayor que 1 posee una representación como producto de números primos.*

DEMOSTRACIÓN. Consideremos el conjunto

$$N := \{x \in \mathbb{N} \mid \forall y \leq x, y \text{ es producto de números primos, } y = 1 \vee y = 0\}$$

Vamos a mostrar que $N = \mathbb{N}$. En efecto, es obvio que $0, 1 \in N$. Sea ahora $n \in N$, $n > 1$, entonces $\forall y \leq n, y = 0 \vee y = 1 \vee y$ es producto de números primos. Consideremos entonces n' , si n' es primo, $n' \in N$. Supongamos que n' no es primo. Entonces existen $q, m \in \mathbb{N}$, $q \neq 1 \neq m$, tales que $n' = m \cdot q$, como $m \mid n'$ y $q \mid n'$, por ejercicio 3.1.4.18), $q < n'$, $m < n'$, entonces $q \leq n$ y $m \leq n$ y como $n \in N$, resulta que ambos son productos de números primos, $q = p_1 \cdot p_2 \cdot \dots \cdot p_r$, $m = q_1 \cdot q_2 \cdot \dots \cdot q_s$. Por consiguiente $n' = p_1 \cdot p_2 \cdot \dots \cdot p_r \cdot q_1 \cdot q_2 \cdot \dots \cdot q_s$ es también producto de números primos por lo que $n' \in N$, entonces por el principio de inducción $N = \mathbb{N}$. \square

3.1.4. Ejercicios y Complementos.

1. Si $x, y \in \mathbb{N}$, mostrar que $x + y = 0 \Rightarrow x = 0 \wedge y = 0$.
2. Dado $x \in \mathbb{N}$ definimos $2x := x + x$, para $n \geq 2$ definimos recursivamente $n'x := nx + x$. Mostrar que $nx = n \cdot x$, $\forall x, n \in \mathbb{N}$.
3. Dado $x \in \mathbb{N}$ definimos $x^0 := 1$, para $n \geq 0$ definimos recursivamente $x^{n'} := x \cdot x^n$. Mostrar que $\forall x, m, n \in \mathbb{N}$, $x^n \cdot x^m = x^{n+m}$ y que $(x^n)^m = x^{n \cdot m}$.
4. Si $x, y \in \mathbb{N}$, mostrar que $x \cdot y = 1 \Rightarrow x = 1 \wedge y = 1$.
5. Mostrar que para cada $m, n \in \mathbb{N}$ vale lo siguiente:
 - a) $(m + n')' = m' + n'$
 - b) $(m \cdot n')' = m \cdot n + m'$
 - c) $(m' \cdot n')' = m' + m \cdot n + n'$.
 - d) $m' + n' = (m + n)' + 1$
 - e) $m' \cdot n' = (m \cdot n)' + (m + n)$.
6. Mostrar que para $m, n, p, q \in \mathbb{N}$ vale lo siguiente:
 - a) $(m + n) \cdot (p + q) = (m \cdot p + m \cdot q) + (n \cdot p + n \cdot q)$
 - b) $m \cdot (m + p) \cdot q = (m \cdot n) \cdot q + m \cdot (p \cdot q)$
 - c) $m \cdot (n + p + q) = m \cdot n + m \cdot p + m \cdot q$.
7. Mostrar que $x + r = y + r \Rightarrow x = y$, $\forall x, y, r \in \mathbb{N}$. (Ley de cancelación de la suma)
8. Mostrar que $n \cdot x = n \cdot y \Rightarrow x = y$, $\forall x \in \mathbb{N}$, $n \neq 0$ (Ley de cancelación del producto)
9. Mostrar que $\forall x, y \in \mathbb{N}$, $x \leq y \wedge y \leq x \Rightarrow x = y$.
10. Mostrar que $\forall x \in \mathbb{N}$, $x \not< x$, es decir que $<$ no es reflexiva.
11. Mostrar que $\forall x, y \in \mathbb{N}$ no pueden valer al mismo tiempo $x < y \wedge y < x$. Es decir que $<$ no es simétrica. Mostrar, además, que $<$ es transitiva.
12. Si $m, n \in \mathbb{N}$ y $m \leq n$, mostrar que entonces $\forall p \in \mathbb{N}$, $m + p \leq n + p$.

13. Mostrar que si $S := \{x \in \mathbb{N} \mid n < x < n', \forall n \in \mathbb{N}\}$, entonces $S = \emptyset$.
14. Sean $m, n \in \mathbb{N}$. Mostrar que vale lo siguiente:
 - a) Si $m = n$, entonces $k' \cdot m > n, \forall k \in \mathbb{N}$.
 - b) Si $k' \cdot m = n$, para algún $k \in \mathbb{N}$, entonces $m < n$.
15. Mostrar que $p \mid (n+m) \wedge p \mid n \Rightarrow p \mid m$.
16. Mostrar que $\forall m, n \in \mathbb{N}, m \leq m \cdot n \wedge n \leq m \cdot n$.
17. Mostrar que $p \mid 0, \forall p \in \mathbb{N}$.
18. Mostrar que si $p \mid n, n \neq 0$, entonces $p \leq n$. Si p es divisor propio, entonces $p < n$
19. Mostrar que $\forall n, m \in \mathbb{N}, n \mid m \wedge m \mid n \Rightarrow n = m$.
20. Mostrar que todo subconjunto de \mathbb{N} posee un elemento más pequeño, es decir que (\mathbb{N}, \leq) está bien ordenado.

3.2. Los Números Enteros

En esta sección daremos una construcción formal de los números enteros a partir de los números naturales y demostraremos algunas de sus propiedades más importantes, de las cuales haremos uso más adelante.

3.2.1. Construcción, Propiedades Generales y Operaciones Algebraicas. Consideremos sobre $\mathbb{N} \times \mathbb{N}$ la relación \sim definida por:

$$(3.24) \quad (n, m) \sim (r, s) \Leftrightarrow n + s = m + r$$

TEOREMA 3.10. *La relación \sim es una relación de equivalencia sobre $\mathbb{N} \times \mathbb{N}$.*

DEMOSTRACIÓN.

1. \sim es reflexiva: En efecto, $(n, m) \sim (n, m)$, ya que $n + m = m + n$, por la comutatividad de la suma de números naturales.
2. \sim es reflexiva: En efecto, si $(n, m) \sim (r, s)$, entonces $n + s = m + r$ y por la comutatividad de la suma de números naturales $s + n = r + m$, por consiguiente $(r, s) \sim (n, m)$.
3. \sim es transitiva: En efecto, si $(n, m) \sim (r, s) \sim (p, q)$, entonces se tiene:

$$(3.25) \quad n + s = m + r$$

$$(3.26) \quad r + q = s + p$$

De (3.25) y (3.26) se obtiene(!):

$$(3.27) \quad (n + s) + q = (m + s) + p$$

entonces por ejercicio 3.1.4,7), resulta

$$(3.28) \quad m + q = n + p$$

Por consiguiente $(n, m) \sim (p, q)$.

□

Por $[n, m]$ denotaremos la clase de equivalencia del elemento (n, m) y definimos

$$\mathbb{Z} := (\mathbb{N} \times \mathbb{N}) / \sim := \{[n, m] \mid (n, m) \in \mathbb{N} \times \mathbb{N}\}$$

como el conjunto de los *números enteros*. Un *número entero* es entonces una clase de equivalencia $[n, m]$.

De la definición de \sim resulta entonces $[0, 0] = [n, n], \forall n \in \mathbb{N}$, la clase $[n, 0] = [n+k, k], \forall n, k \in \mathbb{N}$ y la clase $[0, n] = [k, n+k], \forall n, k \in \mathbb{N}$.

Así, por ejemplo: $[5, 2]$ es de la forma $[n+k, k]$, donde $k = 2, n = 3$ y es, entonces, igual a la clase $[3, 0]$ y la clase $[6, 8]$ es de la forma $[k, n+k]$, donde $k = 6, n = 2$ y es, entonces, igual a la clase $[0, 2]$. En general toda clase $[n, m]$ puede ser identificada con una clase de la forma $[l, 0]$ o de la forma $[0, k]$. Si $n < m$, entonces, de la definición de $<$, $m = n+k$ y $[n, m] = [n, n+k] = [0, k]$. Si $m < n$, entonces $[n, m] = [m+l, m] = [l, 0]$.

3.2.1.1. Suma de Enteros. Por medio de:

$$(3.29) \quad [n, m] + [k, l] := [n+k, m+l] :$$

se define una operación binaria

$+ : \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}$, que llamaremos la *suma de enteros* o *adición*. Es de observar que la operación $+$ dentro de los corchetes es la suma de números naturales, anteriormente definida.

TEOREMA 3.11. $+ : \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}$ está bien definida, es decir no depende de la escogencia del representante de la clase de equivalencia.

DEMOSTRACIÓN. En efecto, sean $[\bar{n}, \bar{m}]$ y $[\bar{p}, \bar{q}]$ otros representantes de $[n, m]$ y $[p, q]$ respectivamente. Entonces valen las igualdades:

$$(3.30) \quad n + \bar{m} = m + \bar{n}$$

y

$$(3.31) \quad p + \bar{q} = q + \bar{p}$$

vamos a mostrar que entonces $[n, m] + [p, q] = [n+p, m+q] = [\bar{n}, \bar{m}] + [\bar{p}, \bar{q}] = [\bar{n} + \bar{p}, \bar{m} + \bar{q}]$. Es decir tenemos que mostrar que

$$(3.32) \quad (n + p) + (\bar{m} + \bar{q}) = (m + q) + (\bar{n} + \bar{p})$$

En efecto,

$$(3.33) \quad (n + p) + (\bar{m} + \bar{q}) = (n + \bar{m}) + (p + \bar{q})$$

$$(3.34) \quad = (m + \bar{n}) + (q + \bar{p}), \text{ por (3.30) y (3.31)}$$

$$(3.35) \quad = (m + q) + (\bar{n} + \bar{p})$$

lo que prueba la aserción. □

El lector comprobará fácilmente las siguientes propiedades de la suma de enteros.

TEOREMA 3.12. $+ : \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}$ posee las siguientes propiedades:

1. $+$ es cerrada en \mathbb{Z} .
2. $+$ es asociativa.
3. $+$ es conmutativa
4. $[n, n] = [0, 0]$ es elemento neutro de $+$ en \mathbb{Z} . Además, si $[x, y] + [n, m] = [n, m]$, $\forall [n, m] \in \mathbb{Z}$, entonces $[x, y] = [0, 0]$. Es decir que el elemento neutro es único.
5. $[n, m]$ es simétrico o inverso respecto de $+$ de $[m, n]$.

La demostración se deduce de forma inmediata de las propiedades de la suma de números naturales y la dejamos al lector como un ejercicio. (ver 3.2.2.1))

COROLARIO 3.13. $(\mathbb{Z}, +)$ es un grupo abeliano.

Dado un número entero $\alpha := [n, m]$, al número $[m, n]$, su inverso adivito, lo denotaremos por $-\alpha$. Vamos a definir la *substracción* o resta de dos enteros α, β como

$$(3.36) \quad \alpha - \beta := \alpha + (-\beta)$$

3.2.1.2. Producto de Enteros. Al igual que en \mathbb{N} podemos definir sobre \mathbb{Z} otra operación binaria $\cdot : \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}$, que llamaremos *producto* o *multiplicación* de enteros, por medio de:

$$(3.37) \quad [n, m] \cdot [p, q] := [n \cdot p + m \cdot q, n \cdot q + m \cdot p]$$

De nuevo las operaciones en los corchetes son la suma y producto de números naturales.

TEOREMA 3.14. $\cdot : \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}$ está bien definida.

DEMOSTRACIÓN. Utilizando la notación del teorema 3.11, tenemos que mostrar que

$$(3.38) \quad (n \cdot p + m \cdot q) + (\bar{n} \cdot \bar{q} + \bar{m} \cdot \bar{p}) = (n \cdot q + m \cdot p) + (\bar{n} \cdot \bar{p} + \bar{m} \cdot \bar{q})$$

En efecto, consideremos la siguiente igualdad:

$$(3.39)$$

$$\begin{aligned} & (n + \bar{m})(p + \bar{p}) + (\bar{n} + m) \cdot (q + \bar{q}) + (p + \bar{q}) \cdot (n + \bar{n}) + (q + \bar{p}) \cdot (m + \bar{m}) = \\ & 2(n \cdot p + \bar{m} \cdot \bar{p} + m \cdot q + \bar{n} \cdot \bar{q}) + \bar{n} \cdot p + m \cdot \bar{p} + n \cdot \bar{q} + \bar{m} \cdot q + \bar{p} \cdot n + q \cdot \bar{n} + \bar{q} \cdot m + p \cdot \bar{m} \end{aligned}$$

Por (3.30) y (3.31) se tiene

$$(3.40)$$

$$\begin{aligned} & (n + \bar{m})(p + \bar{p}) + (\bar{n} + m) \cdot (q + \bar{q}) + (p + \bar{q}) \cdot (n + \bar{n}) + (q + \bar{p}) \cdot (m + \bar{m}) = \\ & (m + \bar{n})(p + \bar{p}) + (\bar{m} + n) \cdot (q + \bar{q}) + (q + \bar{p}) \cdot (n + \bar{n}) + (p + \bar{q}) \cdot (m + \bar{m}) = \\ & 2(n \cdot q + \bar{n} \cdot \bar{p} + m \cdot p + \bar{m} \cdot \bar{q}) + \bar{n} \cdot p + m \cdot \bar{p} + n \cdot \bar{q} + \bar{m} \cdot q + \bar{p} \cdot n + q \cdot \bar{n} + \bar{q} \cdot m + p \cdot \bar{m} \end{aligned}$$

De (3.39) y (3.40) y utilizando las leyes de cancelación de los ejercicios 3.1.4,7) y 3.1.4,8) se obtiene

$$(3.41) \quad n \cdot p + \bar{m} \cdot \bar{p} + m \cdot q + \bar{n} \cdot \bar{q} = n \cdot q + \bar{n} \cdot \bar{p} + m \cdot p + \bar{m} \cdot \bar{q}$$

reordenando los términos en la ecuación (3.41), se obtiene la ecuación (3.38). \square

TEOREMA 3.15. $\cdot : \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}$ posee las siguientes propiedades:

1. \cdot es cerrada en \mathbb{Z}
2. \cdot es asociativa
3. \cdot es conmutativa
4. $[1, 0]$ es elemento neutro en \mathbb{Z} de \cdot . Además si $[n, m] \cdot [x, y] = [n, m], m, \forall [n, m] \in \mathbb{Z}$, entonces $[x, y] = [1, 0]$. Es decir que el elemento neutro respecto de \cdot es único.
5. \cdot es distributiva respecto de $+$

DEMOSTRACIÓN. Únicamente demostraremos la asociatividad, dejando como ejercicio la demostración de las demás propiedades. En efecto

$$\begin{aligned} [n, m] \cdot ([p, q] \cdot [r, s]) &= [n, m] \cdot [p \cdot r + q \cdot s, p \cdot s + q \cdot r] \\ &= [n \cdot (p \cdot r + q \cdot s) + m \cdot (p \cdot s + q \cdot r), n \cdot (p \cdot s + q \cdot r) + m \cdot (p \cdot r + q \cdot s)] \\ &= [(n \cdot p + m \cdot q) \cdot r + (n \cdot q + m \cdot p) \cdot s, (n \cdot p + m \cdot q) \cdot s + (n \cdot q + m \cdot p)r] \\ &= ([n \cdot p + m \cdot q, n \cdot q + m \cdot p]) \cdot [r, s] \\ &= ([n, m] \cdot [p, q]) \cdot [r, s] \end{aligned}$$

\square

Del corolario 3.13 y del teorema 3.15 se obtiene el siguiente corolario:

COROLARIO 3.16. *$(\mathbb{Z}, +, \cdot)$ es un anillo conmutativo con unidad.*

Dado un número entero $\alpha := [n, m]$, por la ley de tricotomía de \mathbb{N} , vale una y sólo una de las siguientes aserciones: $n < m$, $m < n$, $m = n$. Por consiguiente todo número entero está, exclusivamente, en una única clase $[l, 0]$, $[0, k]$ o $[0, 0]$. A los elementos del subconjunto de \mathbb{Z} , $\mathbb{Z}^+ := \{[n, 0] \mid n \neq 0\}$ los llamaremos los *enteros positivos* y a \mathbb{Z}^+ el subconjunto de los enteros positivos. A los elementos del subconjunto de \mathbb{Z} , $\mathbb{Z}^- := \{[0, n] \mid n \neq 0\}$ los llamaremos los *enteros negativos* y \mathbb{Z}^- el subconjunto de los enteros negativos. Entonces, si $\bar{0} := \{[0, 0]\}$, la familia $\mathcal{Z} := \{\bar{0}, \mathbb{Z}^+, \mathbb{Z}^-\}$ es una partición de \mathbb{Z} . Por consiguiente, dado un número entero α , vale que, éste es positivo, negativo o 0, de forma exclusiva.

Por medio de la aplicación inyectiva $i : \mathbb{N} \rightarrow \mathbb{Z}$, definida por $i(n) := [n, 0]$, $\forall n \in \mathbb{N}$, podemos identificar al conjunto \mathbb{N} con el subconjunto $\{[n, 0] \mid n \in \mathbb{N}\}$ de \mathbb{Z} . De este modo identificaremos al número natural n , con el entero $[n, 0]$. Por otra parte si $\alpha \in \mathbb{Z}$, por lo anteriormente expuesto, α está en uno y sólo uno de los tres conjuntos que integran \mathcal{Z} , si $\alpha \in \mathbb{Z}^+$, $\alpha = [l, 0]$ para un único $l \in \mathbb{N}$ e identificaremos a α con el natural l . Si $\alpha \in \mathbb{Z}^-$, entonces $\alpha = [0, k]$ para un único $k \in \mathbb{N}$ e identificaremos a α con $-k := [0, k]$. Si $\alpha \in \bar{0}$, identificaremos a α con el 0 $\in \mathbb{N}$.

3.2.2. Ejercicios y Complementos.

1. Completar la demostración del teorema 3.12.
2. Completar la demostración del teorema 3.15.
3. Mostrar que \mathbb{Z}^+ y \mathbb{Z}^- son cerrados respecto de $+$.
4. Mostrar que \mathbb{Z}^+ es cerrado respecto del producto \cdot .
5. Mostrar que $-(\alpha + \beta) = -\alpha + (-\beta)$
6. Mostrar que $[n, 0] \cdot [0, m] = [0, n \cdot m]$ es decir el producto de un número positivo con uno negativo es siempre negativo.
7. Mostrar que $-(-\alpha) = \alpha$, $\forall \alpha \in \mathbb{Z}$.
8. Mostrar que $(-\alpha) \cdot (-\beta) = \alpha \cdot \beta$, $(-\alpha) \cdot \beta = -(\alpha \cdot \beta)$, $\forall \alpha, \beta \in \mathbb{Z}$.
9. Mostrar que $[0, n] \cdot [0, m] = [n \cdot m, 0]$ es decir que el producto de dos números negativos es positivo.
10. Mostrar que $[n, m] \in \mathbb{Z}^+$ Ssi $n > m$.
11. Mostrar que $\alpha := [n, m] \in \mathbb{Z}^-$ Ssi $n < m$
12. Mostrar que $\alpha := [n, m] \in \mathbb{Z}^+ \Leftrightarrow -\alpha = [m, n] \in \mathbb{Z}^-$, $\forall \alpha \in \mathbb{Z}$.
13. La Relación \leqslant sobre \mathbb{Z} . Dados $[n, m], [p, q] \in \mathbb{Z}$, diremos que $[n, m] \leqslant [p, q]$ Ssi: existe un entero $[a, b] \in \mathbb{Z} \cup \{0\}$, tal que $[p, q] = [n, m] + [a, b]$. Mostrar que \leqslant es una relación de orden sobre \mathbb{Z} y que $\forall [n, m] \in \mathbb{Z}^-, [n, m] \leqslant [0, 0]$.
14. Probar que la relación $<$, definida por $[n, m] < [p, q] \Leftrightarrow \exists [a, b] \in \mathbb{Z}^+$, tal que $[p, q] = [n, m] + [a, b]$ es una relación de orden estricto sobre \mathbb{Z} .
15. Dado $\alpha \in \mathbb{Z}$, $\alpha := [n, m]$, definimos al *sucesor* de α , como $\alpha' := [n', m]$. Mostrar que si $n = m + k$, $k > 0$, entonces $\alpha' = [k', 0]$ y si $m = n + l$, $l > 0$, entonces $\alpha' = [0, l_1]$, donde l_1 es tal que $l = l'_1$.
16. Mostrar que $\alpha < \alpha'$, $\forall \alpha \in \mathbb{Z}$.
17. Mostrar que $\alpha \leqslant \beta \Rightarrow -\beta \leqslant -\alpha \quad \forall \alpha, \beta \in \mathbb{Z}$.
18. Mostrar que $\alpha < \beta$, $\forall \alpha \in \mathbb{Z}^-, \forall \beta \in \mathbb{Z}^+ \cup \{0\}$.
19. Mostrar que si $\alpha \leqslant \beta$ y $\gamma \in \mathbb{Z}$, entonces $\alpha + \gamma \leqslant \beta + \gamma$. Mostrar también que si $\gamma \in \mathbb{Z}^+$, entonces $\alpha \cdot \gamma \leqslant \beta \cdot \gamma$. Mientras que si $\gamma \in \mathbb{Z}^-$, entonces $\beta \cdot \gamma \leqslant \alpha \cdot \gamma$.

20. Decimos que β es *predecesor* de α , donde $\alpha, \beta \in \mathbb{Z}$, si $\alpha = \beta'$. A diferencia de los naturales, mostrar que todo número entero es predecesor de otro y que todo número entero es sucesor de otro.

3.2.3. Valor absoluto y Algoritmo Euclídeo.

OBSERVACIÓN. Por abuso de notación y con la finalidad de simplificarla, en lo sucesivo escribiremos $\alpha\beta$ en lugar de $\alpha \cdot \beta$. De forma análoga para el producto en \mathbb{N} .

3.2.3.1. Valor Absoluto.

DEFINICIÓN 3.3. Dado $\alpha \in \mathbb{Z}$, definimos

$$(3.42) \quad |\alpha| := \begin{cases} \alpha & \text{si } \alpha \in \mathbb{Z}^+ \cup \{0\} \\ -\alpha & \text{si } \alpha \in \mathbb{Z}^- \end{cases}$$

$|\alpha|$ lo llamamos el *valor absoluto* de α .

Entonces $||$ es una aplicación $|| : \mathbb{Z} \rightarrow \mathbb{N}$. Si $\alpha = [n, 0]$, $|\alpha| = n$. Para $\alpha = [0, n]$, $-\alpha = [n, 0]$ y $|\alpha| = n$.

TEOREMA 3.17. $|| : \mathbb{Z} \rightarrow \mathbb{N}$ posee las siguientes propiedades

$$1. \forall \alpha \in \mathbb{Z}$$

$$(3.43) \quad \alpha \leq |\alpha|$$

$$2. \forall \alpha, \beta \in \mathbb{Z}$$

$$(3.44) \quad |\alpha\beta| = |\alpha||\beta|$$

$$3. \forall \alpha, \beta \in \mathbb{Z}$$

$$(3.45) \quad |\alpha + \beta| \leq |\alpha| + |\beta|$$

$$4. Si \beta \in \mathbb{Z}^+, entonces$$

$$(3.46) \quad |\alpha| \leq \beta \Leftrightarrow -\beta \leq \alpha \leq \beta$$

DEMOSTRACIÓN.

1. La desigualdad (3.43) resulta inmediata del ejercicio 3.2.2,18.

2. Para mostrar la igualdad (3.44) consideremos tres casos:

- a) $\alpha, \beta \in \mathbb{Z}^+ \cup \{0\}$. Entonces $|\alpha| = \alpha$, $|\beta| = \beta$ y $\alpha\beta \in \mathbb{Z}^+ \cup \{0\}$, por consiguiente $\alpha\beta = |\alpha\beta|$ de donde resulta la igualdad (3.44).
- b) $\alpha, \beta \in \mathbb{Z}^-$. Entonces, por ejercicio 3.2.2,9), $\alpha\beta \in \mathbb{Z}^+$ y $|\alpha\beta| = \alpha\beta$. Por otra parte $|\alpha| = -\alpha$, $|\beta| = -\beta$ y $|\alpha\beta| = (-\alpha)(-\beta) = \alpha\beta$, por ejercicio 3.2.2,8). Por consiguiente vale la igualdad (3.44).
- c) $\alpha \in \mathbb{Z}^-, \beta \in \mathbb{Z}^+$. Entonces $\alpha\beta \in \mathbb{Z}^-$ y $|\alpha\beta| = -(\alpha\beta) = (-\alpha)(\beta) = |\alpha||\beta|$.

3. Para mostrar la desigualdad (3.45) consideremos los casos siguientes:

- a) $\alpha, \beta \in \mathbb{Z}^+ \cup \{0\}$. Entonces, por ejercicio 3.2.2,3), $(\alpha + \beta) \in \mathbb{Z}^+ \cup \{0\}$ y $|\alpha + \beta| = \alpha + \beta = |\alpha| + |\beta|$.

- b) $\alpha, \beta \in \mathbb{Z}^-$. Entonces, por ejercicio 3.2.2,3), $(\alpha + \beta) \in \mathbb{Z}^-$ y $|\alpha + \beta| = -(\alpha + \beta) = -\alpha + (-\beta) = |\alpha| + |\beta|$.

- c) $\alpha \in \mathbb{Z}^+ \cup \{0\}, \beta \in \mathbb{Z}^-$. Entonces se dan dos casos:

- i) $(\alpha + \beta) \in \mathbb{Z}^-$. entonces $|\alpha + \beta| = -(\alpha + \beta) = -\alpha + |\beta| < |\alpha| + |\beta|$.

- ii) $(\alpha + \beta) \in \mathbb{Z}^+$. Entonces $|\alpha + \beta| = (\alpha + \beta) = |\alpha| + \beta < |\alpha| + |\beta|$.

4. Sea $\beta \in \mathbb{Z}^+$, y supongamos que vale $-\beta \leq \alpha \leq \beta$. Si $\alpha \in \mathbb{Z}^+ \cup \{0\}$, entonces $|\alpha| = \alpha \leq \beta$. Si $\alpha \in \mathbb{Z}^-$, entonces $|\alpha| = -\alpha$ y $-\beta \leq \alpha \Rightarrow -\alpha \leq \beta$, por consiguiente $|\alpha| \leq \beta$.

Supongamos ahora que $|\alpha| \leq \beta$. Si $\alpha \in \mathbb{Z}^+ \cup \{0\}$, entonces, como $\beta \in \mathbb{Z}^+, -\beta \in \mathbb{Z}^-$ y, por ejercicio 3.2.2,18, $-\beta \leq \alpha = |\alpha| \leq \beta$. Si $\alpha \in \mathbb{Z}^-$, entonces $|\alpha| = -\alpha \leq \beta$ y, por ejercicio 3.2.2,17), $-\beta \leq \alpha \leq -\alpha \leq \beta$.

□

3.2.3.2. Algoritmo Euclídeo para Enteros. En analogía a los números naturales, también existe un algoritmo euclídeo de la división para los enteros.

TEOREMA 3.18. *Dados dos números enteros α, β distintos de 0, existen un único $q \in \mathbb{Z}$ y un único $r \in \mathbb{Z}$, $0 \leq r < |\beta|$, tales que*

$$(3.47) \quad \alpha = q\beta + r$$

q se llama el cociente de α por β y r el resto.

DEMOSTRACIÓN. Sean α, β dos enteros cualesquiera distintos de 0 y consideremos los siguientes conjuntos:

$$Z := \{x \in \mathbb{Z} \mid \alpha - \beta x \geq 0\}, \quad R := \{y \mid y := \alpha - \beta x, x \in Z\}$$

Vamos a mostrar, primeramente, que $Z \neq \emptyset$. En efecto, supongamos $\beta \in \mathbb{Z}^-$, entonces $\beta \leq -1$ y por 3.2.2,19), $|\alpha|\beta \leq -|\alpha| \leq \alpha$, entonces $\alpha - |\alpha|\beta \geq 0$, y $|\alpha| \in Z$. Si $\beta > 0$, entonces $\beta \geq 1$ y por 3.2.2,19), $\alpha \geq -|\alpha| \geq \beta(-|\alpha|)$, entonces $0 \leq \alpha - \beta(-|\alpha|)$ y $-|\alpha| \in Z$. Por consiguiente, $Z \neq \emptyset$ en cualquier caso. Entonces $R \neq \emptyset$ y es un subconjunto de \mathbb{N} , ya que sus elementos son enteros positivos. Entonces, como \mathbb{N} está bien ordenado, (ver ejercicio 3.1.4,20), R posee un elemento más pequeño r . Sea $q \in Z$, tal que $r = \alpha - q\beta$. Obviamente $0 \leq r$. Vamos a mostrar que $r < |\beta|$. Supongamos que $r \geq |\beta|$, entonces, si $\beta \in \mathbb{Z}^-$ tendríamos $\alpha - q\beta \geq |\beta| = -\beta$ y $r_1 := \alpha - \beta(q-1) \geq 0$, por lo que $r_1 \in R$, pero $r - r_1 = -\beta = |\beta| > 0$, lo que implicaría que $r_1 < r$, en contradicción a que r es el elemento más pequeño de R . En el caso en que $\beta > 0$, por un razonamiento análogo, se obtiene $r - r_1 = \beta > 0$ y nuevamente tendríamos $r_1 < r$. Por consiguiente, en cualquier caso, $r < |\beta|$.

Unicidad de q y r : Supongamos que existen $q_1 \neq q$ y $r_1 \neq r$ que satisfacen también la igualdad (3.47), y $0 \leq r_1 < |\beta|$. De las desigualdades

$$(3.48) \quad r < |\beta|$$

$$(3.49) \quad r_1 < |\beta|$$

Se obtienen las desigualdades

$$(3.50) \quad r - r_1 < |\beta|$$

$$(3.51) \quad r_1 - r < |\beta|$$

Las cuales implican

$$(3.52) \quad -|\beta| < r - r_1 < |\beta|$$

y por teorema 3.17, inecuación (3.46)

$$(3.53) \quad |r - r_1| < |\beta|$$

Por otra parte se tienen las igualdades

$$(3.54) \quad \alpha = q\beta + r = q_1\beta + r_1$$

De donde se obtiene

$$(3.55) \quad (q_1 - q)\beta = (r - r_1)$$

de la igualdad (3.55) resulta que $|\beta| \mid |r - r_1|$, en contradicción a la desigualdad (3.53). Por consiguiente $r - r_1 = 0$ y por la igualdad (3.55), también $q - q_1 = 0$. \square

En forma análoga que en \mathbb{N} , si $r = 0$ en la igualdad (3.47), entonces se dice que β divide a α , denotado $\beta \mid \alpha$. Decimos que $d \in \mathbb{Z}$ es un divisor común de α y β , si $d \mid \alpha$ y $d \mid \beta$. En tal caso, existen enteros α_1, β_1 , tales que

$$\alpha = d\alpha_1, \quad \beta = d\beta_1$$

Dados dos enteros α, β y d un divisor común, entonces, por el algoritmo euclídeo, se tiene

$$\alpha = q\beta + r, \quad 0 \leq r < |\beta|$$

como $d \mid \alpha$ y $d \mid \beta$, por ejercicio 15, $d \mid r$.

OBSERVACIÓN. El lector podrá verificar fácilmente que pasando a valores absolutos las propiedades de los divisores en \mathbb{Z} son las mismas que en \mathbb{N} .

Supongamos que $d > 0$ es un divisor común de α, β y supongamos que $\alpha > \beta$. Consideremos las siguientes igualdades

$$(3.56) \quad \alpha = q\beta + r$$

$$(3.57) \quad \beta = q_1 r + r_1$$

$$(3.58) \quad r = q_2 r_1 + r_2$$

Si asumimos, por ejemplo, que $r_2 = 0$, nótese que entonces r_1 es un divisor común de α y β , y que $d \mid r_1$, por lo que $r_1 \geq d$.

Bajo nuestra suposición de que $r_2 = 0$, entonces, de las igualdades (3.57) y (3.56), resulta

$$(3.59) \quad r_1 = \beta - q_1 r = \beta - q_1(\alpha - q\beta) = \gamma\alpha + \delta\beta$$

donde $\gamma := -q_1 \in \mathbb{Z}$ y $\delta := (1 + qq_1) \in \mathbb{Z}$.

Decimos que \bar{d} es máximo común divisor, (MCD), de α, β , denotado $\bar{d} = (\alpha, \beta)$, si \bar{d} es divisor común de α, β y dado otro divisor común d , entonces $d \mid \bar{d}$.

Nótese que, r_1 , obtenido en la igualdad (3.57), es, en este caso, el MCD de α, β . Si r_2 , no fuera 0 en la igualdad (3.58), continuamos aplicando el algoritmo euclídeo a r_1, r_2 , si el resto r_3 obtenido no fuera 0, continuamos aplicando el algoritmo a r_2, r_3 y así sucesivamente. Como los restos van decreciendo y son mayores o iguales a 0, al cabo de un número finito de pasos se obtiene, digamos $r_n = 0$, entonces r_{n-1} es el MCD de α, β . El lector comprobará, fácilmente, que si d es un divisor común de α, β , d divide a todos los restos r_i , $i = 1, \dots, n-1$, por lo que $d \mid r_{n-1}$, por otra parte, $r_{n-1} \mid r_{n-2}, r_{n-1} \mid r_{n-3}, \dots, r_{n-1} \mid r, r_{n-1} \mid \beta, r_{n-1} \mid \alpha$.

El siguiente teorema resume estos resultados.

TEOREMA 3.19. *Dados dos números enteros distintos de 0, α, β , $\alpha > \beta$, entonces el máximo común divisor de éstos es igual a r_{n-1} , donde r_{n-1} es el resto de aplicar el algoritmo euclídeo a los restos r_{n-3}, r_{n-2} y el resto r_n de aplicar el algoritmo euclídeo a r_{n-2}, r_{n-1} es igual a 0.*

Por otra parte, si $\bar{d} = (\alpha, \beta)$, entonces existen $\gamma, \delta \in \mathbb{Z}$, tales que

$$(3.60) \quad \bar{d} = \gamma\alpha + \delta\beta$$

DEMOSTRACIÓN. Ya vimos que si $n = 2$, r_1 es, en efecto, el MCD de α, β y que existen enteros γ, δ , tales que la igualdad (3.60) se satisface. Supongamos, por hipótesis de inducción, que el teorema sea verdadero para $n - 1 > 2$ y mostremos que vale para n . Supongamos, pues, que en el proceso de aplicar sucesivamente el algoritmo euclídeo a α, β y sus restos respectivos, $r_n = 0$. Si r es el resto de aplicar el algoritmo euclídeo a α, β , partamos entonces aplicando el algoritmo euclídeo a β, r . Por hipótesis de inducción r_{n-1} es entonces el MCD de β y r . Entonces, como $\alpha = q\beta + r$ resulta que $r_{n-1} \mid \alpha$ y si d es divisor común de α, β , $d \mid r_{n-1}$. Por lo que r_{n-1} es MCD de α, β .

En forma análoga, por hipótesis de inducción, para β, r , existen enteros γ, δ_1 , tales que

$$(3.61) \quad r_{n-1} = \delta_1\beta + \gamma r$$

entonces, como

$$(3.62) \quad r = \alpha - q\beta$$

de (3.61) y (3.62), se obtiene

$$(3.63) \quad r_{n-1} = \delta_1\beta + \gamma(\alpha - q\beta) = \gamma\alpha + \delta\beta$$

donde $\delta := (\delta_1 - \gamma q)$. □

Decimos que dos números enteros α, β son *primos relativos* si $1 = (\alpha, \beta)$, es decir que su único divisor común es 1.

Con la ayuda de la igualdad (3.60), estamos ahora en condiciones de demostrar ciertas propiedades de la divisibilidad de números enteros.

TEOREMA 3.20. *Sean α, β, η , tres números enteros. Si $1 = (\alpha, \eta)$ y $\eta \mid \alpha\beta$, entonces $\eta \mid \beta$*

DEMOSTRACIÓN. En efecto, si $1 = (\alpha, \eta)$, entonces por teorema 3.19, existen enteros γ, δ , tales que

$$(3.64) \quad 1 = \gamma\alpha + \delta\eta$$

multiplicando la igualdad (3.64) por β , obtenemos

$$(3.65) \quad \beta = \gamma\alpha\beta + \delta\eta\beta$$

entonces $\eta \mid \beta$, ya que ambos sumandos de la igualdad (3.65) son divisibles por η . □

En el caso en que p es un número primo y $p \mid \alpha\beta$ entonces se obtiene el siguiente

TEOREMA 3.21. *Si p es un número primo que divide al producto de dos números enteros $\alpha\beta$, entonces $p \mid \alpha$ o $p \mid \beta$.*

DEMOSTRACIÓN. En efecto, como p es un número primo y $p \nmid \alpha$, entonces $1 = (\alpha, p)$ y por el teorema precedente $p \mid \beta$. De forma análoga si $p \nmid \beta$, resulta que $p \mid \alpha$. □

COROLARIO 3.22. *Sean p_1, p_2, p tres números primos. Entonces,*

$$(3.66) \quad p \mid p_1p_2 \Rightarrow p = p_1 \vee p = p_2$$

DEMOSTRACIÓN. Inmediato del teorema 3.21. □

El siguiente teorema es de suma importancia en la teoría de números enteros:

TEOREMA 3.23. *Todo número entero α posee una representación única, salvo orden de sus factores, en factores primos no necesariamente distintos.*

DEMOSTRACIÓN. En el teorema 3.9, mostramos que todo número natural posee una descomposición en factores primos. Entonces si $\alpha > 0$ α se descompone como producto de números primos. Si $\alpha < 0$, entonces $-\alpha > 0$ y si $-\alpha = p_1 p_2 \cdots p_n$, donde $p_1, p_2 \dots p_n$ son números primos, entonces $\alpha = -p_1 p_2 \cdots p_n$. Mostremos entonces la unicidad. Supongamos que $\alpha = p_1 p_2 \cdots p_n$ y $\alpha = q_1 q_2 \cdots q_m$. Entonces, cada $q_i, i = 1, \dots, m$ y cada $p_j, j = 1, \dots, n$, dividen a α . Así pues, $p_j \mid (q_1 q_2 \cdots q_m)$. Por corolario precedente, si $p_j \nmid q_1$, entonces $p_j \mid (q_2 q_3 \cdots q_m)$. Si $p_j \nmid q_2$, entonces $p_j \mid (q_3 q_4 \cdots q_m)$ y así sucesivamente, hasta llegar a un q_i , tal que $p_j \mid q_i$. Entonces, por corolario 3.22, $p_j = q_i$. Entonces si p_j se repite r veces, q_i sólo puede repetirse r veces. \square

Una forma más práctica de encontrar el MCD es la descomposición en factores primos, conocida en la escuela secundaria, en particular cuando se trata de varios números. Sin embargo, desde el punto de vista teórico, el algoritmo euclídeo nos permite deducir propiedades del MCD que no son deducibles de la descomposición en factores primos, como la igualdad (3.60), de la cual nos serviremos más adelante en la teoría de grupos.

EJEMPLOS 3.1.

1. Dados los números enteros $\alpha := 120$, $\beta := 7$, vamos a dar q y $0 \leq r < \beta$, tales que $\alpha = q\beta + r$. $120 = 17 \times 7 + 1$, $q = 17$, $r = 1$.
2. $\alpha := -15$, $\beta := 7$, entonces $-15 = t \times (-3) + 6$, $q = -3$, $r = 6$
3. Consideremos los números 430 y 120. Usaremos el algoritmo euclídeo para encontrar su MCD.

$$\begin{aligned} 430 &= 120 \times 3 + 70 \\ 120 &= 70 + 50 \\ 70 &= 50 + 20 \\ 50 &= 20 \times 2 + 10 \\ 20 &= 10 \times 2 \end{aligned}$$

Entonces $(430, 120) = 10$

4. En el ejemplo precedente, encontrar $\gamma, \delta \in \mathbb{Z}$, tales que $430\gamma + 120\delta = 10$. Como podemos observar $r_3 = 10$, entonces

$$\begin{aligned} r_3 &= r_1 - r_2 q_3 \\ r_2 &= r - r_1 q_2 \\ r_1 &= \beta - rq_1 \\ r &= \alpha = \beta q \end{aligned}$$

Por sustituciones sucesivas se obtiene

$$r_3 = \alpha(-q_1 - q_2 - q_3 q_2) + \beta(1 + qq_1 + qq_3 + q_2 q_3 + qq_1 q_2 q_3)$$

Lo que nos da entonces $\gamma = -5$ y $\delta = 18$

DEFINICIÓN 3.4 (La Función ϕ de Euler). La función $\phi : \mathbb{Z}^+ \rightarrow \mathbb{N}$, definida por

$$(3.67) \quad \phi(1) := 1$$

$$(3.68)$$

$\forall n > 1 \quad \phi(n) :=$ número de enteros positivos menores que n relativamente primos con n

Si p es un número primo, $\phi(p) = p - 1$. Si $n = 10$, $\phi(10) = 3$, ya que los enteros positivos menores que 10 y relativamente primos con 10, son $\{1, 3, 7\}$. ϕ no es creciente ni decreciente, pues, por ejemplo, $\phi(8) = 4$, pues los números enteros positivos, menores que 8 y relativamente primos con 8, son $\{1, 3, 5, 7\}$.

3.2.4. Ejercicios y Complementos.

1. Mostrar que $\forall \alpha, \beta \in \mathbb{Z}$, vale la desigualdad

$$(3.69) \quad ||\alpha| - |\beta|| \leq |\alpha - \beta|$$

2. Encontrar el MCD de los siguientes números enteros y dar γ, δ , para expresarlo como combinación de éstos.

- a) $\alpha := 237, \beta := 81$
- b) $\alpha := 470, \beta := 15$
- c) $\alpha := 616, \beta := 427$

3. Expresar los siguientes números enteros como producto de números primos:

- a) $\alpha := 19500$
- b) $\alpha := 35680$

4. Mostrar que si $\alpha \mid \beta$, entonces $-\alpha \mid \beta, \alpha \mid -\beta, -\alpha \mid -\beta, |\alpha| \mid |\beta|$.

5. Si $\gamma \neq 0$, Mostrar que $(\gamma\alpha, \gamma\beta) = |\gamma|(\alpha, \beta)$

6. Mostrar que si $\alpha \mid \gamma, \beta \mid \gamma$ y $1 = (\alpha, \beta)$, entonces $\alpha\beta \mid \gamma$.

7. Mostrar que si $\alpha = d\alpha_1$ y si $\alpha \mid \beta\alpha_1$, entonces $d \mid \beta$.

8. Decimos que η es el *mínimo común múltiplo*, (mcm), de α, β , denotado $[\alpha, \beta]$, si $\alpha \mid \eta, \beta \mid \eta$ y si γ es tal que $\alpha \mid \gamma$ y $\beta \mid \gamma$, entonces $\eta \mid \gamma$. Encontrar, por medio de descomposición en números primos:

- a) $[25, 30]$
- b) $[23, 715]$
- c) $[7, 23]$

9. Sea $n \in \mathbb{Z}^+$ y $\mathbb{Z}_n^* := \{x \in \mathbb{Z}^+ \mid x < n \text{ y } (x, n) = 1\}$. Mostrar que $\forall m, s \in \mathbb{Z}_n^*, (ms, n) = 1$.

10. Dar \mathbb{Z}_n^* , para $n \in \{2, 4, 5, 6, 7, 8, 10, 12, 16, 20, 24\}$.

11. Mostrar que sobre el conjunto de los números primos la función de Euler ϕ es estrictamente creciente.

3.3. Los Números Racionales

En esta sección daremos una construcción de los números racionales a partir de los números enteros.

3.3.1. Construcción, Propiedades Generales, Operaciones Algebraicas.

3.3.1.1. *Construcción de los Números Racionales.* Consideremos sobre $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ la relación \sim , definida de la siguiente forma:

$$(3.70) \quad (\alpha, \beta) \sim (\gamma, \delta) \Leftrightarrow \alpha\delta = \gamma\beta$$

TEOREMA 3.24. \sim es una relación de equivalencia sobre $\mathbb{Z} \times \mathbb{Z} \setminus \{0\}$

DEMOSTRACIÓN.

1. \sim es reflexiva. En efecto $(\alpha, \beta) \sim (\alpha, \beta)$, ya que $\alpha\beta = \alpha\beta$
2. \sim es simétrica. Si $(\alpha, \beta) \sim (\gamma, \delta)$, entonces $\alpha\delta = \gamma\beta$, lo que implica también que $(\gamma, \delta) \sim (\alpha, \beta)$.

3. \sim es transitiva. Si $(\alpha, \beta) \sim (\gamma, \delta) \sim (\eta, \lambda)$, entonces se tienen las igualdades

$$\alpha\delta = \gamma\beta$$

$$\gamma\lambda = \eta\delta$$

Multiplicando ambas igualdades, obtenemos

$$\alpha\delta\gamma\lambda = \gamma\beta\eta\delta$$

$$(\alpha\lambda)(\delta\gamma) = (\eta\beta)(\delta\gamma)$$

Entonces por la ley de cancelación, 3.1.4,8), se obtiene

$$\alpha\lambda = \eta\beta$$

Por consiguiente $(\alpha, \beta) \sim (\eta, \lambda)$

□

DEFINICIÓN 3.5. Al conjunto de las clases de equivalencia $\mathbb{Q} := \mathbb{Z} \times (\mathbb{Z} \setminus \{0\}) / \sim$, lo llamamos el conjunto de los números racionales. La clase de (α, β) se suele representar por $\frac{\alpha}{\beta}$ y la llamamos el *número racional de numerador α y denominador β* .

OBSERVACIÓN 3.1. Nótese que si $\alpha = d\alpha_1$, $\beta = d\beta_1$, entonces $(\alpha, \beta) \sim (\alpha_1, \beta_1)$, ya que

$$(3.71) \quad \alpha\beta_1 = \alpha_1d\beta_1 = \alpha_1\beta$$

En particular, para $d := -1$, se obtiene que $\frac{\alpha}{\beta} = \frac{-\alpha}{-\beta}$. Entonces todo número racional posee una única representación por $\frac{\alpha}{\beta}$, donde $1 = (\alpha, \beta)$ y $\beta \in \mathbb{Z}^+$, llamada la *representación canónica*.(ver ejercicio 3.3.2,5)).

Por ejemplo $\frac{25}{30} = \frac{5}{6}$.

Consideremos la aplicación $i : \mathbb{Z} \rightarrow \mathbb{Q}$, definida por $i(\alpha) := \frac{\alpha}{1}$. i es inyectiva, pues $\frac{\alpha}{1} = \frac{\beta}{1} \Rightarrow \alpha = \beta$. Entonces i mapea de forma natural \mathbb{Z} con el subconjunto de todas las clases de la forma $\frac{\alpha}{1}$, por lo que podemos considerar a \mathbb{Z} como un subconjunto de \mathbb{Q} .

3.3.1.2. Suma de Números Racionales. Dados dos números racionales $\frac{\alpha}{\beta}, \frac{\gamma}{\delta}$ se define:

$$(3.72) \quad \frac{\alpha}{\beta} + \frac{\gamma}{\delta} := \frac{\alpha\delta + \gamma\beta}{\beta\delta}$$

TEOREMA 3.25. *La operación $+$ es una operación binaria cerrada $+ : \mathbb{Q} \times \mathbb{Q} \rightarrow \mathbb{Q}$ y está bien definida. Es decir no depende de los representantes escogidos. $+$ se denomina la suma o adición de números racionales.*

DEMOSTRACIÓN. En efecto, $\frac{\alpha}{\beta} + \frac{\gamma}{\delta} := \frac{\alpha\delta + \gamma\beta}{\beta\delta} \in \mathbb{Q}$, por consiguiente $+ : \mathbb{Q} \times \mathbb{Q} \rightarrow \mathbb{Q}$.

Supongamos que $\frac{\alpha_1}{\beta_1}, \frac{\gamma_1}{\delta_1}$, son otros representantes de $\frac{\alpha}{\beta}, \frac{\gamma}{\delta}$, entonces tenemos las igualdades

$$\alpha\beta_1 = \alpha_1\beta$$

$$\gamma\delta_1 = \gamma_1\delta$$

Debemos mostrar que

$$(3.73) \quad \frac{\alpha\delta + \gamma\beta}{\beta\delta} = \frac{\alpha_1\delta_1 + \gamma_1\beta_1}{\beta_1\delta_1}$$

En efecto

$$\begin{aligned} (\alpha\delta + \gamma\beta)\beta_1\delta_1 &= \alpha\delta\beta_1\delta_1 + \gamma\beta\beta_1\delta_1 \\ &= \alpha_1\beta\delta\delta_1 + \gamma_1\delta\beta\beta_1 \\ &= (\alpha_1\delta_1 + \gamma_1\beta_1)\delta\beta \end{aligned}$$

Lo que muestra la igualdad (3.73). Por consiguiente + está bien definida. \square

En el siguiente teorema enumeraremos algunas de las propiedades principales de la suma de racionales.

TEOREMA 3.26. $+ : \mathbb{Q} \times \mathbb{Q} \rightarrow \mathbb{Q}$ posee las siguientes propiedades:

1. $+$ es asociativa, es decir $\forall x, y, z \in \mathbb{Q}$ vale

$$(3.74) \quad x + (y + z) = (x + y) + z$$

2. $+$ es conmutativa, es decir $\forall x, y \in \mathbb{Q}$ vale

$$(3.75) \quad x + y = y + x$$

3. $\frac{0}{1}$ es elemento neutro de $+$, y lo identificaremos con 0.

4. $-\frac{\alpha}{\beta} := \frac{-\alpha}{\beta} = \frac{\alpha}{-\beta}$ es simétrico o inverso aditivo de $\frac{\alpha}{\beta}$

La demostración del teorema 3.26 la dejamos al lector como ejercicio.

Dados dos racionales $\frac{\alpha}{\beta}, \frac{\gamma}{\delta}$, definimos $\frac{\alpha}{\beta} - \frac{\gamma}{\delta} := \frac{\alpha}{\beta} + \left(-\frac{\gamma}{\delta}\right)$

Como una consecuencia inmediata del teorema 3.26, se obtiene el siguiente

COROLARIO 3.27. $(\mathbb{Q}, +)$ forma un grupo abeliano.

3.3.1.3. Producto de Números Racionales. Dados dos números racionales $\frac{\alpha}{\beta}, \frac{\gamma}{\delta}$ se define:

$$(3.76) \quad \frac{\alpha}{\beta} \cdot \frac{\gamma}{\delta} := \frac{\alpha\gamma}{\beta\delta}$$

TEOREMA 3.28. La operación \cdot es una operación binaria cerrada $\cdot : \mathbb{Q} \times \mathbb{Q} \rightarrow \mathbb{Q}$ y está bien definida. Es decir que no depende del representante escogido.

DEMOSTRACIÓN. En efecto $\frac{\alpha}{\beta} \cdot \frac{\gamma}{\delta} := \frac{\alpha\gamma}{\beta\delta} \in \mathbb{Q}$.

Supongamos que $\frac{\alpha_1}{\beta_1}, \frac{\gamma_1}{\delta_1}$, son otros representantes de $\frac{\alpha}{\beta}, \frac{\gamma}{\delta}$, entonces tenemos las igualdades

$$\alpha\beta_1 = \alpha_1\beta$$

$$\gamma\delta_1 = \gamma_1\delta$$

Debemos mostrar que

$$(3.77) \quad \alpha\gamma\delta_1\beta_1 = \alpha_1\gamma_1\delta\beta$$

En efecto

$$(3.78) \quad \alpha\gamma\delta_1\beta_1 = \alpha\beta_1\gamma\delta_1 = \alpha_1\beta\gamma_1\delta = \alpha_1\gamma_1\delta\beta$$

Por consiguiente $\frac{\alpha\gamma}{\delta\beta} = \frac{\alpha_1\gamma_1}{\delta_1\beta_1}$

□

TEOREMA 3.29. $\cdot : \mathbb{Q} \times \mathbb{Q} \rightarrow \mathbb{Q}$ posee las siguientes propiedades:

1. \cdot es asociativa, es decir

$$(3.79) \quad x \cdot (y \cdot z) = (x \cdot y) \cdot z, \forall x, y, z \in \mathbb{Q}$$

2. \cdot es conmutativa, es decir

$$(3.80) \quad x \cdot y = y \cdot x, \forall x, y \in \mathbb{Q}$$

3. La clase $\frac{1}{1}$ es elemento neutro de \cdot en \mathbb{Q} y lo identificaremos con 1.

4. Si $\frac{\alpha}{\beta} \neq 0$, entonces la clase $\frac{\beta}{\alpha}$ es inverso o simétrico de $\frac{\alpha}{\beta}$.

5. \cdot es distributiva respecto de $+$, es decir

$$(3.81) \quad (x + y) \cdot z = x \cdot z + y \cdot z, \quad y - x \cdot (y + z) = x \cdot y + x \cdot z, \forall x, y, z \in \mathbb{Q}$$

La demostración de este teorema le queda al lector como ejercicio.

De forma inmediata se obtiene el siguiente

COROLARIO 3.30.

1. $(\mathbb{Q} \setminus \{0\}, \cdot)$ es un grupo abeliano.

2. $(\mathbb{Q}, +, \cdot)$ es un campo, llamado el campo de los números racionales.

3.3.2. Ejercicios y Complementos.

1. Mostrar los teoremas 3.26 y 3.29.

2. Mostrar que $\frac{\alpha}{\beta}$ está en la clase de $\frac{0}{1}$ Ssi $\alpha = 0$.

3. Dar representación canónica de las siguientes fracciones:

a) $\frac{25}{40}$.

b) $\frac{34}{-50}$.

c) $\frac{-125}{-340}$.

4. Mostrar que si $\frac{\alpha}{\beta} \cdot \frac{\gamma}{\delta} = 0$, entonces $\frac{\alpha}{\beta} = 0$ o $\frac{\gamma}{\delta} = 0$.

5. Mostrar que la representación canónica de un número racional es única.

6. La siguiente definición asume que la fracción está expresada con denominador positivo. Diremos que $\frac{\alpha}{\beta} \leq \frac{\gamma}{\delta}$ Ssi $\alpha\delta \leq \gamma\beta$. Mostrar que \leq es una relación de orden sobre \mathbb{Q} . Si, $\frac{\alpha}{\beta} \leq \frac{\gamma}{\delta}$, entonces diremos que $\frac{\alpha}{\beta}$ es menor o igual que $\frac{\gamma}{\delta}$.

Diremos que $\frac{\alpha}{\beta} > \frac{\gamma}{\delta}$ Ssi $\frac{\gamma}{\delta} < \frac{\alpha}{\beta}$

7. En forma análoga al ejercicio precedente, definimos $\frac{\alpha}{\beta} < \frac{\gamma}{\delta}$ Ssi $\alpha\delta < \gamma\beta$. Mostrar que $<$ es una relación de orden estricto sobre \mathbb{Q} . Diremos que $\frac{\alpha}{\beta} > \frac{\gamma}{\delta}$ Ssi $\frac{\gamma}{\delta} < \frac{\alpha}{\beta}$.

8. Ordenar las siguientes fracciones en forma ascendente: $\frac{25}{30}, \frac{75}{125}, \frac{3}{4}, \frac{5}{8}$.

9. Dados $x := \frac{\alpha}{\beta}$, $y := \frac{\gamma}{\delta}$, tales que $x < y$, mostrar que $x < \frac{x+y}{2} < y$.
10. Deducir del ejercicio precedente que en \mathbb{Q} ningún elemento es sucesor o predecesor de otro.
11. Mostrar que $\frac{\alpha}{\beta} \leq 0$ Ssi $\alpha \leq 0$. Mostrar también que $\frac{\alpha}{\beta} \geq 0$ Ssi $\alpha \geq 0$. (No olvidar que $\beta \in \mathbb{Z}^+$).
12. Mostrar que en \mathbb{Q} se satisface la ley de tricotomía y que todo racional se encuentra en uno y sólo uno de los siguientes conjuntos:

$$\bar{0} := \{0\} \quad \mathbb{Q}^+ := \left\{ \frac{\alpha}{\beta} \in \mathbb{Q} \mid \frac{\alpha}{\beta} > 0 \right\} \quad \mathbb{Q}^- := \left\{ \frac{\alpha}{\beta} \in \mathbb{Q} \mid \frac{\alpha}{\beta} < 0 \right\}$$

13. dado $\frac{\alpha}{\beta} \in \mathbb{Q}$, definimos

$$\left| \frac{\alpha}{\beta} \right| := \begin{cases} \frac{\alpha}{\beta} & \text{si } \frac{\alpha}{\beta} \geq 0 \\ -\frac{\alpha}{\beta} & \text{si } \frac{\alpha}{\beta} < 0. \end{cases}$$

Mostrar que $\left| \cdot \right|$ es una función $\left| \cdot \right| : \mathbb{Q} \rightarrow \mathbb{Q}^+ \cup \{0\}$

14. Mostrar que $\left| \cdot \right|$ cumple con (3.43), (3.44), (3.45), (3.46), del teorema 3.17, así como la desigualdad (3.69) de la serie de ejercicios 3.2.4.

CAPÍTULO 4

INTRODUCCIÓN A LA TEORÍA DE GRUPOS

4.1. Reseña Histórica

La teoría de grupos ha alcanzado un gran desarrollo y aplicación en diferentes ramas de las matemáticas, como en la topología, topología algebraica, geometría, geometría diferencial y algebraica, así como en la física moderna, la química y la cristalografía. También en la teoría musical se han encontrado aplicaciones de la teoría de grupos.

Ya en su artículo *Réflexions sur la résolution algébrique des équations*, publicado en 1770, Joseph Lagrange, (figura 4.1), estudia las propiedades de las *permutaciones*, en particular de las permutaciones entre las raíces de un polinomio, introduciendo, por primera vez, símbolos para dichas raíces y estudiándolas en abstracto. Sin embargo no es hasta 1899 que el matemático italiano Paolo Ruffini, (figura 4.2) desarrolla la teoría de grupos de permutaciones. Sin embargo es el matemático francés Évariste Galois¹, quien en 1832 descubre la propiedad de cerradura en los grupos de permutaciones.

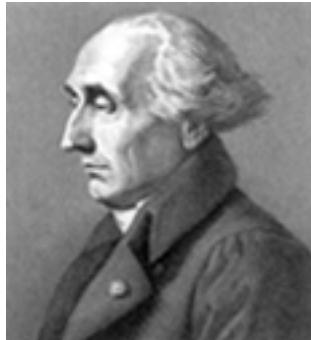


FIGURA 4.1. Joseph Lagrange

Los matemáticos franceses Augustin Cauchy y Camille Jordan, (figura 4.3), continuaron con el desarrollo de los grupos de permutaciones. Entre otras cosas, Jordan da una definición de la noción de *isomorfismo*, siempre en el marco de las permutaciones y a él se debe la amplia difusión del término *grupo*.

Sin embargo, la noción abstracta de grupo aparece, por primera vez, en los trabajos de Arthur Cayley, en 1854. Cayley descubre que no solamente existen grupos de permutaciones, sino que también las matrices invertibles, con el producto usual de matrices, constituyen un grupo y muestra, sin embargo, que todo grupo es isomorfo a un subgrupo de

¹Galois murió a los 21 años a consecuencia de un duelo, sus trabajos no fueron publicados hasta 1846, después de su muerte.



FIGURA 4.2. Paolo Ruffini

permutaciones. Sin embargo la definición de grupo, como se conoce actualmente, es debida al matemático Walther von Dyck (1882). Si bien el matemático noruego Niels Henrik Abel, logró demostrar que la ecuación general polinómica de grado 5 no es soluble por medio de un proceso de radicación, es Évariste Galois, quien aplicando la teoría de grupos, asocia un grupo a la ecuación, llamado actualmente el *grupo de Galois* y logra demostrar que la ecuación general de grado $n \geq 5$ no es soluble por radicación y relaciona la solubilidad, por radicación, de una determinada ecuación, con la solubilidad de su grupo de Galois correspondiente.

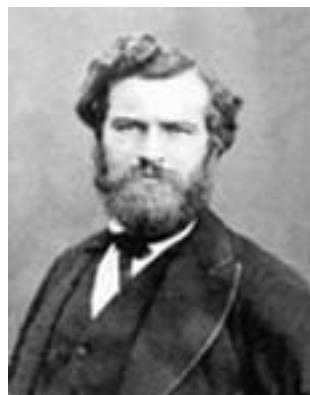


FIGURA 4.3. Camille Jordan

Posteriormente el matemático alemán Felix Klein, en su *Erlangen Programm* (1872), da una serie de aplicaciones de la teoría de grupos a la geometría, introduciendo los grupos de simetría de figuras geométricas. En el ámbito de la geometría diferencial Sophus Lie introduce grupos en los cuales la operación binaria es diferenciable, así como la aplicación que a cada elemento le asigna su inversa, llamados *grupos de Lie*.

En la teoría de números existen ya con Friedrich Gauss los primeros pasos que llevarán más adelante la aplicación de la teoría de grupos. Gauss descubre la propiedad de asociatividad en el estudio de la estructura multiplicativa de los grupos residuales módulo n , en parte ya estudiados por Leonhard Euler. En particular, en esta área son importantes los trabajos de los matemáticos alemanes Leopold Kronecker y Ernst Kummer.



FIGURA 4.4. Felix Klein

En lo que concierne la clasificación de grupos finitos juega un papel muy importante el matemático noruego Ludwig Mejell Sylow.

El objetivo principal de la teoría de grupos, es lograr una clasificación de los mismos en clases de isomorfía, en particular de grupos bien conocidos, que servirán de modelo. Desde el punto de vista de la teoría de grupos, dos grupos isomorfos poseen exactamente las mismas propiedades algebraicas, sin importar cuáles son sus elementos específicos.

4.2. Definición y Propiedades Generales

Como vimos en el capítulo precedente un grupo es una estructura algebraica (G, \cdot) , que satisface las condiciones siguientes:

1. \cdot es una operación binaria interna, cerrada y asociativa.
2. G posee un *elemento neutro* e respecto de \cdot .
3. $\forall x \in G, \exists x^{-1} \in G$, tal que $x \cdot x^{-1} = e = x^{-1} \cdot x$. x^{-1} se llama *el inverso* o *simétrico* de x respecto de \cdot .

Si además la operación es conmutativa, entonces se dice que (G, \cdot) es un *grupo abeliano*.



FIGURA 4.5. Niels Abel

OBSERVACIÓN. Por abuso de lenguaje y de notación y con el fin de facilitar la escritura, denotaremos, en adelante, por G al grupo (G, \cdot) . Por \cdot denotaremos, salvo casos particulares, la operación binaria de cualquier grupo. Igualmente escribiremos xy en lugar de $x \cdot y$. En el caso de los grupos abelianos denotaremos la operación por $+$, salvo casos particulares, su elemento neutro por 0 , y el simétrico de un elemento x por $-x$

EJEMPLOS 4.1.

1. Sea $S := \{1, 2, \dots, n\}$, $G := \{\psi : S \rightarrow S \mid \psi \text{ es una biyección}\}$. (G, \circ) , donde \circ es la composición de aplicaciones, es un grupo. En efecto \circ es cerrada sobre G , ya que si ϕ y ψ son biyecciones, también $\phi \circ \psi$ es una biyección. Si 1_S es la biyección identidad, definida por $1_S(x) := x, \forall x \in S$, entonces $\psi \circ 1_S = 1_S \circ \psi = \psi, \forall \psi \in G$, por lo que 1_S es el elemento neutro de G . Si $\psi \in G$, entonces la aplicación inversa ψ^{-1} es también biyección sobre S , por lo que $\psi^{-1} \in G$ y $\psi \circ \psi^{-1} = \psi^{-1} \circ \psi = 1_S$, por consiguiente cada elemento de G posee un inverso en G respecto de \circ . \circ es asociativa: en efecto dadas cualesquiera $\psi, \phi, \beta \in G$, $(\psi \circ (\phi \circ \beta))(x) = \psi((\phi \circ \beta)(x)) = \psi(\phi(\beta(x))) = ((\psi \circ \phi) \circ \beta)(x), \forall x \in S$ por consiguiente $\psi \circ (\phi \circ \beta) = (\psi \circ \phi) \circ \beta, \forall \psi, \phi, \beta \in G$. Como el lector comprobará fácilmente, en general $\psi \circ \phi \neq \phi \circ \psi$, por lo que \circ no es commutativa.
2. Sea G el conjunto de las matrices 2×2 de la forma $A := \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}$, donde $a \in \mathbb{R}, a \neq 0$. Entonces con el producto usual de matrices \cdot , (G, \cdot) es un grupo abeliano. En efecto, del álgebra lineal sabemos que el producto de matrices es asociativo, la matriz identidad $I := \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in G$ es el elemento neutro y dada $A := \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} \in G$, $A^{-1} := \begin{pmatrix} a^{-1} & 0 \\ 0 & a \end{pmatrix} \in G$ es su inversa. El lector comprobará fácilmente que (G, \cdot) es abeliano.
3. En general, si G es el conjunto de todas las matrices diagonales $n \times n$ reales (complejas), de la forma

$$D := \begin{pmatrix} a_1 & 0 & \dots & 0 \\ 0 & a_2 & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & a_n \end{pmatrix}$$

tales que $a_1 \cdot a_2 \cdot \dots \cdot a_n \neq 0$, entonces (G, \cdot) , donde \cdot es el producto usual de matrices, es un grupo abeliano, cuyo elemento neutro es la matriz identidad

$$I := \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \end{pmatrix}$$

y para cada matriz D de la forma arriba indicada

$$D^{-1} := \begin{pmatrix} a_1^{-1} & 0 & \dots & 0 \\ 0 & a_2^{-1} & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & a_n^{-1} \end{pmatrix}$$

es la matriz inversa.

TEOREMA 4.1. *En todo grupo G el elemento neutro es único y cada elemento $x \in G$ posee un único inverso. Por otra parte la ecuación:*

$$(4.1) \quad ax = b$$

posee una solución única en G .

DEMOSTRACIÓN. En efecto, supongamos que $e, e' \in G$ sean elementos neutros, entonces $e = ee' = e'$.

Por otra parte si $x^{-1}, \bar{x}^{-1} \in G$ son elementos inversos de x , entonces $x^{-1} = ex^{-1} = (\bar{x}^{-1}x)x^{-1} = \bar{x}^{-1}(xx^{-1}) = \bar{x}^{-1}e = \bar{x}^{-1}$.

Si $x \in G$, satisface la ecuación (4.1) para dos elementos fijos $a, b \in G$, entonces, multiplicando, por la izquierda, ambos miembros de la ecuación por a^{-1} obtenemos $a^{-1}(ax) = (a^{-1}a)x = ex = x = a^{-1}b$, y por la unicidad de a^{-1} , x es único. \square

4.2.1. Ejercicios y Complementos.

1. Mostrar que la ecuación:

$$(4.2) \quad xa = b$$

también posee solución única en un grupo G .

2. Mostrar que si G es un grupo, $\forall g \in G$, $(g^{-1})^{-1} = g$ y $\forall g, h \in G$, $(gh)^{-1} = h^{-1}g^{-1}$.
3. Mostrar que en un grupo G , si $gh = gk$ o $hg = kg$, entonces $h = k$ (ley de cancelación).
4. Dado un grupo G , y $g \in G$, definimos la siguiente notación: $a^0 := e$, $a^1 := a$, $a^2 := aa$, $a^3 = aa^2, \dots, a^k := aa^{k-1}$ y $a^{-2} := (a^{-1})^2, \dots, a^{-k} := (a^{-1})^k$. En el caso, de un grupo abeliano, donde, por conveniencia, hemos decidido denotar por la adición + la operación binaria, se interpretará $a^k := ka := \underbrace{a + a + \dots + a}_k$, $a^0 := 0a := 0$ y $a^{-k} := \underbrace{(-a) + (-a) + \dots + (-a)}_k$. Mostrar que, para cualesquier $m, n \in \mathbb{Z}$ valen las igualdades:

$$(4.3) \quad a^m a^n = a^{m+n}$$

$$(4.4) \quad (a^m)^n = a^{mn}$$

5. Sea S un conjunto no vacío y $\mathcal{A}(S) := \{\sigma \mid \sigma : S \rightarrow S, \text{ es una aplicación biyectiva}\}$. Mostrar que $(\mathcal{A}(S), \circ)$, donde \circ es la composición de aplicaciones, es un grupo. En particular, si S es un conjunto finito de $n \geq 1$ elementos, los elementos de $\mathcal{A}(S)$ se llaman *permutaciones*. Denotaremos, en este caso, por \mathfrak{S}_n al *grupo de permutaciones* de un conjunto de n elementos.
6. Sea G un grupo y $g \in G$ un elemento, tal que $ag = a$, es decir un inverso por la derecha de a , mostrar que entonces $g = a^{-1}$. Igualmente mostrar que si $ha = a$, inverso por la izquierda, entonces $h = a^{-1}$.
7. Mostrar que si en un grupo G , existe un elemento $g \in G$, tal que $\forall a \in G$, $ag = a$ o $ga = a$, entonces $g = e$.
8. Sea (G, \cdot) un grupo. Decimos que $H \subseteq G$ es un *subgrupo* de G si (H, \cdot) es un grupo. Si la contención es propia, diremos que H es un *subgrupo propio* de G . Mostrar que $H := \{-1, 1\}$ es un subgrupo propio del grupo multiplicativo, (con el producto usual de números complejos), $G := \{1, -1, i, -i\}$.

9. Si H es un subgrupo del grupo G , mostrar que si $y \in H$, entonces $xy \in H \Rightarrow x \in H$.
10. Mostrar que $H \subseteq G$ es un subgrupo Ssi H es cerrado respecto de \cdot y $x^{-1} \in H, \forall x \in H$.
11. Mostrar que si H, K son subgrupos de G , entonces $K \cap H$ es un subgrupo de G .
12. Sea $O(n) := \{A \in GL(n) \mid A^{-1} = A^t\}$, donde $GL(n)$ es el grupo lineal de las matrices invertibles reales $n \times n$ introducido en el ejemplo 2.3, 6). Mostrar que $(O(n), \cdot)$, donde \cdot es el producto usual de matrices, es un subgrupo de $GL(n)$, llamado el grupo de *matrices ortogonales reales*. Mostrar, además, que $SO(n) := \{A \in O(n) \mid \det A = 1\}$ es un subgrupo de $O(n)$, llamado el *grupo especial de matrices ortogonales*.
13. Sea $SL(n) := \{A \in GL(n) \mid \det A = 1\}$. Mostrar que $SL(n)$ es un subgrupo de $GL(n)$, llamado el *subgrupo lineal especial*.
14. Sea $BL(n) := \{A \in GL(n) \mid a_{ij} = 0, \text{ si } i > j\}$. Mostrar que $BL(n)$ es un subgrupo de $GL(n)$, llamado el *subgrupo de Borel* de $GL(n)$.
15. Sea $SB(n) := \{A \in BL(n) \mid \det A = 1\}$. Mostrar que $SB(n)$ es un subgrupo de $BL(n)$ llamado el *subgrupo de Borel especial*.
16. Sean G, K subgrupos de G . Mostrar que $H \cap K$ es un subgrupo de G . Dar un ejemplo en el que se muestre que, en general, $H \cup K$ no es un subgrupo.
17. Sea \mathcal{H} una familia de subgrupos de G . Mostrar que entonces

$$\bigcap_{H \in \mathcal{H}} H$$

es un subgrupo de G .

4.2.2. Conjunto de Generadores y Grupos Cíclicos. Dados un grupo G y un subconjunto $S \subseteq G$, decimos que S es un *conjunto de generadores* de G , o que S genera al grupo G , si todo elemento de G es producto de elementos de S y sus inversos. En tal caso escribiremos $G = \langle S \rangle$. Si G es generado por un único elemento $g \in G$, entonces diremos que G es un *grupo cíclico*, en tal caso escribiremos $G = \langle g \rangle$. Si S es un conjunto finito y $G = \langle S \rangle$, entonces diremos que G es un *grupo finitamente generado*.

EJEMPLOS 4.2.

1. El grupo $(\mathbb{Z}, +)$ es un grupo cíclico, generado por $1 \in \mathbb{Z}$.
2. El grupo $(\mathbb{Z}^2, +)$ es un grupo generado por dos elementos $\{(1, 0), (0, 1)\}$
3. Los grupos $(\mathbb{Q}, +)$ y $(\mathbb{R}, +)$ no poseen un número finito de generadores.

Llamaremos *orden* de un grupo G , denotado $\circ(G)$, al número de elementos del conjunto G . Si G es un conjunto infinito, entonces diremos que su orden es infinito.

TEOREMA 4.2. *Si G es un grupo finito de orden n y $g \in G$, entonces existe un entero positivo $m \leq n$, tal que $g^m = e$*

DEMOSTRACIÓN. En efecto, consideremos la sucesión de elementos g, g^2, \dots, g^n , si todos los elementos son diferentes entonces $G = \{g, g^2, \dots, g^n\}$ y debe de existir un entero positivo $m \leq n$, tal que $g^m = e$. Si no todos los elementos de la sucesión son distintos, entonces existen enteros $r < s \leq n$, tales que $g^r = g^s$, entonces, si $m := s - r$ se obtiene $g^m = e$. \square

Llamaremos *orden de un elemento* $g \in G$, denotado $\circ(g)$, al menor entero positivo, m , tal que $g^m = e$.

EJEMPLOS 4.3.

1. Los grupos $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ son grupos de orden infinito.
2. El grupo multiplicativo $G := \{1, -1, i, -i\}$ es un grupo de orden 4. los elementos $i, -i$ son respectivamente de orden 4, mientras que $1, -1$ son de orden 1 y 2 respectivamente. G es cíclico, ya que $G = \langle i \rangle$.

TEOREMA 4.3. *Sea G un grupo de orden finito. Entonces $H \subseteq G$ es un subgrupo Ssi H es cerrado respecto de la operación.*

DEMOSTRACIÓN. Debemos mostrar que si $g \in H$, también $g^{-1} \in H$. En efecto, sea $g \in H$, $g \neq e$. Como H es cerrado $g^n \in H$, $\forall n \in \mathbb{Z}^+$. Como G es de orden finito, existe $m \in \mathbb{Z}^+$, tal que $\circ(g) = m$. Entonces $g^m = e$ y $g^{-1} = g^{m-1} \in H$. Por consiguiente H es subgrupo de G . \square

TEOREMA 4.4. *Sea G un grupo, $g \in G$ y $m \in \mathbb{Z}^+$, tal que $g^m = e$, entonces $\circ(g) \mid m$. Por otra parte si $\circ(g) \mid m$, entonces $g^m = e$.*

DEMOSTRACIÓN. En efecto, por el algoritmo euclídeo, existen $q, r \in \mathbb{Z}$, tales que $m = \circ(g)q + r$, $r \leq 0 < \circ(g)$. Entonces, si $r \neq 0$, $e = g^m = g^{\circ(g)q+r} = g^r$, donde $r < \circ(g)$, lo cual es una contradicción a la definición de $\circ(g)$. Por consiguiente $r = 0$ y $\circ(g) \mid m$. Si $\circ(g) \mid m$, es claro que $g^m = e$. \square

4.2.3. Relación de Congruencia y Clases Laterales.

DEFINICIÓN 4.1. Sea G un grupo, H un subgrupo de G . Dados $a, b \in G$, decimos que a es congruente con b módulo H , denotado $a \equiv b \pmod{H}$, si $ab^{-1} \in H$.

TEOREMA 4.5. *La relación $a \equiv b \pmod{H}$ es una relación de equivalencia sobre G .*

DEMOSTRACIÓN.

1. \equiv es reflexiva. En efecto, $a \equiv a \pmod{H}$, pues $aa^{-1} = e \in H$.
2. \equiv es simétrica. Si $a \equiv b \pmod{H}$, entonces $ab^{-1} \in H$, como H es subgrupo, $ba^{-1} = (ab^{-1})^{-1} \in H$, por consiguiente $b \equiv a \pmod{H}$.
3. \equiv es transitiva. En efecto, $a \equiv b \pmod{H}$ y $b \equiv c \pmod{H}$ implican $ab^{-1} \in H$ y $bc^{-1} \in H$, entonces $ac^{-1} = (ab^{-1})(bc^{-1}) \in H$, por consiguiente $a \equiv c \pmod{H}$.

\square

Dado un subgrupo H de un grupo G , y un elemento $g \in G$, definimos los conjuntos

$$gH := \{gh \mid h \in H\} \quad Hg := \{hg \mid h \in H\}$$

Llamados respectivamente *clase lateral izquierda* de H respecto de g y *clase lateral derecha* de H respecto de g

Nótese que si $ab^{-1} \in H$, entonces existe $h \in H$, tal que $ab^{-1} = h$ y $a = hb \in Hb$. Por otra parte, si $a \in Hb$, entonces existe $h \in H$, tal que $a = hb$ y $ab^{-1} = h \in H$, por lo que $a \equiv b \pmod{H}$.

Entonces tenemos el siguiente resultado:

TEOREMA 4.6.

1. $a \equiv b \pmod{H}$ Ssi $a \in Hb$.

2. El conjunto $\bar{a} := \{x \mid x \equiv a\} = \{x \mid xa^{-1} \in H\} = Ha$. Es decir la clase de equivalencia de a es precisamente Ha , la clase lateral derecha de H respecto de a .
3. $Ha \cap Hb = \emptyset$ o bien, $Hb = Ha$.
4. $G = \bigcup_{g \in G} Hg$

DEMOSTRACIÓN. Sólo nos queda por mostrar 3 y 4. En efecto, como los conjuntos Ha y Hb son las clases de equivalencia respecto de la relación \equiv , las aserciones resultan del teorema 1.4. \square

Dado un elemento $g \in G$, consideremos la aplicación $\phi : H \rightarrow Hg$, definida por $\phi(h) := hg$, $\forall h \in H$, entonces ϕ es una biyección entre H y Hg . ϕ es obviamente sobre-yectiva. ϕ es inyectiva, pues si $\phi(h) = \phi(h_1)$, entonces $hg = h_1g$ y por la ley de cancelación 4.2.1,3), $h = h_1$. Por consiguiente ϕ es una biyección. Esto quiere decir, entonces, que todas las clases laterales derechas poseen la misma cardinalidad, la del subgrupo H .

Al conjunto cociente de las clases de equivalencia \equiv (mód H) lo denotaremos por G/H . Llamaremos índice de H en G , $i_G(H)$ a la cardinalidad de G/H .

EJEMPLOS 4.4.

1. Sea $G := \{1, -1, i, -i\}$ con el producto usual de números complejos. H el subgrupo $H := \{1, -1\}$. Entonces $Hi = \{i, -i\}$. $G/H = \{\bar{1}, \bar{i}\}$. $\circ(H) = 2$, $i_G(H) = 2$.
2. Sea $G := \{0, 1, 2, 3, 4, 5\}$, donde $0, 1, 2, 3, 4, 5$ son símbolos formales, dotado del producto \odot , definido por la siguiente tabla:

\odot	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	0	5	4	3	2
2	2	4	0	5	1	3
3	3	5	4	0	2	1
4	4	2	3	1	5	0
5	5	3	1	2	0	4

Sea $H := \{0, 4, 5\}$, como H es cerrado respecto de \odot , H es un subgrupo y $\circ(H) = 3$. $H \odot 1 = \{1, 2, 3\}$. Entonces $G/H = \{\bar{0}, \bar{1}\}$, y $i_G(H) = 2$.

3. Consideremos el grupo $(\mathbb{Z}, +)$ y $H := 2\mathbb{Z} := \{2x \mid x \in \mathbb{Z}\}$, el subgrupo de los enteros pares. En este caso tanto el orden de \mathbb{Z} , como el de H no son finitos. $\bar{1} = H + 1 = \{1, 3, 5, \dots\}$, $\bar{0} = H + 0 = 2\mathbb{Z} = H$, y $\mathbb{Z}/2\mathbb{Z} = \{\bar{0}, \bar{1}\}$. $i_{\mathbb{Z}}(H) = 2$.

Notemos que en los dos primeros ejemplos $\circ(G) = \circ(H)i_G(H)$. Esto no es una causalidad y es un resultado que es válido para cualquier grupo de orden finito y cualquier subgrupo de éste, como le demostraremos en el siguiente teorema, debido a Lagrange. Si G no es de orden finito, el teorema continúa siendo válido, ya que en dicho caso uno de los dos factores será infinito.

TEOREMA 4.7 (Teorema de Lagrange). *Si G es un grupo de orden finito y H un subgrupo de G , entonces $\circ(G) = \circ(H)i_G(H)$. Por lo que $\circ(H) \mid \circ(G)$.*

DEMOSTRACIÓN. En efecto, como \equiv (mód H) es una relación de equivalencia, los elementos de G/H forman una partición de G y

$$G = \bigcup_{\bar{g} \in G/H} \bar{g}$$

como cada elemento de G está en una única clase \bar{g} y cada clase contiene exactamente $\circ(H)$ elementos y existen exactamente $i_G(H)$ clases distintas, se obtiene que $\circ(G) = \circ(H)i_G(H)$. \square

Del teorema 4.7 obtenemos de forma inmediata el siguiente

COROLARIO 4.8. *Si G es un grupo finito de orden $\circ(G) = n$, entonces $g^n = e$, $\forall g \in G$.*

DEMOSTRACIÓN. Tomemos $H := \langle g \rangle$, el grupo cíclico generado por g . Entonces $\circ(H) = \circ(g)$ y, por el teorema de Lagrange, $\circ(g) \mid \circ(G) = n$. Por lo tanto $g^n = e$. \square

COROLARIO 4.9. *Si G es un grupo finito de orden p , donde p es un número primo, entonces G es un grupo cíclico y cualquiera de sus elementos distintos de e generan G .*

DEMOSTRACIÓN. En efecto, sea $g \in G$, $g \neq e$, entonces $\circ(g) \neq 1$. Por corolario 4.8, $\circ(g) \mid \circ(G)$, como p es primo y $\circ(g) \neq 1$, resulta que $\circ(g) = p = \circ(G)$, por consiguiente $G = \langle g \rangle$. \square

Como una aplicación del corolario 4.8, vamos a mostrar un famoso teorema de Euler, de gran interés en la teoría algebraica de números.

TEOREMA 4.10 (Euler). *Si $n \in \mathbb{Z}^+$ y $x \in \mathbb{Z}$ es primo relativo con n , entonces*

$$(4.6) \quad x^{\phi(n)} \equiv 1, \quad (\text{mód } n)$$

DEMOSTRACIÓN. Como $(x, n) = 1$, por ejercicio 4.2.4.8), el conjunto de clases de equivalencia módulo n de todos los enteros relativamente primos con n es $\mathbb{Z}_{\phi(n)}^*$ y con el producto definido por $\bar{x} \cdot \bar{y} := \overline{(xy)}$ forma un grupo de orden $\phi(n)$, entonces, por corolario 4.8

$$(4.7) \quad \bar{x}^{\phi(n)} = \bar{1}$$

lo que implica que (4.6), vale. \square

En el caso particular, en que p es un número primo se obtiene el siguiente resultado debido a Fermat:

COROLARIO 4.11 (Fermat). *Para todo número entero x , vale*

$$(4.8) \quad x^p \equiv x \quad (\text{mód } p)$$

El resultado de Fermat, nos dice que $p \mid (x^p - x)$, $\forall x \in \mathbb{Z}$.

Sea G un grupo y H, K dos subgrupos de G , consideremos el conjunto

$$HK := \{x \in G \mid x = hk, h \in H, k \in K\}$$

Entonces, cabe preguntarse si HK es o no un subgrupo de G y en caso en que no, bajo qué circunstancias lo es. Al respecto tenemos, entonces, el siguiente

TEOREMA 4.12. *HK es un subgrupo de G , Ssi $HK = KH$.*

DEMOSTRACIÓN. Supongamos que HK es un subgrupo. Vamos a mostrar entonces que

$$(4.9) \quad HK = KH$$

Mostremos primero que

$$(4.10) \quad HK \subseteq KH$$

En efecto, sea $x \in HK$, entonces existen $h \in H$, $k \in K$, tales que $x = hk$. Como HK es un subgrupo, se tiene que $x^{-1} \in HK$, por lo que existen $h_1 \in H$, $k_1 \in K$, tales que $x^{-1} = h_1k_1$, entonces $x = (x^{-1})^{-1} = k_1^{-1}h_1^{-1} \in KH$, de donde resulta (4.10).

Mostremos ahora que

$$(4.11) \quad KH \subseteq HK$$

En efecto, si $x \in KH$, entonces existen $k \in K, h \in H$, tales que $x = kh$, entonces $x^{-1} = h^{-1}k^{-1} \in HK$, como HK es subgrupo, entonces $x = (x^{-1})^{-1} \in HK$, de donde resulta (4.11). De (4.10) y (4.11), resulta (4.9).

Si (4.9), vamos a mostrar que HK es cerrado y que $x \in HK \Rightarrow x^{-1} \in HK$. En efecto, sean $x, y \in HK$, entonces existen $h, h_1 \in H, k, k_1 \in K$, tales que $x = hk, y = h_1k_1$, entonces, por (4.9), existen $k_2 \in K, h_2 \in H$, tales que $hk_1 = h_2k_2$ y se tiene

$$\begin{aligned} xy &= (hk)(h_1k_1) \\ &= (h(kh_1))k_1 \\ &= h(h_2k_2)k_1 \\ &= (hh_2)(k_2k_1) \in HK \end{aligned}$$

Por lo que HK es cerrado.

Sea ahora $x \in HK$ y mostremos que $x^{-1} \in HK$. En efecto, como $x \in HK$, existen $h \in H, k \in K$, tales que $x = hk$, entonces $x^{-1} = k^{-1}h^{-1} \in KH = HK$. Lo que muestra que HK es un subgrupo. \square

COROLARIO 4.13. *Si G es un grupo abeliano, entonces HK , es un subgrupo, para cualesquier subgrupos H, K de G .*

LEMA 4.14. *Un elemento $x \in HK$ posee representaciones diferentes, como producto de elementos de H y K Ssi $H \cap K \neq \{e\}$.*

DEMOSTRACIÓN. En efecto, supongamos que $x = hk = h_1k_1$, donde $h_1 \neq h$ y $k_1 \neq k$, entonces $e \neq h_1^{-1}h = k_1k^{-1} \in H \cap K$.

Por otra parte si $H \cap K \neq \{e\}$, sea $h \in H \cap K, h \neq e$. Sea ahora $h_1 \in H, h_1 \neq h$. Entonces $h = h_1(h_1^{-1}h)$ y $h_1 = (h_1^{-1}h_1)h$. Entonces $h_1k = (h_1^{-1}h_1)(hk) = h_2k_1$, donde $h_2 := h_1^{-1}h_1 \neq h_1$ y $k_1 = hk \neq k$. Por consiguiente el elemento $x = h_1k$ posee dos representaciones distintas. \square

LEMA 4.15. *Si G es un grupo de orden finito y $\circ(HK)$ denota el número de elementos del conjunto HK , entonces $x \in HK$, posee $\circ(H \cap K)$ representaciones diferentes.*

DEMOSTRACIÓN. En efecto, sea $x \in HK$, $x := hk$. Entonces por cada $h_1 \in H \cap K$, tenemos una representación diferente, pues $x = hk = h(h_1h_1^{-1})k = (hh_1)(h_1^{-1}k) = h_2k_1$, donde $h \neq h_2 := hh_1$ y $k \neq k_1 := h_1^{-1}k$. \square

TEOREMA 4.16. *Si G es un grupo finito, entonces*

$$(4.12) \quad \circ(HK) = \frac{\circ(H) \circ (K)}{\circ(H \cap K)}$$

DEMOSTRACIÓN. En efecto en HK comparecen $\circ(H) \circ (K)$ productos de elementos de H con elementos de K . Por lema 4.15 cada elemento posee $\circ(H \cap K)$ representaciones diferentes. Por consiguiente vale (4.12). \square

Como un corolario al teorema 4.12 se tiene

COROLARIO 4.17. *Si H, K son subgrupos del grupo finito G y $\circ(H) > \sqrt{\circ(G)}, \circ(K) > \sqrt{\circ(G)}$, entonces $H \cap K \neq \{e\}$*

DEMOSTRACIÓN. En efecto, como $HK \subseteq G$, $\circ(HK) \leq \circ(G)$. Entonces

$$\circ(G) \geq \circ(HK) = \frac{\circ(H) \circ(K)}{\circ(H \cap K)} > \frac{\sqrt{\circ(G)}}{\circ(H \cap K)} = \frac{\circ(G)}{\circ(H \cap K)}$$

Como la desigualdad es estricta se debe tener que $\circ(H \cap K) > 1$. Por consiguiente $H \cap K \neq \{e\}$. \square

Como una aplicación del corolario 4.17 se obtiene el siguiente resultado, que es un preámbulo a los teoremas de Sylow que estudiaremos más adelante.

COROLARIO 4.18. Si G es un grupo finito de orden $\circ(G) = pq$, donde p, q son números primos y $p > q$, entonces G posee, a lo sumo, un subgrupo de orden p .

DEMOSTRACIÓN. En efecto, supongamos que H, K son subgrupos de orden p . Entonces, por corolario 4.17, $H \cap K \neq \{e\}$. Como $H \cap K$ es subgrupo de H , cuyo orden es un número primo y $\circ(H \cap K) \neq \{e\}$, resulta entonces que $H \cap K = H$. El mismo argumento aplicado a K nos da que $H \cap K = K$. Por consiguiente $H = K$. \square

Como consecuencia de los teoremas de Sylow veremos que, en efecto, bajo las condiciones del corolario 4.18, G posee al menos un subgrupo de orden p , lo que nos dará como resultado que G posee exactamente un único grupo de orden p .

LEMA 4.19. Todo subgrupo G del grupo de los enteros $(\mathbb{Z}, +)$, es de la forma $(m\mathbb{Z}, +)$,

$$m\mathbb{Z} := \{mx \mid x \in \mathbb{Z}\},$$

donde m es el menor entero positivo contenido en G . G es entonces un grupo cíclico generado por m .

DEMOSTRACIÓN. En efecto, sea $m \in \mathbb{Z}^+$ el menor entero positivo contenido en G , entonces $\forall x \in \mathbb{Z}$, $mx \in G$ y $m\mathbb{Z} \subseteq G$. Por otra parte si $n \in G$, $n \geq m$ y por el algoritmo euclídeo, $n = mq + r$, $q, r \in \mathbb{Z}$, $0 \leq r < m$. Si $r \neq 0$, entonces $r \in G$, donde $r < m$, en contradicción a la escogencia de m . Por lo tanto $G = m\mathbb{Z}$. \square

4.2.4. Ejercicios y Complementos.

1. Mostrar que todo grupo cíclico es abeliano.
2. Mostrar que todo grupo finito de orden primo es cíclico.
3. Mostrar que si $G := \langle g \rangle$ es un grupo cíclico infinito, entonces $H_m := \langle g^m \rangle$ es subgrupo propio de G , $\forall m \in \mathbb{Z}$.
4. Mostrar que todo subgrupo de un grupo cíclico es también cíclico.
5. Mostrar que, dados dos enteros positivos $m, n \in \mathbb{Z}$, $n\mathbb{Z} \cap m\mathbb{Z} = \mu\mathbb{Z}$, donde $\mu := \text{lcm}(m, n)$.
6. Sea $G := (\mathbb{Z}, +)$ el grupo de los números enteros con la adición usual, $n \in \mathbb{Z}^+$ y $H := n\mathbb{Z}$ el subgrupo de los múltiplos de n . Definimos $x \equiv y \pmod{n}$. Ssi: $x \equiv y \pmod{n\mathbb{Z}}$ y denotaremos $\mathbb{Z}_n := \mathbb{Z}/n\mathbb{Z}$, al conjunto de las respectivas clases de equivalencia. Mostrar que $i_{\mathbb{Z}}(\mathbb{Z}_n) = n$ y que $\mathbb{Z}_n = \{\bar{0}, \bar{1}, \dots, \bar{(n-1)}\}$. Mostrar además que la operación $\bar{x} + \bar{y} := \bar{(x+y)}$, está bien definida y es una operación binaria $+ : \mathbb{Z}_n \times \mathbb{Z}_n \rightarrow \mathbb{Z}_n$ y que $(\mathbb{Z}_n, +)$ es un grupo abeliano.
7. Bajo las mismas condiciones que en el ejercicio precedente, mostrar que $m \in \bar{l}$. Ssi $m = nq + l$.
8. Utilizar ejercicio 3.2.4.9), para mostrar que si $n \in \mathbb{Z}^+$, entonces \mathbb{Z}_n^* , coincide con el conjunto de clases de equivalencia, módulo n de todos los enteros relativamente primos con n y que con el producto definido por $\bar{x} \cdot \bar{y} := \overline{(xy)}$ forma

un grupo abeliano, de orden $\phi(n)$. En el caso particular en que p es un número primo, entonces $\mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{0\}$, es un grupo de orden $(p - 1)$.

9. Sea $g \in G$ un elemento de orden $\circ(g) = n$, mostrar que si $m \in \mathbb{Z}_n^*$, entonces $\langle g \rangle = \langle g^m \rangle$ y deducir de este resultado que si G es un grupo cíclico de orden n , entonces G puede ser generado de $\phi(n)$ formas distintas.
10. Dar \mathbb{Z}_n^* , para cada n del conjunto $\{4, 5, 8, 9, 10, 11, 12, 15, 16, 17, 18, 20, 24\}$ e indicar en cada caso $\circ(\mathbb{Z}_n^*)$. Indicar, además, en cuáles casos \mathbb{Z}_n^* es un grupo cíclico y cuáles son sus diferentes generadores. En el caso en que \mathbb{Z}_n^* no es cíclico dar el conjunto de generadores correspondiente.
11. En el ejercicio precedente verificar que \mathbb{Z}_n^* no es cíclico para $n \in \{8, 12, 16, 20, 24\}$. ¿Qué propiedades en común tienen los enteros que están en este conjunto? ¿Podríamos conjeturar que si $n = 4m$, $m > 2$, entonces \mathbb{Z}_n^* no es cíclico?
12. Mostrar que $n\mathbb{Z} \cap m\mathbb{Z} = \mu\mathbb{Z}$, donde $\mu := [n, m] := \text{lcm}(n, m)$
13. Sean G un grupo y H un subgrupo de G . Mostrar que la relación definida por $a \equiv' b \pmod{H}$ (mód H) Ssi: $a^{-1}b \in H$, es una relación de equivalencia, cuyas clases de equivalencia son las clases laterales izquierdas de H , cuya cardinalidad es también la cardinalidad de H . Mostrar, además, que si G es un grupo abeliano, entonces las clases laterales izquierdas y derechas son iguales y la relación \equiv' coincide con la relación \equiv .
14. Sea H un subgrupo de G y $g \in G$. Mostrar que gHg^{-1} es un subgrupo de G .
15. Si H es un subgrupo de G , sea

$$N := \bigcap_{g \in G} gHg^{-1}$$

Mostrar que N es un subgrupo de G y que $aNa^{-1} = N$, $\forall a \in G$.

16. Mostrar que si todo elemento de un grupo G es de orden $\circ(g) = 2$, entonces G es abeliano.
17. Mostrar que si $\circ(G)$ es primo, los únicos subgrupos posibles de G son G y el subgrupo trivial $\{e\}$.
18. Mostrar que si en un grupo G existen elementos de orden n y m respectivamente, entonces G posee un elemento cuyo orden es el lcm. de n y m .

4.2.5. Subgrupos Normales y Grupos Cociente.

DEFINICIÓN 4.2. Sea G un grupo. Decimos que un subgrupo H de G es un *subgrupo normal* o un *divisor normal* si

$$(4.13) \quad gHg^{-1} = H, \quad \forall g \in G$$

Decimos que un grupo G es *simple*, si no contiene subgrupos normales propios no triviales. De (4.13) resulta inmediato que si H es un subgrupo normal, entonces

$$(4.14) \quad gH = Hg \quad \forall g \in G$$

y que entonces las relaciones \equiv y \equiv' coinciden.

Del teorema 4.12 obtenemos el siguiente corolario, cuya demostración la dejamos al lector.

COROLARIO 4.20. Si H, N son subgrupos de G , y N normal en G , entonces HK es un subgrupo de G .

TEOREMA 4.21. Si H es un subgrupo normal del grupo G , entonces la operación \cdot , definida por $\bar{x} \cdot \bar{y} := \overline{(xy)}$, $\forall \bar{x}, \bar{y} \in G/H$ está bien definida y es una operación binaria $\cdot : G/H \times G/H \rightarrow G/H$ y $(G/H, \cdot)$ es un grupo llamado el **grupo cociente** de G por H .

DEMOSTRACIÓN. Tenemos que mostrar que si $w, z \in G$ son otros representantes de \bar{x}, \bar{y} respectivamente, entonces

$$(4.15) \quad \bar{x} \cdot \bar{y} = \overline{xy} = H(xy) = H(wz) = \overline{wz} = \bar{w} \cdot \bar{z}$$

Como $x \equiv w \pmod{H}$, $y \equiv z \pmod{H}$ $\exists h_1, h_2 \in H$, tales que $x = h_1 w$ y $y = h_2 z$, entonces

$$(4.16) \quad \bar{x} \cdot \bar{y} = H(xy) = H((h_1 w)(h_2 z)) = H(h_1(w h_2)(z))$$

Como H es normal, vale la igualdad (4.14), $\forall g \in G$ y existe $h_3 \in H$, tal que $wh_2 = h_3 w$, entonces

$$(4.17) \quad H(h_1(w h_2)(z)) = H(h_1(h_3 w)(z)) = H(h_1 h_3)(wz) = H(wz) = \bar{w} \cdot \bar{z}$$

Entonces de (4.16) y (4.17), resulta que $\bar{x} \cdot \bar{y} = \bar{w} \cdot \bar{z}$. Por consiguiente \cdot está bien definida sobre G/H y obviamente es una operación binaria cerrada $\cdot : G/H \times G/H \rightarrow G/H$.

Vamos a mostrar ahora que $(G/H, \cdot)$ es un grupo.

1. \cdot es asociativa. En efecto

$$\bar{x} \cdot (\bar{y} \cdot \bar{z}) = \overline{x(yz)} = \overline{(xy)z} = \overline{(xy)} \cdot \bar{z} = (\bar{x} \cdot \bar{y}) \cdot \bar{z}, \forall \bar{x}, \bar{y}, \bar{z} \in G/H.$$

2. $\bar{e} := He = H$ es elemento neutro de \cdot . En efecto $\bar{e} \cdot \bar{x} = \overline{e\bar{x}} = \bar{x} = \overline{\bar{x}e} = \bar{x} \cdot e$.

3. $\overline{x^{-1}}$ es elemento simétrico de \bar{x} . En efecto, $\bar{x} \cdot \overline{x^{-1}} = \overline{xx^{-1}} = \bar{e} = \overline{x^{-1}x} = \overline{x^{-1}} \cdot \bar{x}$.

Por consiguiente $(G/H, \cdot)$ es un grupo. \square

Del teorema de Lagrange 4.7 se obtiene el siguiente corolario

COROLARIO 4.22. Si G es un grupo finito y H un subgrupo normal de G , entonces $\circ(G/H) = i_G(H) = \frac{\circ(G)}{\circ(H)}$

4.2.6. Centro de un Grupo, Centralizador, Normalizador, Subgrupo de Comunicadores.

DEFINICIÓN 4.3. Sea G un grupo. Al conjunto

$$(4.18) \quad Z(G) := \{x \in G \mid xg = gx, \forall g \in G\} = \{x \in G \mid x = gxg^{-1}, \forall g \in G\}$$

lo llamamos el *centro* de G .

TEOREMA 4.23. El centro de un grupo $Z(G)$ es un subgrupo de G .

DEMOSTRACIÓN. $Z(G)$ es cerrado. En efecto, sean $x, y \in Z(G)$, vamos a mostrar que $xy \in Z(G)$. Como $xy \in Z(G)$, entonces $\forall g \in G$, vale $xg = gx$ y $yg = gy$. Entonces

$$\begin{aligned} (xy)g &= x(yg) \\ &= x(gy) \\ &= (xg)y \\ &= (gx)y \\ &= g(xy) \end{aligned}$$

por consiguiente $xy \in Z(G)$.

Si $x \in Z(G)$, vamos a mostrar que $x^{-1} \in G$. En efecto

$$\begin{aligned} gx^{-1} &= (xg^{-1})^{-1} \\ &= (g^{-1}x)^{-1} \\ &= x^{-1}g \end{aligned}$$

Por consiguiente $x^{-1} \in Z(G)$. Por lo tanto $Z(G)$ es un subgrupo de G . \square

En particular si $g \in G$, el centro del subgrupo cíclico $\langle g \rangle$ está dado por

$$(4.19) \quad N(g) := \{x \in G \mid xg = gx\} = \{x \in G \mid g = x^{-1}gx\}$$

y lo llamamos el *centralizador* o *normalizador* del elemento g . Por teorema 4.23, $N(g)$ es un subgrupo de G .

DEFINICIÓN 4.4. Sea G un grupo. Decimos que x, y son *elementos conjugados* si existe $g \in G$, tal que $y = g^{-1}xg$.

Se tiene el siguiente lema, cuya demostración la dejamos al lector:

LEMA 4.24. *La relación ser elementos conjugados es una relación de equivalencia sobre G .*

LEMA 4.25. *Sea G un grupo, $x, g, h \in G$, entonces $g^{-1}xg = h^{-1}xh$ Ssi $g \equiv h \pmod{N(x)}$*

DEMOSTRACIÓN. En efecto, $g^{-1}xg = h^{-1}xh$ Ssi $hg^{-1}xgh^{-1} = x$ Ssi $(gh^{-1})^{-1}x(gh^{-1}) = x$ Ssi $gh^{-1} \in N(x)$ Ssi $g \equiv h \pmod{N(x)}$. \square

Si denotamos por

$$(4.20) \quad C(x) := \{y \in G \mid y = g^{-1}xg, g \in G\}$$

la clase de equivalencia de x respecto de la relación ser elemento conjugado y por c_x la cardinalidad de $C(x)$, entonces para el caso en que G es un grupo finito se tiene el

TEOREMA 4.26. *Si G es un grupo finito de orden $\circ(G)$, entonces $c_x = i_G(N(x)) = \frac{\circ(G)}{\circ(N(x))}$ y se tiene además la ecuación*

$$(4.21) \quad \circ(G) = \sum_{C(x)} i_G(N(x)) = \sum_{C(x)} \frac{\circ(G)}{\circ(N(x))}$$

DEMOSTRACIÓN. En efecto, por lema 4.25, $C(x)$ tiene tantos elementos distintos como clases laterales distintas de $N(x)$ existan, por consiguiente $c_x = i_G(N(x))$.

Por otra parte, como

$$G = \bigcup_{x \in G} C(x)$$

vale entonces que

$$\circ(G) = \sum_{C(x)} c_x = \sum_{C(x)} i_G(N(x)) = \sum_{C(x)} \frac{\circ(G)}{\circ(N(x))}$$

\square

Como consecuencia inmediata del teorema 4.26, se obtiene el siguiente corolario, cuya demostración se deja al lector:

COROLARIO 4.27. *Sea G un grupo. Entonces $x \in Z(G)$ Ssi $N(x) = G$. En el caso en que G es un grupo finito, entonces $x \in Z(G)$ Ssi $\circ(N(x)) = \circ(G)$.*

El corolario 4.27, nos permite escribir la ecuación (4.21), de la siguiente forma:

$$(4.22) \quad \circ(G) = \circ(Z(G)) + \sum_{c_x > 1} c_x$$

La ecuación (4.22), recibe el nombre de *ecuación de clase* de G . Los resultados mostrados en el siguiente teorema y su corolario, son consecuencia inmediata del teorema 4.26 y del corolario 4.27.

TEOREMA 4.28. Si $\circ(G) = p^n$, donde p es un número primo, entonces $Z(G) \neq \{e\}$.

DEMOSTRACIÓN. Dado $x \in G$, como $\circ(N(x)) \mid \circ(G)$, resulta, entonces, que $\circ(N(x)) = p^{n_x}$. Por corolario 4.27, $x \in Z(G)$ Ssi $n_x = n$. Aplicando la ecuación (4.22) y poniendo $m := \circ(Z(G))$ obtenemos

$$(4.23) \quad p^n = \circ(G) = \sum_{C(x)} \frac{p^n}{p^{n_x}} = m + \sum_{n_x < n} \frac{p^n}{p^{n_x}}$$

como $n_x \leq x$, resulta que p divide a cada $\frac{p^n}{p^{n_x}}$ y por consiguiente a toda la sumatoria. De aquí resulta entonces que

$$p \left| \left(p^n - \sum_{n_x < n} \frac{p^n}{p^{n_x}} \right) \right. = m$$

por consiguiente $\circ(Z(G)) > 1$ y $Z(G) \neq \{e\}$. \square

Como corolario del teorema 4.28 se obtiene el siguiente resultado:

COROLARIO 4.29. Si $\circ(G) = p^2$, donde p es un número primo, entonces G es un grupo abeliano.

DEMOSTRACIÓN. Vamos a mostrar que $Z(G) = G$. En efecto, como, por teorema 4.28, $Z(G) \neq \{e\}$, entonces

$$\circ(Z(G)) = \begin{cases} p & \text{o bien} \\ p^2 & \end{cases} .$$

Si $\circ(Z(G)) = p^2$, entonces $Z(G) = G$ y estamos listos. Vamos a mostrar, entonces, que no puede valer que $\circ(Z(G)) = p$. Supongamos que $\circ(Z(G)) = p$. Entonces existe $g \in G \setminus Z(G)$ y $Z(G) \subseteq N(g)$, como $g \in N(G)$, resulta que $\circ(Z(G)) < \circ(N(g))$. Por el teorema de Lagrange, resulta que $\circ(N(g)) = p^2 = \circ(G)$, lo que implica, por corolario 4.27, $g \in Z(G)$, en contradicción a la escogencia de g . Por lo tanto $Z(G) = G$. \square

DEFINICIÓN 4.5. Si H es un subgrupo de G , al conjunto

$$(4.24) \quad N(H) := \{x \in G \mid xHx^{-1} = H\}$$

lo llamamos el *normalizador* de H .

TEOREMA 4.30. $N(H)$ es un subgrupo de G y $H \subseteq N(H)$.

DEMOSTRACIÓN. En efecto, $N(H)$ es cerrado, pues dados $x, y \in N(H)$, entonces

$$\begin{aligned} (xy)N(H)(xy)^{-1} &= (xy)H(y^{-1}x^{-1}) \\ &= x(yHy^{-1})x \\ &= xHx^{-1} \\ &= H \end{aligned}$$

Por otra parte $xHx^{-1} = H \Rightarrow H = x^{-1}Hx$, por lo que $x \in N(H) \Rightarrow x^{-1} \in N(H)$. Por lo tanto $N(H)$ es un subgrupo de G .

Obviamente $\forall h \in H, hHh^{-1} = H$, por lo que $H \subseteq N(H)$. \square

Dado un grupo G y elementos $x, y \in G$, al elemento $[x, y] := xyx^{-1}y^{-1}$ lo llamamos el *comutador* de x, y .

DEFINICIÓN 4.6. Consideremos el conjunto

$$(4.25) \quad U := \{[x, y] \mid x, y \in G\}$$

Al grupo $K(G) := \langle U \rangle$ lo llamamos el *subgrupo de conmutadores* de G ,

Es claro que si G es un grupo abeliano, entonces el grupo de conmutadores es el grupo trivial $\{e\}$.

TEOREMA 4.31. *$K(G)$ es un subgrupo normal de G .*

DEMOSTRACIÓN. Vamos a mostrar que dado $g \in G$ cualquiera y cualquier conmutador $[x, y] \in U$, entonces $g[x, y]g^{-1} \in K(G)$. En efecto

$$\begin{aligned} g[x, y]g^{-1} &= gxyx^{-1}y^{-1}g^{-1} \\ &= (gx)g^{-1}x^{-1}x(gy)x^{-1}y^{-1}g^{-1} \\ &= (gxg^{-1}x^{-1})(x(gy)x^{-1}(gy)^{-1}) \\ &= [g, x][x, gy] \in K(G) \end{aligned}$$

□

Por consiguiente $K(G)$ es un subgrupo normal de G .

4.2.7. Ejercicios y Complementos.

1. Mostrar el corolario 4.20.
2. Mostrar que si el producto de dos clases laterales derechas (izquierdas) de un subgrupo H de G es otra clase lateral derecha (izquierda), entonces H es normal.
3. Mostrar que todo subgrupo H tal que $i_G(H) = 2$, es normal.
4. Mostrar que si H es un subgrupo normal de índice primo, entonces G/H es cíclico.
5. Mostrar que se H es el único subgrupo de orden $\circ(H)$ del grupo finito G , entonces H es normal.
6. Mostrar que si $N(H)$ es el normalizador del subgrupo H de G , entonces H es un subgrupo normal de $N(H)$.
7. Mostrar que si H es un subgrupo normal de un subgrupo N de G , entonces $N \subseteq N(H)$. Es decir $N(H)$ es el subgrupo mayor en el cual H es normal. Deducir de este resultado que H es normal en G Ssi $N(H) = G$.
8. Sea H un subgrupo del grupo G . Mostrar que

$$C(H) := \{x \in G \mid xhx^{-1} = x, \forall h \in H\}$$

es un subgrupo de G , llamado el *centralizador* de H . Mostrar también, que $C(H) \subseteq N(H)$.

9. Mostrar que si N, M son subgrupos normales de G , entonces también NM es un subgrupo normal de G .
10. Mostrar que si $N \cap M = \{e\}$, donde N, M son subgrupos normales de G , entonces $nm = mn, \forall m \in M, n \in N$.
11. Si $K(G)$ es el subgrupo de conmutadores de G , mostrar que $G/K(G)$ es un grupo abeliano. Mostrar también que G/H es abeliano Ssi H es un subgrupo normal que contiene a $K(G)$.
12. Si un subgrupo cíclico H es normal en G , mostrar que todo subgrupo de H es también normal en G .
13. Mostrar que si H es normal en G , y $g \in G$ es un elemento de orden $\circ(g)$, entonces, el orden $\circ(\bar{g})$, donde \bar{g} es la clase de g en G/H , divide a $\circ(g)$.

14. Si N es un subgrupo normal del grupo finito G , tal que $i_G(N)$ es relativamente primo con $\circ(H)$, mostrar que entonces todo elemento $x \in G$, tal que $x^{\circ(N)} = e$, debe de estar en N .
15. Mostrar lema 4.24.
16. Sean N, H subgrupos de G y N normal en G . Mostrar que $N \cap H$ es normal en H .

4.3. Homomorfismos de Grupos

Dados dos grupos $(G, *)$, (\hat{G}, \odot) , recordamos que un homomorfismo de grupos es una aplicación $\varphi : G \rightarrow \hat{G}$, tal que $\varphi(x * y) = \varphi(x) \odot \varphi(y)$, $\forall x, y \in G$.

Por lo que sigue, salvo casos particulares, usaremos la notación especificada en la observación precedente.

EJEMPLOS 4.5.

1. Sea $(\mathbb{R}, +)$ el grupo de los números reales con la adición y (\mathbb{R}^+, \cdot) el grupo de los reales positivos con el producto usual \cdot . Entonces la función $\log : \mathbb{R}^+ \rightarrow \mathbb{R}$ es un homomorfismo de grupos. En efecto $\log(x \cdot y) = \log(x) + \log(y)$, $\forall x, y \in \mathbb{R}^+$.
2. Dados dos grupos $(G, *)$, (\hat{G}, \odot) , la aplicación *trivial* $e : G \rightarrow \hat{G}$, definida por $e(x) := \hat{e}$, $\forall x \in G$, es un homomorfismo de grupos, llamado el *homomorfismo trivial*.
3. Dado un grupo G y un elemento fijo $g \in G$ la aplicación $\varphi_g : G \rightarrow G$, definida por $\varphi_g(x) := gxg^{-1}$ es un homomorfismo, llamado un *homomorfismo interno*. En efecto $\varphi_g(xy) = g(xy)g^{-1} = gx(g^{-1}g)yg^{-1} = (gxg^{-1})(gyg^{-1}) = \varphi_g(x)\varphi_g(y)$. En el caso en que G es un grupo abeliano, se obtiene la aplicación identidad, la cual también es un homomorfismo, llamado el *homomorfismo identidad*.

TEOREMA 4.32. Si $\varphi : G \rightarrow \hat{G}$ es un homomorfismo de grupos, entonces:

1. Si e, \hat{e} son los elementos neutros de G y \hat{G} respectivamente, $\varphi(e) = \hat{e}$
2. Si x^{-1} es el elemento inverso de $x \in G$, $\varphi(x^{-1}) = (\varphi(x))^{-1}$, elemento inverso de $\varphi(x) \in \hat{G}$.

DEMOSTRACIÓN.

1.

$$\begin{aligned}\hat{e} &= \varphi(e)(\varphi(e))^{-1} \\ &= \varphi(ee)(\varphi(e))^{-1} \\ &= (\varphi(e)\varphi(e))(\varphi(e))^{-1} \\ &= \varphi(e)(\varphi(e)(\varphi(e))^{-1}) \\ &= \varphi(e)\hat{e} \\ &= \varphi(e)\end{aligned}$$

2. $\forall x \in G \quad \varphi(x)\varphi(x^{-1}) = \varphi(xx^{-1}) = \varphi(e) = \hat{e}$ y $\varphi(x^{-1})\varphi(x) = \varphi(x^{-1}x) = \varphi(e) = \hat{e}$.

Por consiguiente $\varphi(x^{-1}) = (\varphi(x))^{-1}$, $\forall x \in G$.

□

DEFINICIÓN 4.7. Decimos que un subgrupo H de G es un *subgrupo característico* de G , si H permanece invariante bajo cualquier automorfismo de G , es decir $\varphi[H] = H$, $\forall \varphi \in \text{Aut}(G)$. En particular un subgrupo normal es aquel que permanece invariante bajo todos los automorfismos internos.

4.3.1. Ejercicios y complementos.

1. Si $\psi : G \rightarrow \hat{G}$ es un homomorfismo de grupos, mostrar que $\psi[G] \subseteq \hat{G}$ es un subgrupo de \hat{G} .
2. Si $\varphi : G \rightarrow \bar{G}$ y $\psi : \bar{G} \rightarrow \hat{G}$ son homomorfismos de grupos, mostrar que la composición $(\psi \circ \varphi) : G \rightarrow \hat{G}$ es un homomorfismo de grupos.
3. Si $\text{Aut}(G)$ es el conjunto de automorfismos sobre el grupo G , mostrar que $(\text{Aut}(G), \circ)$ es un grupo, llamado el *grupo de automorfismos* de G , cuyo elemento neutro es el isomorfismo identidad $1_G : G \rightarrow G$, tal que $1_G(x) := x, \forall x \in G$.
4. Sea $\mathcal{I}(G) := \{\varphi : G \rightarrow G \mid \varphi \text{ homomorfismo interno}\}$. Mostrar que \mathcal{I} es un subgrupo de $\text{Aut}(G)$, llamado el *subgrupo de automorfismos internos* de $\text{Aut}(G)$.
5. Sea $\psi : G \rightarrow \bar{G}$ un homomorfismo de grupos. $g \in G$ un elemento tal que $\circ(g) < \infty$. Mostrar que $\circ(\psi(g)) \mid \circ(g)$ y que entonces $\circ(\psi(g))$ es un divisor común de $\circ(G)$ y de $\circ(\bar{G})$.
6. Mostrar que si $\psi : G \rightarrow \hat{G}$ es un isomorfismo de grupos y $g \in G$ un elemento de orden $\circ(g)$, entonces $\circ(\psi(g)) = \circ(g)$. En particular, si $\psi : G \rightarrow G$ es un automorfismo, entonces $\circ(g) = \circ(\psi(g)), \forall g \in G$.
7. Sea G un grupo cíclico de orden n , y $g \in G$ un generador. Mostrar que todo homomorfismo $\psi : G \rightarrow \hat{G}$ queda totalmente determinado por la imagen de g , y que $\psi[G]$ es un subgrupo cíclico de \hat{G} de orden $\circ(\psi(g)) \leq n$.
8. Sea G un grupo cíclico de orden n , $\text{Aut}(G)$ el grupo de automorfismos sobre G . Mostrar que existe un isomorfismo $\Psi : \mathbb{Z}_n^* \rightarrow \text{Aut}(G)$. (Ayuda: si $g \in G$ es un generador, hacer ver que cualquier homomorfismo $\varphi : G \rightarrow G$ es de la forma $\varphi(g) := g^l$ y que $\varphi \in \text{Aut}(G)$ Ssi $(n, l) = 1, 0 < l < n$).
9. Sean G, \bar{G} dos grupos finitos, tales que $1 = (\circ(G), \circ(\bar{G}))$. Mostrar que el único homomorfismo posible entre ellos es el homomorfismo trivial \mathbf{e} .
10. Si $\psi : G \rightarrow \hat{G}$ es un homomorfismo de grupos y \hat{H} un subgrupo de \hat{G} , mostrar que
$$H := \psi^{-1}[\hat{H}] := \{g \in G \mid \psi(g) \in \hat{H}\}$$
es un subgrupo de G .

11. Mostrar que si G es un grupo abeliano, entonces la aplicación $(\cdot)^{-1} : G \rightarrow G$, definida por $(\cdot)^{-1}(x) := x^{-1}, \forall x \in G$ es un isomorfismo. ¿Qué pasa si G no es abeliano?
12. Sea $\varphi : G \rightarrow \hat{G}$ un homomorfismo de grupos abelianos. Mostrar que el siguiente diagrama es comutativo

$$\begin{array}{ccc} G & \xrightarrow{\varphi} & \hat{G} \\ (\cdot)^{-1} \downarrow & \cup & \downarrow (\cdot)^{-1} \\ G & \xrightarrow{\varphi} & \hat{G} \end{array}$$

Mostrar también que basta con que uno de los dos grupos G o \hat{G} sea abeliano para que la aplicación $\varphi^{-1} := (\cdot)^{-1} \circ \varphi = \varphi \circ (\cdot)^{-1}$ sea un homomorfismo. (Atención: no confundir φ^{-1} con la inversa de φ respecto de la composición de homomorfismos).

13. Sean G, \hat{G} grupos. Definimos

$$\text{hom}(G, \hat{G}) := \{\varphi : G \rightarrow \hat{G} \mid \varphi \text{ es un homomorfismo}\}$$

Mostrar que si \hat{G} es abeliano, entonces podemos dotar a $\text{hom}(G, \hat{G})$ de la siguiente operación binaria $\cdot : \text{hom}(G, \hat{G}) \times \text{hom}(G, \hat{G}) \rightarrow \text{hom}(G, \hat{G})$, definida por

$(\varphi \cdot \psi)(x) := \varphi(x)\psi(x)$, $\forall x \in G$. Mostrar que, en efecto $\varphi \cdot \psi \in \text{hom}(G, \hat{G})$ y que $(\text{hom}(G, \hat{G}), \cdot)$ es un grupo. ¿Cuál sería el elemento neutro? Dado φ ¿Cuál sería su inversa respecto de \cdot ? Mostrar que $\text{hom}(G, \hat{G})$ es abeliano ¿Qué pasa si \hat{G} no es abeliano?

14. Mostrar que si H es un subgrupo característico de G , entonces $\forall \varphi \in \text{Aut}(G)$, $\varphi|_H \in \text{Aut}(H)$.
15. Mostrar que si N es un subgrupo normal de G , entonces todo subgrupo característico de N es subgrupo normal en G .
16. Mostrar que el centro $Z(G)$ del grupo G es un subgrupo característico de G y que cada subgrupo de $Z(G)$ es normal en G .
17. Mostrar que $K(G)$, el subgrupo de conmutadores de G , es un subgrupo característico de G . En particular $K(G)$ es invariante respecto de todos los isomorfismos internos. Usar esta propiedad para dar otra demostración de que $K(G)$ es normal en G .
18. Sea \mathcal{G} el conjunto de todos los grupos. Diremos que $G \approx H$ si existe un isomorfismo $\psi : G \rightarrow H$. Mostrar que \approx es una relación de equivalencia sobre \mathcal{G} . Si $G \approx H$, entonces diremos que G y H están en la misma *clase de isomorfía*. Desde el punto de vista de la teoría de grupos, dos grupos en la misma clase de isomorfía se consideran como iguales, ya que sus propiedades, como grupo, son idénticas.

4.3.2. Núcleo de Homomorfismos de Grupos, Propiedades, Teoremas de Factorización e Isomorfía. Recordamos que el *núcleo* o *kernel* de un homomorfismo de grupos $\psi : G \rightarrow \tilde{G}$ es el conjunto

$$(4.26) \quad \ker \psi := \{g \in G \mid \psi(g) = \bar{e}\}$$

TEOREMA 4.33. Si $\psi : G \rightarrow \tilde{G}$ es un homomorfismo de grupos, entonces $\ker \psi$ es un subgrupo normal de G .

DEMOSTRACIÓN. Debemos mostrar que $\ker \psi$ es un subgrupo y que

$$(4.27) \quad g(\ker \psi)g^{-1} = \ker \psi \quad \forall g \in G$$

En efecto, $\ker \psi$ es cerrado, ya que si $g, h \in \ker \psi$, entonces

$$\psi(gh) = \psi(g)\psi(h) = \bar{e}\bar{e} = \bar{e}$$

Por consiguiente $gh \in \ker \psi$. Por otra parte si $g \in \ker \psi$, entonces

$$\psi(g^{-1}) = (\psi(g))^{-1} = \bar{e}^{-1} = \bar{e}$$

Por consiguiente $g^{-1} \in \ker \psi$ y $\ker \psi$ es un subgrupo de G .

Mostremos ahora (4.27). Vamos a mostrar primero que

$$(4.28) \quad g(\ker \psi)g^{-1} \subseteq \ker \psi$$

En efecto, sea $gxg^{-1} \in g(\ker \psi)g^{-1}$, donde $x \in \ker \psi$. Entonces

$$\begin{aligned} \psi(gxg^{-1}) &= \psi(g)\psi(x)\psi(g^{-1}) \\ &= \psi(g)\bar{e}\psi(g^{-1}) \\ &= \psi(g)\psi(g^{-1}) \\ &= \bar{e} \end{aligned}$$

Entonces $gxg^{-1} \in \ker \psi$, $\forall x \in \ker \psi$ y por lo tanto $g(\ker \psi)g^{-1} \subseteq \ker \psi$.

Ahora bien, de (4.28) se obtiene

$$(4.29) \quad \ker \psi \subseteq g^{-1}(\ker \psi)g, \quad \forall g \in G$$

entonces si tomamos $g_1 := g^{-1}$ en (4.29), obtenemos

$$(4.30) \quad \ker \psi \subseteq g_1^{-1}(\ker \psi)g_1 = (g^{-1})^{-1}(\ker \psi)g^{-1} = g(\ker \psi)g^{-1}$$

Entonces de (4.28) y (4.30) resulta (4.27). Por consiguiente $\ker \psi$ es normal. \square

TEOREMA 4.34. *Un homomorfismo de grupos $\varphi : G \rightarrow \hat{G}$ es inyectivo Ssi $\ker \varphi = \{e\}$*

DEMOSTRACIÓN. En efecto, si φ es inyectiva, entonces, por teorema 4.32, $\varphi(e) = \hat{e}$ y $\ker \varphi = \{e\}$.

Por otra parte si $\ker \varphi = \{e\}$ y $\varphi(g) = \varphi(h)$, entonces $\varphi(gh^{-1}) = \varphi(g)(\varphi(h))^{-1} = \varphi(g)(\varphi(g))^{-1} = \hat{e}$, lo que implica que $gh^{-1} \in \ker \varphi$, es decir que $gh^{-1} = e$. Por consiguiente $g = h$ y φ es inyectiva. \square

DEFINICIÓN 4.8. Sea G un grupo y H un subgrupo normal de G . Entonces sabemos que G/H es un grupo y se tiene un homomorfismo de grupos $\pi : G \rightarrow G/H$, definido por $\pi(g) := \bar{g}$, llamado el *homomorfismo canónico o proyección canónica*.

De la definición del producto en G/H y de la aplicación π es obvio que π es un homomorfismo sobreyectivo. Como $\pi(g) = \bar{g} = \bar{e} \Leftrightarrow g \in H$, resulta, entonces, que $\ker \pi = H$.

TEOREMA 4.35 (Teorema de Factorización para Grupos). *Sea $\varphi : G \rightarrow \hat{G}$ un homomorfismo de grupos de núcleo $\ker \varphi$, entonces existe un único homomorfismo*

$$(4.31) \quad \bar{\varphi} : G / \ker \varphi \rightarrow \hat{G}$$

tal que el siguiente diagrama es comutativo

$$(4.32) \quad \begin{array}{ccc} G & \xrightarrow{\varphi} & \hat{G} \\ \pi \downarrow & \nearrow \bar{\varphi} & \\ G / \ker \varphi & & \end{array}$$

Además $\bar{\varphi}$ es inyectiva y si φ es sobreyectiva, entonces $\bar{\varphi}$ es un isomorfismo.

DEMOSTRACIÓN. En efecto, si definimos

$$(4.33) \quad \bar{\varphi}(\bar{g}) := \varphi(g)$$

vemos que $\bar{\varphi}$ hace comutativo al diagrama (4.32) y cualquier otra aplicación que haga comutar a (4.32) debe coincidir con $\bar{\varphi}$. Debemos mostrar que $\bar{\varphi}$ está bien definida, es decir, que no depende del representante escogido, y que es un homomorfismo de grupos.

De (4.31) se obtiene $\bar{\varphi}(\bar{g}\bar{h}) = \varphi(gh) = \varphi(g)\varphi(h) = \bar{\varphi}(\bar{g})\bar{\varphi}(\bar{h})$, por lo que $\bar{\varphi}$, en caso de estar bien definida, sería un homomorfismo.

$\bar{\varphi}$ está bien definida. En efecto, sea h otro representante de \bar{g} , entonces $gh^{-1} \in \ker \varphi$, entonces $\bar{\varphi}(\bar{g}\bar{h}^{-1}) = \varphi(gh^{-1})$, como $gh^{-1} \in \ker \varphi$, entonces $\hat{e} = \varphi(gh^{-1}) = \varphi(g)(\varphi(h))^{-1} = \bar{\varphi}(\bar{g})(\bar{\varphi}(\bar{h}))^{-1}$, de donde resulta que $\bar{\varphi}(\bar{g}) = \bar{\varphi}(\bar{h})$. Lo que muestra que $\bar{\varphi}$ está bien definida.

$\bar{\varphi}$ es inyectiva. En efecto, $\bar{\varphi}(\bar{g}) = \varphi(g) = \hat{e}$ Ssi $g \in \ker \varphi = \bar{e}$, Ssi $\bar{g} = \bar{e}$, entonces $\ker \bar{\varphi} = \{\bar{e}\}$ y por teorema 4.34 $\bar{\varphi}$ es inyectiva.

Si φ es sobreyectiva, entonces, por definición, $\bar{\varphi}$ es también sobreyectiva. Por consiguiente $\bar{\varphi}$ es un isomorfismo de grupos. \square

LEMA 4.36. *Sean N, H subgrupos normales de G , tales que $N \subseteq H$. Entonces existe un homomorfismo sobreyectivo $\varphi : G/N \rightarrow G/H$ y $\ker \varphi = H/N$.*

DEMOSTRACIÓN. Denotemos, para $g \in G$, \tilde{g} , la clase de equivalencia de $g \pmod{N}$ y \bar{g} , su clase de equivalencia \pmod{H} . Vamos a demostrar que la aplicación $\varphi : G/N \rightarrow G/H$ definida por $\varphi(\tilde{g}) := \bar{g}$, está bien definida y es un homomorfismo de grupos. En efecto, sea $k \in G$ otro representante de \tilde{g} , entonces $kg^{-1} \in N$ y existe $n \in N$, tal que $kg^{-1} = n$, de donde $k = ng$, entonces

$$\begin{aligned}\varphi(\tilde{k}) &= \bar{k} \\ &= Hk \\ &= H(ng) \\ &= Hg, \text{ ya que } n \in H \\ &= \bar{g} \\ &= \varphi(\tilde{g})\end{aligned}$$

lo que muestra que φ está bien definida. Por otra parte

$$\begin{aligned}\varphi(\tilde{g}\tilde{g}_1) &= \varphi(\tilde{g}\tilde{g}_1) \\ &= \bar{g}\bar{g}_1 \\ &= \bar{g}\tilde{g}_1 \\ &= \varphi(\tilde{g})\varphi(\tilde{g}_1)\end{aligned}$$

Lo que muestra que φ es un homomorfismo. Obviamente φ es sobreyectiva. Ahora bien

$$\varphi(\tilde{g}) = \bar{e} \Leftrightarrow g \in H \Leftrightarrow \tilde{g} \in H/N$$

por consiguiente $\ker \varphi = H/N$ □

TEOREMA 4.37 (Segundo Teorema de Isomorfía). *Bajo las mismas condiciones del lema 4.36 se tiene un isomorfismo $\hat{\varphi} := (G/N)/(H/N) \rightarrow G/H$.*

DEMOSTRACIÓN. En efecto, por el teorema de factorización 4.35 y lema 4.36, la aplicación $\varphi := G/N \rightarrow G/H$, induce un homomorfismo inyectivo $\hat{\varphi} : (G/N)/(H/N) \rightarrow G/H$, cuyo núcleo es H/N , tal que el diagrama

$$(4.34) \quad \begin{array}{ccc} G/N & \xrightarrow{\varphi} & G/H \\ \pi \downarrow & \nearrow \hat{\varphi} & \\ (G/N)/(H/N) & & \end{array}$$

es comutativo. Como, por lema 4.36, φ es sobreyectiva, resulta, también, por teorema 4.35, que $\hat{\varphi}$ es un isomorfismo. □

Como una aplicación del teorema 4.35, vamos a mostrar que el grupo del círculo, (\mathbb{S}^1, \cdot) , donde

$$\mathbb{S}^1 := \{z \in \mathbb{C} \mid |z| = 1\}$$

y · el producto usual de complejos, es isomorfo al grupo $(\mathbb{R}/\mathbb{Z}, +)$. En efecto, consideremos el homomorfismo $\varphi : \mathbb{R} \rightarrow \mathbb{S}^1$, definido por $\varphi(t) := e^{2\pi it}$. El lector se cerciorará que, en efecto, φ es un homomorfismo de grupos, cuyo núcleo es \mathbb{Z} , y que φ es sobreyectiva, entonces, por el teorema de factorización 4.35, φ induce un isomorfismo $\hat{\varphi} : \mathbb{R}/\mathbb{Z} \rightarrow \mathbb{S}^1$.

Otro resultado interesante, consecuencial teorema de factorización es el siguiente

COROLARIO 4.38. *Sea $\Phi : G \rightarrow \mathcal{I}(G)$ la aplicación definida por $\Phi(g) := \varphi_g$, donde φ_g es el automorfismo interno $\varphi_g(x) := gxg^{-1}$. Entonces Φ es un homomorfismo sobreyectivo de grupos, cuyo núcleo es el centro $Z(G)$ de G y Φ induce un isomorfismo $\hat{\Phi} : G/Z(G) \rightarrow \mathcal{I}(G)$*

DEMOSTRACIÓN. Basta mostrar que Φ es un homomorfismo sobreyectivo de núcleo $Z(G)$, entonces, por el teorema de factorización 4.35, se obtiene el isomorfismo $\hat{\Phi}$.

En efecto, sean $g, h \in G$, entonces $\Phi(gh)(x) = \varphi_{gh}(x) = (gh)x(gh)^{-1} = (gh)x(h^{-1}g^{-1}) = g(hxh^{-1})g^{-1} = (\varphi_g \circ \varphi_h)(x)$, $\forall x \in G$. Entonces $\Phi(gh) = \varphi_g \circ \varphi_h$ por lo que Φ es homomorfismo. Φ es obviamente sobreyectivo. Por otra parte $\Phi(g) = 1_G$ Ssi $\forall x \in G$, $\varphi_g(x) = gxg^{-1} = x$ Ssi $gx = xg$, $\forall x \in G$, Ssi $g \in Z(G)$. Por consiguiente $\ker \Phi = Z(G)$. \square

TEOREMA 4.39 (Primer teorema de Isomorfía). *Sean H, N subgrupos de G , N normal en G . Entonces existe un isomorfismo natural*

$$\hat{\psi} : H/H \cap N \rightarrow HN/N$$

DEMOSTRACIÓN. Por 4.20, es HN un subgrupo de G y por ejercicio 4.2.7, 16), $H \cap N$ y N son normales en H y HN respectivamente, por lo que los grupos $H/H \cap N$ y HN/N están bien definidos. Consideremos el diagrama comutativo

$$\begin{array}{ccc} H & \xrightarrow{i} & HN \\ & \searrow \psi & \downarrow \pi \\ & & HN \end{array}$$

donde i es la inclusión H en HN y π la proyección canónica. Entonces ψ es sobreyectiva y $\ker \psi = H \cap N$, entonces, por el teorema de factorización, ψ induce un isomorfismo

$$\hat{\psi} : H/H \cap N \rightarrow HN/N$$

que hace commutar al cuadrado

$$\begin{array}{ccc} H & \xrightarrow{i} & HN \\ \bar{\pi} \downarrow & \swarrow \psi & \downarrow \pi \\ H/H \cap N & \xrightarrow{\hat{\psi}} & HN \end{array}$$

\square

4.3.3. Ejercicios y Complementos.

1. Sea $\psi : G \rightarrow \hat{G}$ un homomorfismo de grupos. Si \hat{H} es un subgrupo normal de \hat{G} , mostrar que $H := \psi^{-1}[\hat{H}]$ es un subgrupo normal de G y $\ker \psi \subseteq H$.
2. Sea $\psi : G \rightarrow \hat{G}$ un homomorfismo de grupos. Si H es un subgrupo normal de G , mostrar que $\hat{H} := \psi[H]$ es entonces un subgrupo normal en $\psi[G]$. Si ψ es sobreyectiva, entonces \hat{H} es subgrupo normal de \hat{G} .
3. Sea $\psi : G \rightarrow \hat{G}$ un homomorfismo sobreyectivo de grupos.
 - a) Consideremos las familias de conjuntos

$$\mathcal{S}_G(\ker \psi) := \{H \subseteq G \mid H \text{ subgrupo y } \ker \psi \subseteq H\} \quad \mathcal{S}_{\hat{G}} := \{\hat{H} \subseteq \hat{G} \mid \hat{H} \text{ subgrupo}\}$$

Mostrar que ψ induce una biyección $\Psi : \mathcal{S}_{\hat{G}} \rightarrow \mathcal{S}_G(\ker \psi)$, por medio de $\Psi(\hat{H}) := \psi^{-1}[\hat{H}]$. Por lo que existe una correspondencia biunívoca entre todos los subgrupos de \hat{G} y los subgrupos de G que contienen al $\ker \psi$.

b) Si definimos

$$\mathcal{N}_G(\ker \psi) := \{H \subseteq G \mid H \text{ normal y } \ker \psi \subseteq H\} \quad \mathcal{N}_{\hat{G}} := \{\hat{H} \subseteq \hat{G} \mid \hat{H} \text{ normal}\}$$

Mostrar que la restricción de Ψ a $\mathcal{N}_{\hat{G}}$ es también una biyección

$\Psi|_{\mathcal{N}_G} : \mathcal{N}_{\hat{G}} \rightarrow \mathcal{N}_G(\ker \psi)$. Es decir que existe una correspondencia biunívoca entre los subgrupos normales de \hat{G} y los subgrupos normales de G que contienen al $\ker \psi$.

4. Mostrar que los subgrupos de G/H están en correspondencia biunívoca con los subgrupos de G que contienen a H . Igualmente mostrar que los subgrupos normales de G/H están en correspondencia biunívoca con los subgrupos normales de G que contienen a H .
5. Si $\varphi : G \rightarrow \hat{G}$ es un homomorfismo de grupos, donde \hat{G} es abeliano, mostrar que $K(G) \subseteq \ker \varphi$? ¿Qué pasa si $K(G) = G$?
6. Sea G un grupo cíclico infinito y \mathbb{Z} el grupo aditivo de los enteros. Mostrar que $\psi : \mathbb{Z} \rightarrow G$, definido por $\psi(n) := g^n$, $\forall n \in \mathbb{Z}$, donde g es un generador de G , es un isomorfismo. Por lo que todo grupo cíclico infinito es isomorfo al grupo aditivo de los enteros. Mostrar además, que si G es un grupo cíclico finito, entonces existe $n \in \mathbb{Z}$, tal que G es isomorfo a $\mathbb{Z}/n\mathbb{Z}$.
7. Mostrar que $\varphi : \mathbb{R} \rightarrow \mathbb{S}^1$, definida por $\varphi(t) := e^{2\pi it}$ es un homomorfismo sobreyectivo de grupos, cuyo núcleo es \mathbb{Z} .
8. Sea $(GL(n), \cdot)$ el grupo de las matrices invertibles reales $n \times n$.
 $\det : GL(n) \rightarrow \mathbb{R} \setminus \{0\}$, la función que a cada matriz le asocia su determinante.
Mostrar que \det es un homomorfismo sobreyectivo entre $(GL(n), \cdot)$ y el grupo multiplicativo $(\mathbb{R} \setminus \{0\}, \cdot)$, cuyo núcleo es el subgrupo $SL(n)$ de $GL(n)$, donde

$$SL(n) := \{A \in GL(n) \mid \det A = 1\}$$

Deducir de ésto que \det induce un isomorfismo entre $GL(n)/SL(n)$ y $\mathbb{R} \setminus \{0\}$.

9. Si $O(n)$ es el subgrupo de matrices ortogonales de $GL(n)$ y $SO(n)$ el subgrupo especial de matrices ortogonales cuyo determinante es 1. Mostrar que \det induce un isomorfismo de grupos entre $O(n)/SO(n)$ y el grupo multiplicativo (G, \cdot) , donde $G := \{1, -1\}$.

4.3.4. Sucesiones Exactas de Homomorfismos de Grupos.

DEFINICIÓN 4.9. Decimos que una sucesión de grupos y grupos homomorfismos

$$(4.35) \quad \cdots \xrightarrow{\varphi_n} G_n \xrightarrow{\varphi_{n-1}} G_{n-1} \xrightarrow{\varphi_{n-2}} \cdots \xrightarrow{\varphi_1} G_1 \xrightarrow{\varphi_0} G_0$$

es exacta, si

$$(4.36) \quad \forall n \in \mathbb{N}, \text{ Im } \varphi_n = \ker \varphi_{n-1}$$

En particular, decir que la sucesión

$$(4.37) \quad \{e\} \rightarrow H \xrightarrow{\varphi} G$$

es exacta, es equivalente a decir que φ es un homomorfismo inyectivo.

En forma análoga, decir que la sucesión

$$(4.38) \quad G \xrightarrow{\varphi} H \rightarrow \{e\}$$

es exacta, es equivalente a decir que φ es un homomorfismo sobreyectivo.

Particularmente interesantes son las sucesiones exactas cortas de la forma

$$(4.39) \quad \{e\} \rightarrow H \xrightarrow{\varphi} G \xrightarrow{\psi} \hat{G} \rightarrow \{e\}$$

Lo que es equivalente a decir que φ es una inyección, ψ es un homomorfismo sobreyectivo y que $H \xrightarrow{\varphi} \text{Im } \varphi = \ker \psi$, donde \approx indica que H es isomorfo, por medio de φ , a $\text{Im } \varphi$. Por abuso de lenguaje se suele identificar H con $\text{Im } \varphi$.

Dado un homomorfismo $\varphi : G \rightarrow \hat{G}$ y un grupo abeliano M , éste induce un homomorfismo $\varphi^* : \text{hom}(\hat{G}, M) \rightarrow \text{hom}(G, M)$. En efecto, sea $\alpha \in \text{hom}(\hat{G}, M)$ y consideremos el siguiente diagrama

$$(4.40) \quad \begin{array}{ccc} G & \xrightarrow{\varphi} & \hat{G} \\ & & \downarrow \alpha \\ & & M \end{array}$$

el cual puede ser completado a un diagrama comutativo

$$(4.41) \quad \begin{array}{ccc} G & \xrightarrow{\varphi} & \hat{G} \\ & \searrow \alpha \circ \varphi & \downarrow \alpha \\ & & M \end{array}$$

entonces definimos $\varphi^*(\alpha) := \alpha \circ \varphi \in \text{hom}(G, M)$.

En forma análoga, si $\varphi : G \rightarrow \hat{G}$ es un homomorfismo de grupos abelianos y M un grupo, entonces φ induce un homomorfismo $\varphi_* : \text{hom}(M, G) \rightarrow \text{hom}(M, \hat{G})$. En efecto, sea $\alpha \in \text{hom}(M, G)$ y consideremos el diagrama

$$(4.42) \quad \begin{array}{ccc} & & G \xrightarrow{\varphi} \hat{G} \\ & \uparrow \alpha & \\ M & & \end{array}$$

el cual puede ser completado a un diagrama comutativo

$$(4.43) \quad \begin{array}{ccc} & & G \xrightarrow{\varphi} \hat{G} \\ & \uparrow \alpha & \nearrow \varphi \circ \alpha \\ M & & \end{array}$$

entonces definimos $\varphi_*(\alpha) := \varphi \circ \alpha \in \text{hom}(M, \hat{G})$.

TEOREMA 4.40. *Si M es un grupo abeliano, entonces la sucesión exacta*

$$(4.44) \quad H \xrightarrow{\varphi} G \xrightarrow{\psi} \hat{G} \rightarrow \{e\}$$

induce la sucesión exacta

$$(4.45) \quad \{e\} \rightarrow \text{hom}(\hat{G}, M) \xrightarrow{\psi^*} \text{hom}(G, M) \xrightarrow{\varphi^*} \text{hom}(H, M)$$

donde e designa el homomorfismo trivial.

DEMOSTRACIÓN. Tenemos que mostrar las siguientes acercaciones:

- a) ψ^* es inyectiva
- b) $\text{Im } \psi^* \subseteq \ker \varphi^*$
- c) $\ker \varphi^* \subseteq \text{Im } \psi^*$

- a) Vamos a mostrar que $\ker \psi^* = \{\mathbf{e}\}$. En efecto, sea $\alpha \in \ker \psi^*$, entonces $\psi^*(\alpha) = \alpha \circ \psi = \mathbf{e}$ y $\forall x \in G$, $\alpha(\psi(x)) = e$, lo que implica que $\text{Im } \psi \subseteq \ker \alpha$, como ψ es sobreyectiva, $\text{Im } \psi = \hat{G} \subseteq \ker \alpha$, por consiguiente $\hat{G} = \ker \alpha$ y $\alpha = \mathbf{e}$.
- b) Sea $\beta \in \text{Im } \psi^*$, entonces existe $\alpha \in \text{hom}(\hat{G}, M)$, tal que $\psi^*(\alpha) = \alpha \circ \varphi = \beta$, y $\varphi^*(\beta) = \beta \circ \varphi = (\alpha \circ \psi) \circ \varphi$, como la sucesión (4.44) es exacta, $\text{Im } \varphi = \ker \psi$, de donde $\varphi^*(\beta)(x) = (\alpha \circ (\psi \circ \varphi))(x) = \alpha(e) = e$, $\forall x \in G$. Por consiguiente $\text{Im } \psi^* \subseteq \ker \varphi^*$.
- c) Sea $\beta \in \ker \varphi^*$. Debemos mostrar que existe $\alpha \in \text{hom}(\hat{G}, M)$, tal que $\psi^*(\alpha) = \beta$. En efecto, si $\beta \in \ker \varphi$, entonces $\varphi^*(\beta) = \mathbf{e}$ y $\forall x \in G$, $\varphi^*(\beta)(x) = \beta(\varphi(x)) = e$, lo que implica que $\varphi(x) \in \ker \beta$, $\forall x \in G$. Por consiguiente $\text{Im } \varphi \subseteq \ker \beta$.

Como, por hipótesis, la sucesión (4.44) es exacta se tiene, entonces, que $\ker \psi = \text{Im } \varphi \subseteq \ker \beta$ y que ψ es sobreyectiva. Entonces, por el teorema 4.35, ψ induce un isomorfismo $\hat{\psi} : G/\ker \psi \rightarrow \hat{G}$ el cual posee una inversa $\hat{\psi}^{-1}$. Por otra parte, como $\ker \psi \subseteq \ker \beta$, por lema 4.36, se tiene un homomorfismo $\hat{\pi} : G/\ker \psi \rightarrow G/\ker \beta$ y se obtiene el siguiente diagrama commutativo, en sus dos partes:

$$(4.46) \quad \begin{array}{ccccc} & & M & & \\ & \beta & \longleftarrow & \longrightarrow & \hat{G} \\ & \hat{\beta} \uparrow & & \downarrow \pi & \swarrow \hat{\psi}^{-1} \\ G/\ker \beta & \xleftarrow{\hat{\pi}} & G/\ker \psi & & \end{array}$$

Entonces, si definimos $\alpha := \hat{\beta} \circ \hat{\pi} \circ \hat{\psi}^{-1} \in \text{hom}(\hat{G}, M)$, por la comutatividad del diagrama (4.46), se obtiene $\beta = \psi^*(\alpha)$.

□

TEOREMA 4.41. *Sea M un grupo, entonces la sucesión exacta de grupos abelianos*

$$(4.47) \quad \{\mathbf{e}\} \rightarrow H \xrightarrow{\varphi} G \xrightarrow{\psi} \hat{G}$$

induce una sucesión exacta

$$(4.48) \quad \{\mathbf{e}\} \rightarrow \text{hom}(M, H) \xrightarrow{\varphi_*} \text{hom}(M, G) \xrightarrow{\psi_*} \text{hom}(M, \hat{G})$$

DEMOSTRACIÓN. Como en el teorema precedente, desarrollaremos la demostración mostrando las siguientes acercaciones:

- a) $\ker \varphi_* = \{\mathbf{e}\}$, o sea φ_* es inyectiva.
 - b) $\text{Im } \varphi_* \subseteq \ker \psi_*$
 - c) $\ker \psi_* \subseteq \text{Im } \varphi_*$
- a) En efecto, sea $\alpha \in \ker \varphi_*$, entonces $\varphi_*(\alpha) = \mathbf{e}$ y $\forall x \in M$, $\varphi_*(\alpha)(x) = \varphi(\alpha(x)) = e$, esto implica que $\alpha(x) \in \ker \varphi$, $\forall x \in M$. Como la sucesión (4.47) es exacta, resulta que φ es inyectiva y $\ker \varphi = \{\mathbf{e}\}$, por consiguiente $\alpha(x) = e$, $\forall x \in M$, lo que implica que $\alpha = \mathbf{e}$.
 - b) Sea $\beta \in \text{Im } \varphi_*$, entonces existe $\alpha \in \text{hom}(M, H)$, tal que $\beta = \varphi_*(\alpha)$ y $\psi_*(\beta) = \psi_*(\varphi_*(\alpha)) = (\psi \circ \varphi)(\alpha)$. Dado $x \in M$, tenemos entonces $\psi_*(\beta)(x) = (\psi \circ \varphi)(\alpha)(x) = \psi(\varphi(\alpha(x))) = e$, ya que, por la exactitud de (4.47), $\text{Im } \varphi = \ker \psi$. Por consiguiente $\beta \in \ker \psi_*$.
 - c) Sea $\beta \in \ker \psi_*$, entonces $\psi_*(\beta) = \mathbf{e} = \psi \circ \beta$ y $\forall x \in M$, $\psi(\beta(x)) = e$, esto implica que $\beta(x) \in \ker \psi = \text{Im } \varphi$. Como φ es inyectiva, existe un único $h_x \in H$, tal que $\varphi(h_x) = \beta(x)$. Si definimos $\alpha : M \rightarrow H$, por $\alpha(x) := h_x$, entonces $\alpha \in \text{hom}(M, H)$ (ver ejercicio 4.3.5,4) y $\varphi_*(\alpha) = \beta$. Por consiguiente $\beta \in \text{Im } \varphi_*$.

□

OBSERVACIÓN 4.1. Advertimos al lector que una sucesión exacta corta de grupos,

$$(4.49) \quad \{e\} \rightarrow H \xrightarrow{\varphi} G \xrightarrow{\psi} \hat{G} \rightarrow \{e\},$$

en general, no induce, en el caso en que M es un grupo abeliano, una sucesión exacta

$$(4.50) \quad \{e\} \rightarrow \text{hom}(\hat{G}, M) \xrightarrow{\psi^*} \text{hom}(G, M) \xrightarrow{\varphi^*} \text{hom}(H, M) \rightarrow \{e\}$$

ni tampoco, en el caso en que la sucesión (4.49) sea de grupos abelianos, una sucesión exacta

$$(4.51) \quad \{e\} \rightarrow \text{hom}(M, H) \xrightarrow{\varphi_*} \text{hom}(M, G) \xrightarrow{\psi_*} \text{hom}(M, \hat{G}) \rightarrow \{e\}$$

ya que no podemos garantizarnos, que dado un homomorfismo $\beta : H \rightarrow M$ éste sea imagen, bajo φ^* de un homomorfismo $\alpha : G \rightarrow M$, ni tampoco que dado un homomorfismo $\beta : M \rightarrow \hat{G}$ éste sea imagen, bajo ψ_* de un homomorfismo $\alpha : M \rightarrow G$. (Ver ejercicios 4.3.5,5) y 4.3.5,6))

4.3.5. Ejercicios y Complementos.

1. Mostrar que la sucesión

$$(4.52) \quad \{e\} \rightarrow G \xrightarrow{\varphi} H \rightarrow \{e\}$$

es exacta Ssi φ es un isomorfismo.

2. Mostrar que si la sucesión (4.39) es exacta, entonces se tiene un isomorfismo $\hat{\psi} : G/H \rightarrow \hat{G}$.
3. Mostrar que si $\psi : G \rightarrow \hat{G}$ es un homomorfismo de grupos sobrejetivo, entonces se tiene una sucesión exacta

$$(4.53) \quad \{e\} \rightarrow \ker \psi \xrightarrow{\iota} G \xrightarrow{\psi} \hat{G} \rightarrow \{e\}$$

donde ι es la inclusión de $\ker \psi$ en G

4. Mostrar que la aplicación α definida en la demostración del teorema 4.41 es, en efecto, un homomorfismo en $\text{hom}(M, H)$
5. Mostrar que si M es un grupo abeliano que posee la propiedad de que dado un homomorfismo $\beta : H \rightarrow M$ existe un homomorfismo $\alpha : G \rightarrow M$ tal que el diagrama

$$(4.54) \quad \begin{array}{ccccc} \{e\} & \longrightarrow & H & \xrightarrow{\varphi} & G \\ & & \beta \downarrow & \nearrow \alpha & \\ & & M & & \end{array}$$

es comutativo, entonces, la sucesión (4.50), inducida por la sucesión exacta (4.49), es exacta.

6. Mostrar que si M es un grupo que posee la propiedad de que dado un homomorfismo $\beta : M \rightarrow \hat{G}$, existe un homomorfismo $\alpha : M \rightarrow G$, tal que el diagrama

$$(4.55) \quad \begin{array}{ccccc} & & M & & \\ & \swarrow \alpha & \downarrow \beta & \searrow & \\ G & \xrightarrow{\psi} & \hat{G} & \longrightarrow & \{e\} \end{array}$$

es conmutativo, entonces, la sucesión (4.51), inducida por la sucesión exacta de grupos abelianos (4.49), es exacta.

CAPÍTULO 5

GRUPOS DE PERMUTACIONES Y SIMETRÍA

5.0.6. Grupos de Permutaciones. Como vimos en la serie de ejercicios y complementos 4.2.1,5), una permutación es una biyección sobre un conjunto finito y al grupo de todas las permutaciones sobre un conjunto de n elementos lo designaremos por \mathfrak{S}_n y se llama el *n-grupo de simetría*. Por facilidad usaremos, como modelo, para el conjunto de n elementos, al conjunto: $S_n := \{1, 2, \dots, n\}$, en el entendido de que los resultados no varían al tomar como muestra cualquier otro conjunto de n elementos, ya que siempre existirá una biyección entre ellos.

A raíz de los intentos de demostrar porqué, para las ecuaciones polinómicas de grado mayor o igual que 5, no era posible encontrar una fórmula por radicación, en donde era claro el papel que jugaban las permutaciones entre las posibles raíces de dichos polinomios, surgió el interés por el estudio, como entes propios, de las permutaciones y sus leyes de composición, llegando a ser el prototipo de los primeros grupos estudiados y, como veremos más adelante, en el teorema de Cayley, todo grupo finito es isomorfo a un determinado grupo de permutaciones.

Usualmente denotaremos una permutación $\sigma \in \mathfrak{S}_n$, por medio de una matriz de la forma:

$$(5.1) \quad \sigma := \begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix}$$

Así, por ejemplo, para $n = 4$, $S_4 := \{1, 2, 3, 4\}$, si $\sigma : S \rightarrow S$ es la biyección definida por: $\sigma(1) := 2, \sigma(2) := 3, \sigma(3) := 4, \sigma(4) := 1$, tenemos la matriz:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$$

Dadas dos permutaciones $\sigma, \tau \in \mathfrak{S}_n$, definiremos $\tau\sigma := \tau \circ \sigma$. Si

$$\sigma := \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \quad \tau := \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}$$

entonces

$$\tau\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix} \quad \sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}$$

Del ejemplo precedente se ve que en general el producto de permutaciones no es conmutativo, por lo que \mathfrak{S}_n , salvo para $n = 2$ no es un grupo abeliano. En el estudio de las permutaciones juegan un papel muy importante dos tipos particulares, los *ciclos* y las *transposiciones*.

Una *transposición* es una permutación que únicamente permuta dos elementos, dejando fijos el resto. Por ejemplo

$$\sigma := \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 4 & 5 \end{pmatrix}$$

Si σ es la transposición que sólo permuta i con j , $i, j \in S_n$, dejando fijos el resto de elementos de S_n , entonces escribiremos $\sigma := (i \ j)$. En este caso $\sigma^2 = e$ y $\sigma = \sigma^{-1}$.

Entonces, con esta nomenclatura, la transposición del ejemplo precedente se escribe $\sigma = (1 \ 2)$.

$(i) = (i \ i)$, denominará la permutación identidad, para cualquier $i \in S_n$.

Dada una permutación de un conjunto de n elementos

$$\sigma := \begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix}$$

tal que $\sigma(n) \neq n$, siempre podemos representar a σ como el producto de una permutación σ_n que deja fijo n con una transposición adecuada. En efecto, si suponemos que para $j \neq n$, $\sigma(j) = n$, entonces

$$\sigma_n := (\sigma(n) \ \sigma(j)) \begin{pmatrix} 1 & 2 & \dots & j & \dots & i & \dots & n \\ \sigma(1) & \sigma(2) & \dots & i & \dots & \sigma(i) & \dots & \sigma(n) \end{pmatrix}$$

es una permutación que deja fijo n y $(\sigma(n) \ \sigma(j))\sigma_n = \sigma$

TEOREMA 5.1. *El grupo de permutaciones \mathfrak{S}_n es un grupo de orden $n!$ y no commutativo para $n > 2$.*

DEMOSTRACIÓN. Haremos la prueba por inducción sobre n . En efecto si $n = 2$, entonces las únicas permutaciones posibles son la identidad y la transposición $(1 \ 2)$, por lo que $\circ(\mathfrak{S}_2 = 2 = 2!)$. Como grupo de orden primo \mathfrak{S}_2 es cíclico, por ejercicio 4.2.4.2) y por consiguiente abeliano. El lector comprobará fácilmente que a partir de $n = 3$, \mathfrak{S}_3 ya no es abeliano y que su orden es $6 = 3!$. Supongamos, entonces, por hipótesis de inducción que, dado $n > 3$ el teorema sea válido para $n - 1$ y $\circ(\mathfrak{S}_{n-1}) = (n - 1)!$. Entonces, existen $(n - 1)!$ permutaciones que dejan fijo a n . Ahora bien, por cada permutación σ_n que deja fijo n , podemos obtener n permutaciones distintas $(j \ n)\sigma_n$, $1 \leq j \leq n$. Como, por hipótesis de inducción, existen $(n - 1)!$ permutaciones que dejan fijo n , se obtienen en total $n(n - 1)! = n!$ permutaciones distintas. Por otra parte, vimos que toda permutación $\sigma \in \mathfrak{S}_n$ se puede expresar de esta forma. Por consiguiente $\circ(\mathfrak{S}_n) = n!$.

□

De la demostración del teorema precedente se obtiene el siguiente

COROLARIO 5.2. *El índice de \mathfrak{S}_{n-1} en \mathfrak{S}_n es igual a n .*

DEMOSTRACIÓN. En efecto \mathfrak{S}_n es la unión de las clases n laterales $(j \ n)\mathfrak{S}_{n-1}$. Por consiguiente $i_{\mathfrak{S}_n}(\mathfrak{S}_{n-1}) = n$. □

5.0.7. Ejercicios y Complementos.

1. Dadas las permutaciones

$$\sigma := \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 4 & 5 & 6 & 7 & 8 & 1 & 2 \end{pmatrix} \quad \tau := \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 8 & 7 & 5 & 3 & 1 & 6 & 2 & 4 \end{pmatrix}$$

dar: a) $\sigma\tau$, b) $\tau\sigma$, c) σ^2 , d) τ^3

2. Mostrar que si σ es una permutación que deja fijos i, j , entonces σ commuta con la transposición $(i \ j)$.

3. Escribir el siguiente producto de transposiciones como una matriz de la forma (5.1)

$$\sigma = (1 \ 3)(2 \ 4)(3 \ 2).$$

Como veremos más adelante, toda permutación σ puede ser expresada como un producto de transposiciones.

5.0.8. Acción de Grupo. Ciclos de una Permutación.

5.0.8.1. Acción de Grupo.

DEFINICIÓN 5.1. Una *acción* del grupo G sobre un conjunto S por la izquierda, es una operación binaria $\circ : G \times S \rightarrow S$, tal que:

- a) $e \circ s = s, \forall s \in S$
- b) $(gh) \circ s = g \circ (h \circ s), \forall g, h \in G, \forall s \in S$

En forma análoga, una acción del grupo G sobre un conjunto S por la derecha, es una operación binaria $\circ : S \times G \rightarrow S$, tal que:

- a) $s \circ e = s, \forall s \in S$
- b) $s \circ (gh) = (s \circ g) \circ h, \forall g, h \in G, \forall s \in S$.

Dada una acción de grupo \circ por la izquierda y $s \in S$, llamamos órbita de s al conjunto

$$\text{orb}(s) := \{g \circ s \mid g \in G\}$$

Si \circ es una acción de grupo por la derecha, entonces la órbita de un elemento s es el conjunto

$$\text{orb}(s) := \{s \circ g \mid g \in G\}$$

Denotaremos

$$S/G := \{\text{orb}(s) \mid s \in S\}$$

TEOREMA 5.3. Si \circ es una acción del grupo G sobre el conjunto S , entonces la relación $s_1 \equiv_G s$ si $s_1 \in \text{orb}(s)$ es una relación de equivalencia sobre S , cuyas clases de equivalencia, de cada elemento, son precisamente las órbitas.

OBSERVACIÓN. Aunque en la demostración nosotros asumiremos que la acción es por la izquierda, el lector podrá cerciorarse de que el teorema también vale para una acción por la derecha.

DEMOSTRACIÓN.

- a) \equiv_G es reflexiva. $s \equiv_G s$, pues $s = e \circ s \in \text{orb}(s)$
- b) \equiv_G es simétrica. En efecto si $s_1 \equiv_G s$ entonces $s_1 \in \text{orb}(s)$, esto implica que existe $g \in G$, tal que $s_1 = g \circ s$. Por otra parte $s = e \circ s = (g^{-1}g)s = g^{-1}(g \circ s) = g^{-1}s_1$, lo que implica que $s \in \text{orb}(s_1)$, por consiguiente $s \equiv_G s_1$.
- c) \equiv_G es transitiva. Si $s_1 \equiv_G s$ y $s \equiv_G s_2$, entonces existen $g, h \in G$, tales que $s_1 = g \circ s$ y $s = h \circ s_2$. Entonces $s_1 = g \circ s = g \circ (h \circ s_2) = (gh) \circ s_2$, lo que implica que $s_1 \in \text{orb}(s_2)$. Por consiguiente $s_1 \equiv_G s_2$.

□

Del teorema 5.3 se obtiene el siguiente

COROLARIO 5.4.

- a) Dos órbitas son disjuntas o son iguales.
- b) $S = \bigcup_{s \in S} \text{orb}(s)$

Por lo que cada elemento de S está en una única órbita.

EJEMPLOS 5.1.

1. Sea S un conjunto cualquiera no vacío, \mathfrak{S} el grupo de todas las biyecciones sobre S . Consideremos la siguiente operación binaria $* : \mathfrak{S} \times S \rightarrow S$, definida por $\varphi * s := \varphi(s)$. $\forall (\varphi, s) \in \mathfrak{S} \times S$. $*$ es una acción del grupo \mathfrak{S} sobre S . En efecto $\mathbf{e} * s = \mathbf{e}(s) = s$ y $(\varphi \circ \psi) * s = (\varphi \circ \psi)(s) = \varphi(\psi(s)) = \varphi * (\psi * s)$.
2. Sea $\mathbb{S}^1 := \{\mathbf{x} \in \mathbb{R}^2 \mid \|\mathbf{x}\| = 1\}$, el círculo de radio 1 con centro en el origen. $G := \{1, -1\}$ con el producto usual. Entonces la operación binaria $\cdot : G \times \mathbb{S}^1 \rightarrow \mathbb{S}^1$, definida por $\lambda \cdot \mathbf{x} := \lambda \mathbf{x}$ es una acción del grupo G sobre \mathbb{S}^1 por la izquierda (comprobar!). $\mathbb{S}^1/G = \mathbb{P}^1$, el espacio proyectivo de dimensión 1.
3. En forma análoga al ejemplo precedente, G actúa, por la izquierda, sobre la n -esfera $\mathbb{S}^n := \{\mathbf{x} \in \mathbb{R}^{n+1} \mid \|\mathbf{x}\| = 1\}$ y $\mathbb{S}^n/G = \mathbb{P}^n$ el espacio proyectivo n -dimensional.

En la geometría y topología diferencial y algebraica juegan un papel muy importante las llamadas G -variedades. Éstas son variedades que se obtienen como órbitas de una acción de un grupo G sobre otra variedad.

5.0.8.2. Ciclos de una Permutación. Sea $\sigma \in \mathfrak{S}_n$ y $G := \langle \sigma \rangle$ el grupo cíclico generado por σ , entonces por medio de la operación binaria $\cdot : G \times \mathfrak{S}_n \rightarrow \mathfrak{S}_n$, definida por $\sigma \cdot s := \sigma(s)$, G actúa por la izquierda sobre \mathfrak{S}_n . La órbita de s es entonces $\text{orb}(s) = \{\sigma(s), \sigma^2(s), \dots, \sigma^r(s)\}$, donde, $\sigma^r(s) = s$ y $r \leqslant o(\sigma)$.

DEFINICIÓN 5.2. A la r -eada ordenada

$$\sigma_s := (s \ \sigma(s) \ \dots \ \sigma^{r-1}(s))$$

la llamamos un *ciclo*, de *longitud* $l(\sigma_s) := r - 1$, o un *r-ciclo*, de la permutación σ , correspondiente al elemento s .

Como los ciclos nos representan órbitas ordenadas, cada elemento $s \in \mathfrak{S}_n$ se encuentra en un único ciclo.

EJEMPLO 5.2. Consideremos la permutación sobre \mathfrak{S}_8

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

Para encontrar sus ciclos partimos de un elemento cualquiera s y aplicamos sucesivamente σ hasta llegar de nuevo a s , luego tomamos un s_1 que no aparezca en la órbita de s , hasta que hayamos obtenido todos los elementos de \mathfrak{S}_8 al hacer la unión de todos los ciclos. Empecemos, pues, con $s = 1$. Su ciclo correspondiente es

$$\sigma_1 := (1 \ 3 \ 5 \ 7)$$

Como el 2 no aparece en este ciclo, procedemos entonces, de forma análoga con $s = 2$

$$\sigma_2 := (2 \ 4 \ 6 \ 8)$$

Como ya todos los elementos del conjunto $\mathfrak{S}_4 := \{1, 2, 3, 4, 5, 6, 7, 8\}$ están en uno de los dos ciclos, éstos son los únicos ciclos de σ . En este ejemplo los dos ciclos son 4-ciclos o ciclos de longitud 3.

EJEMPLO 5.3. Consideremos la permutación

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

Sus ciclos son:

$$\sigma_1 := \begin{pmatrix} 1 & 3 & 7 \end{pmatrix}$$

$$\sigma_2 := \begin{pmatrix} 2 & 4 & 6 \end{pmatrix}$$

$\sigma_5 := (5)$, $\sigma_8 := (8)$. En este caso obtenemos que σ posee dos 3-ciclos y dos 1-ciclo, o ciclos de longitud 0.

DEFINICIÓN 5.3. Decimos que una permutación es *cíclica* o *circular* si sólamente posee un único ciclo.

EJEMPLO 5.4.

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$$

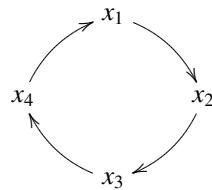
Su único ciclo es

$$\begin{pmatrix} 1 & 2 & 3 & 4 \end{pmatrix}$$

Nótese que una permutación cíclica o circular, por ejemplo, que su único ciclo es

$$\begin{pmatrix} x_1 & x_2 & x_3 & x_4 \end{pmatrix}$$

sigue el siguiente esquema circular, el cual da origen al nombre



Mientras sigamos la dirección de las flechas es irrelevante con qué elemento del ciclo arranquemos.

Nótese, también, que todo r -ciclo, $r < n$, puede ser considerado como una permutación que sólo mueve los elementos que están en él, de forma circular y deja fijo el resto de los $n - r$ elementos de S_n . En particular toda transposición es un 2-ciclo o ciclo de longitud 1.

TEOREMA 5.5. *Todo ciclo σ de longitud $l(\sigma) = r - 1$ genera un grupo cíclico de orden $r = l(\sigma) + 1$. Si*

$$\sigma := \begin{pmatrix} x_1 & x_2 & \cdots & x_r \end{pmatrix}$$

entonces

$$\tau := \begin{pmatrix} x_r & x_{r-1} & \cdots & x_1 \end{pmatrix}$$

es la inversa σ^{-1} de σ .

DEMOSTRACIÓN. Sea $X := \{x_1, \dots, x_r\}$. Si $s \notin X$, $\sigma(s) = s$, entonces basta mostrar que σ^r , es la identidad sobre X y que si $j < r$, entonces σ^j no es la identidad sobre X . En efecto, como σ es un ciclo de longitud $l(\sigma) = r - 1$, para $1 \leq i < r$ se tiene $\sigma(x_i) = x_{i+1}$. Si j es tal que $i + j \leq r$, entonces $\sigma^j(x_1) = x_{i+j}$. Para $i = r$, $\sigma(x_r) = x_1$ y $\sigma^i(x_r) = x_i$, $\forall i \leq r$. Entonces $\sigma^r(x_i) = \sigma^i(\sigma^{r-i}(x_i)) = \sigma^i(x_r) = x_i$. Lo que muestra que σ^r restringido a X es la identidad. Si $j < r$, sea i tal que $i + j \leq r$, entonces $\sigma^j(x_i) = x_{i+j} \neq x_i$, por lo que σ_j no es la identidad sobre X .

Por otra parte, para $1 \leq i < r$, $\tau\sigma(x_i) = \tau(x_{i+1}) = x_i$ y para $i = r$, $\tau(\sigma(x_r)) = \tau(x_1) = x_r$, por lo que $\tau\sigma$ es la identidad sobre X . Además para $1 < i \leq r$, se tiene que $\sigma(\tau(x_i)) = \sigma(x_{i-1}) = x_i$ y para $i = 1$, $\sigma(\tau(x_1)) = \sigma(x_r) = x_1$, lo que muestra que también

$\sigma\tau$ es la identidad sobre X . Por consiguiente $\tau = \sigma^{-1}$, ya que los elementos que no están en X no son afectados por σ y τ . Así pues

$$\mathbf{e} = \begin{pmatrix} x_1 & x_2 & \cdots & x_r \end{pmatrix} \begin{pmatrix} x_r & x_{r-1} & \cdots & x_1 \end{pmatrix}$$

□

De la demostración del teorema 5.5 resulta el siguiente

COROLARIO 5.6. Si $\sigma := \begin{pmatrix} x_1 & x_2 & \cdots & x_r \end{pmatrix}$, entonces σ^j es el ciclo o producto de ciclos que mapea $x_i \rightarrow x_{i+j}$, donde $i + j$ se toma $(\text{mód } r)$

EJEMPLOS 5.5.

1.

$$\begin{pmatrix} 2 & 4 & 6 \end{pmatrix}^2 = \begin{pmatrix} 2 & 6 & 4 \end{pmatrix}$$

2.

$$\begin{pmatrix} x_1 & x_2 & x_3 & x_4 \end{pmatrix}^2 = \begin{pmatrix} x_1 & x_3 \end{pmatrix} \begin{pmatrix} x_2 & x_4 \end{pmatrix}$$

3.

$$\begin{pmatrix} x_1 & x_2 & x_3 & x_4 \end{pmatrix}^3 = \begin{pmatrix} x_1 & x_4 & x_3 & x_2 \end{pmatrix}$$

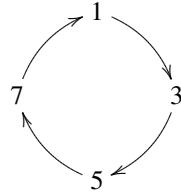
Analicemos de cerca el ejemplo 5.2. Consideremos el ciclo σ_1 como una permutación circular de sus elementos. El resto de los elementos $F_1 := \{1, 2, 3, 4, 5, 6, 7, 8\} \setminus \{1, 3, 5, 7\} = \{2, 4, 6, 8\}$ permanecen entonces fijos. Si escribimos σ_1 en la forma usual obtenemos

$$\sigma_1 := \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 2 & 5 & 4 & 7 & 6 & 1 & 8 \end{pmatrix}$$

Los elementos que permanecen fijos dan lugar a ciclos de longitud 0, los cuales son de la forma (i) , $i \in F_1$, que no mueven nada y pueden ser identificados con \mathbf{e} .

Si restringimos σ_1 al conjunto de elementos que no permanecen fijos $F_2 := \{1, 3, 5, 7\}$ se obtiene

$$\sigma_1|_{F_2} = \begin{pmatrix} 1 & 3 & 5 & 7 \\ 3 & 5 & 7 & 1 \end{pmatrix}$$



que es una permutación circular, cuyo único ciclo es precisamente σ_1 .

En forma análoga podemos proceder con σ_2 , que será una permutación que deja fijos los elementos del conjunto F_2 . Un simple cálculo muestra que $\sigma = \sigma_1\sigma_2 = \sigma_2\sigma_1$.

En general se tiene el siguiente resultado

LEMA 5.7. *El producto de dos ciclos disjuntos σ, τ es commutativo.*

DEMOSTRACIÓN. Debemos mostrar que $\forall s \in S_n$, $\sigma(\tau(s)) = \tau(\sigma(s))$. En efecto, si s no pertenece a ninguno de los dos ciclos, entonces s permanece fijo, tanto bajo σ como bajo τ y $\sigma(\tau(s)) = s = \tau(\sigma(s))$. Por otra parte si s pertenece al ciclo σ , s no pertenece al ciclo τ y permanece fija bajo τ , entonces $\tau(\sigma(s)) = \sigma(s) = \sigma(\tau(s))$. Un razonamiento análogo nos muestra que si s está en el ciclo τ , entonces $\sigma(\tau(s)) = \tau(s) = \tau(\sigma(s))$. □

DEFINICIÓN 5.4. Dada una permutación $\sigma \in \mathfrak{S}_n$ sobre un conjunto S_n , al conjunto

$$D(\sigma) := \{s \in S_n \mid \sigma(s) \neq s\}$$

lo llamamos el *dominio de acción* de la permutación σ .

Es obvio que si $s_1 = \sigma(s) \neq s$, entonces $\sigma(s_1) \neq s_1$, pues de lo contrario σ no sería una biyección. De esto se deduce que $\sigma[D(\sigma)] = D(\sigma)$, $\forall \sigma \in \mathfrak{S}_n$. En el caso en que σ es un ciclo, nótese que si $s \in D(\sigma)$, entonces $D(\sigma) = \text{orb}(s)$.

Una generalización del lema 5.7 es el siguiente

LEMA 5.8. Si $\sigma, \tau \in \mathfrak{S}_n$ son dos permutaciones, tales que $D(\sigma) \cap D(\tau) = \emptyset$, entonces $\sigma\tau = \tau\sigma$.

DEMOSTRACIÓN. La demostración es similar a la del lema 5.7. En efecto, si $s \notin (D(\sigma) \cup D(\tau))$, entonces $\sigma(\tau(s)) = \sigma(s) = s$ y $\tau(\sigma(s)) = \tau(s) = s$. Si $s \in D(\sigma)$, entonces $s, \sigma(s) \notin D(\tau)$ y $\sigma(\tau(s)) = \sigma(s) = \tau(\sigma(s))$. En forma análoga, si $s \in D(\tau)$, entonces $\tau(\sigma(s)) = \tau(s) = \sigma(\tau(s))$. Por consiguiente, en cualquier caso $\sigma\tau(s) = \tau\sigma(s)$, $\forall s \in S_n$, lo que implica que $\sigma\tau = \tau\sigma$. \square

LEMA 5.9. Si $\sigma_1, \dots, \sigma_m$ son ciclos disjuntos de longitud $l(\sigma_i) > 0$ y $\sigma := \sigma_1 \cdots \sigma_m$, entonces los ciclos de σ , de longitud $l(\sigma_i) > 0$, son exactamente $\sigma_1, \dots, \sigma_m$.

DEMOSTRACIÓN. En efecto, sea $s \in D(\sigma)$, y $(s \ \sigma(s) \ \dots \ \sigma^{r-1}(s))$ el ciclo correspondiente. Como σ es el producto de ciclos disjuntos, s está en un único $D(\sigma_i)$, y $\sigma(s) = \sigma_i(s)$, por lo que $(s \ \sigma(s) \ \dots \ \sigma^{r-1}(s)) = (s \ \sigma_i(s) \ \dots \ \sigma_i^{r-1}(s)) = \sigma_i$. \square

TEOREMA 5.10 (Descomposición Canónica en Producto de Ciclos Disjuntos). *Toda permutación $\sigma \in \mathfrak{S}_n$ distinta de la identidad, posee una representación única, salvo orden de sus factores, como producto de todos sus ciclos disjuntos de longitud $l(\sigma_s) > 0$.*

DEMOSTRACIÓN. Sean $\sigma_1, \dots, \sigma_m$ todos los ciclos disjuntos, de longitud $l(\sigma_i) > 0$, correspondientes a σ , entonces, para $i \neq j$, $1 \leq i, j \leq m$, $D(\sigma_i) \cap D(\sigma_j) = \emptyset$. Si $s \in S_n$ permanece fijo bajo σ , entonces s está en un ciclo de longitud 0 y no está en ningún $D(\sigma_i)$, $1 \leq i \leq m$, por lo que no es afectada por ninguno σ_i , $1 \leq i \leq m$ y $(\sigma_1 \cdots \sigma_m)(s) = s = \sigma(s)$. Si s no queda fijo bajo σ , entonces s está en exactamente un único $D(\sigma_i)$, lo que significa que $\sigma(s) = \sigma_i(s)$ y s no es afectado por σ_j , $j \neq i$. entonces $(\sigma_1 \cdots \sigma_m)(s) = \sigma_i(s) = \sigma(s)$. Por consiguiente $\forall s \in S_n$, $\sigma(s) = (\sigma_1 \cdots \sigma_m)(s)$ lo que muestra que $\sigma = \sigma_1 \cdots \sigma_m$.

Por otra parte, si σ es producto de ciclos τ_1, \dots, τ_k , disjuntos, de longitud $l(\tau_i) > 0$, estos son, por lema 5.9, sus ciclos correspondientes, por lo que $\{\sigma_1, \dots, \sigma_m\} = \{\tau_1, \dots, \tau_k\}$, por consiguiente $k = m$ y, después de un reordenamiento adecuado, $\sigma_i = \tau_i$. \square

La descomposición canónica en producto de ciclos disjuntos tiene sus ventajas, ya que con ello se facilita el cálculo de potencias e inversas de una permutación, ya que, al ser disjuntos los ciclos, el producto entre ellos es conmutativo y para el cálculo de las inversas aplicamos el resultado del teorema 5.5 a cada ciclo individual.

EJEMPLOS 5.6.

- Consideremos la permutación sobre S_8 , del ejemplo 5.2

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

sus ciclos correspondientes son:

$$\sigma_1 := (1 \ 3 \ 5 \ 7) \quad \sigma_2 := (2 \ 4 \ 6 \ 8)$$

Por consiguiente

$$\sigma = \sigma_1 \sigma_2 = (1 \ 3 \ 5 \ 7)(2 \ 4 \ 6 \ 8)$$

$$\sigma^{-1} = \sigma_1^{-1} \sigma_2^{-1} = (7 \ 5 \ 3 \ 1)(8 \ 6 \ 4 \ 2)$$

$$\sigma^2 = \sigma_1^2 \sigma_2^2 = (1 \ 3 \ 5 \ 7)^2 (2 \ 4 \ 6 \ 8)^2 = (1 \ 5)(3 \ 7)(2 \ 6)(4 \ 8)$$

2. $\sigma := \sigma_1 \sigma_2 \sigma_3$ producto de ciclos no disjuntos

$$\sigma = \sigma_1 \sigma_2 \sigma_3 = (1 \ 3 \ 5 \ 2)(2 \ 4 \ 6)(7 \ 5 \ 8)$$

y deseamos una representación de σ como producto de ciclos disjuntos. Procedemos de la siguiente forma: Empezamos por los elementos de $D(\sigma_3)$, por ejemplo el 7 y aplicamos sucesivamente $\sigma_3, \sigma_2, \sigma_1$, vemos que $7 \rightarrow 5 \rightarrow 2$, ahora 2 no es afectado por σ_3 , sólo por σ_2 y obtenemos $2 \rightarrow 4$, 4 es afectado sólo por σ_2 y $4 \rightarrow 6$ y $6 \rightarrow 2 \rightarrow 1$, $1 \rightarrow 3$, $3 \rightarrow 5$ y $5 \rightarrow 8$, por lo que nos queda el ciclo

$$\sigma := (7 \ 2 \ 4 \ 6 \ 1 \ 3 \ 5 \ 8) \quad \sigma^{-1} := (8 \ 5 \ 3 \ 1 \ 6 \ 4 \ 2 \ 7)$$

$$\sigma^3 := (7 \ 6 \ 5 \ 2 \ 1 \ 8 \ 4 \ 3) \quad \sigma^{-3} := (7 \ 2 \ 4 \ 6 \ 1 \ 3 \ 5 \ 8)$$

3. Dar la representación como producto de ciclos disjuntos de

$$\sigma := (1 \ 2 \ 3)(3 \ 1 \ 4)(3 \ 5)$$

Empecemos con 3, $3 \rightarrow 5$ y ahí se queda. $5 \rightarrow 3 \rightarrow 1 \rightarrow 2$, 2 se cierra el primer ciclo. $4 \rightarrow 3 \rightarrow 1$, $1 \rightarrow 4$, se cierra el segundo y último ciclo. Entonces

$$\sigma := (3 \ 5 \ 2)(4 \ 1)$$

También el cálculo de elementos conjugados de la forma $\tau\sigma\tau^{-1}$ se facilita con la representación canónica en producto de ciclos disjuntos, como lo muestra el siguiente

TEOREMA 5.11. *Dado el ciclo*

$$\sigma := (x_1 \ x_2 \ \cdots \ x_r)$$

y una permutación cualquiera τ , entonces

$$(5.2) \quad \tau\sigma\tau^{-1} = (\tau(x_1) \ \tau(x_2) \ \cdots \ \tau(x_r))$$

DEMOSTRACIÓN. En efecto, $\tau\sigma\tau^{-1}(x) = \tau\sigma(\tau^{-1}(x))$, si $\tau^{-1}(x) \notin D(\sigma)$, entonces $\sigma(\tau^{-1}(x)) = \tau^{-1}(x)$ y $\tau(\sigma(\tau^{-1}(x))) = x$. Si $\tau^{-1}(x) \in D(\sigma)$, entonces existe $x_i \in D(\sigma)$, tal que $\tau^{-1}(x) = x_i$ y $x = \tau(x_i)$. Entonces $\tau\sigma\tau^{-1}(\tau(x_i)) = \tau(\sigma(\tau^{-1}(x))) = \tau(\sigma(x_i)) = \tau(x_{i+1})$, $i + 1 \pmod r$, de donde resulta (5.2). \square

Si $\sigma := \sigma_1 \sigma_2 \cdots \sigma_m$ es la descomposición canónica de σ como producto de ciclos disjuntos, entonces $\tau\sigma\tau^{-1} = \tau\sigma_1 \sigma_2 \cdots \sigma_m \tau^{-1} = \tau\sigma_1 \tau^{-1} \tau\sigma_2 \tau^{-1} \cdots \tau\sigma_m \tau^{-1}$. Entonces reescribimos cada ciclo σ_i , $1 \leq i \leq m$ de la forma (5.2)

Como ya hemos visto, para $n \geq 3$, el grupo \mathfrak{S}_n no es commutativo. Pero, además, fuera de la identidad, ninguna permutación commuta con todos los elementos de \mathfrak{S}_n , como se muestra en el siguiente

TEOREMA 5.12. *Para $n \geq 3$ el centro $Z(\mathfrak{S}_n) = \{\mathbf{e}\}$.*

DEMOSTRACIÓN. Sea $\sigma \in \mathfrak{S}_n$, $\sigma \neq \mathbf{e}$, entonces existe $a \in S_n$, tal que $\sigma(a) \neq a$, como $n \geq 3$, existe $c \in S_n$, tal que $a \neq c \neq \sigma(a)$, entonces la transposición

$$\begin{pmatrix} a & c \end{pmatrix}$$

está bien definida y

$$\sigma \begin{pmatrix} a & c \end{pmatrix} \sigma^{-1} = \begin{pmatrix} \sigma(a) & \sigma(c) \end{pmatrix} \neq \begin{pmatrix} a & c \end{pmatrix}$$

por consiguiente $\sigma \notin Z(\mathfrak{S}_n)$. \square

Dada una permutación $\sigma \in \mathfrak{S}_n$, denotaremos por $C(\sigma)$ el conjunto de sus ciclos disjuntos.

DEFINICIÓN 5.5. Decimos que dos permutaciones $\sigma, \tau \in \mathfrak{S}_n$ son *semejantes*, si existe una biyección $\Psi : C(\sigma) \rightarrow C(\tau)$, tal que $l(\Psi(\sigma_s)) = l(\sigma_s)$, $\forall \sigma_s \in C(\sigma)$.

Por ejemplo las permutaciones

$$\sigma = \begin{pmatrix} 1 & 5 \end{pmatrix} \begin{pmatrix} 3 & 4 & 2 \end{pmatrix} \quad \tau = \begin{pmatrix} 1 & 2 \end{pmatrix} \begin{pmatrix} 4 & 3 & 5 \end{pmatrix}$$

son semejantes.

TEOREMA 5.13. *Dos permutaciones $\sigma, \tau \in \mathfrak{S}_n$ son semejantes Ssi son conjugadas. Es decir que existe $\phi \in \mathfrak{S}_n$, tal que $\sigma = \phi\tau\phi^{-1}$.*

DEMOSTRACIÓN. Si σ, τ son conjugadas, entonces, por teorema 5.11, σ, τ son semejantes.

Supongamos, entonces, que σ, τ son semejantes y distintas a la identidad, para la cual el teorema es obvio. Entonces $C(\sigma) = \{\sigma_1, \dots, \sigma_m\}$ y $C(\tau) = \{\tau_1, \dots, \tau_m\}$, con $l(\sigma_i) = l(\tau_i)$, $1 \leq i \leq m$. Entonces podemos escribir

$$\sigma_i := \begin{pmatrix} x_1^i & x_2^i & \cdots & x_{r_i}^i \end{pmatrix} \quad \tau_i := \begin{pmatrix} y_1^i & y_2^i & \cdots & y_{r_i}^i \end{pmatrix}$$

Entonces, para cada $1 \leq i \leq m$, se tiene una bijección $\phi_i : D(\sigma_i) \rightarrow D(\tau_i)$, definida por $\phi_i(x_j^i) := y_j^i$, $1 \leq j \leq r_i$, la cual puede ser extendida a una biyección $\phi : S_n \rightarrow S_n$ y $\phi \in \mathfrak{S}_n$. Entonces

$$\tau_i := \begin{pmatrix} \phi(x_1^i) & \phi(x_2^i) & \cdots & \phi(x_{r_i}^i) \end{pmatrix} = \phi\sigma_i\phi^{-1}, \quad \forall i, 1 \leq i \leq m$$

De aquí resulta, entonces, que $\tau = \phi\sigma\phi^{-1}$. \square

Dejamos al lector la demostración del siguiente

COROLARIO 5.14. *La relación de semejanza es una relación de equivalencia sobre \mathfrak{S}_n*

Otro resultado interesante es el siguiente

TEOREMA 5.15. *Toda permutación $\sigma \in \mathfrak{S}_n$, $n \geq 3$ puede ser representada como un producto de transposiciones.*

DEMOSTRACIÓN. Basta mostrar el teorema para el caso de un ciclo. La demostración resulta del proceso de recurrencia siguiente

$$\begin{aligned} \begin{pmatrix} x_1 & x_2 & \cdots & x_r \end{pmatrix} &= \begin{pmatrix} x_1 & x_2 \end{pmatrix} \begin{pmatrix} x_2 & x_3 & \cdots & x_r \end{pmatrix} \\ &= \begin{pmatrix} x_1 & x_2 \end{pmatrix} \begin{pmatrix} x_2 & x_3 \end{pmatrix} \begin{pmatrix} x_3 & x_4 & \cdots & x_r \end{pmatrix} \\ &= \cdots \end{aligned}$$

\square

EJEMPLO 5.7. El ciclo $\sigma := \begin{pmatrix} x_1 & x_2 & x_3 & x_4 \end{pmatrix}$, siguiendo el proceso descrito en la demostración del teorema 5.15, se descompone en las transposiciones

$$\begin{pmatrix} x_1 & x_2 \end{pmatrix} \begin{pmatrix} x_2 & x_3 \end{pmatrix} \begin{pmatrix} x_3 & x_4 \end{pmatrix}$$

OBSERVACIÓN 5.1. Como se podrá observar, del proceso de recurrencia, para la descomposición de un ciclo σ , en transposiciones, si el ciclo es de longitud $l(\sigma)$, se obtienen $l(\sigma)$ transposiciones. $l(\sigma)$ es el menor número de transposiciones que se necesitan para representar σ como producto de éstas.

A diferencia de la representación canónica como producto de ciclos disjuntos, la representación como producto de transposiciones no es única, ni todas las transposiciones son disjuntas. Siempre es posible agregar factores de la forma $\mathbf{e} = \begin{pmatrix} x_1 & x_2 \end{pmatrix} \begin{pmatrix} x_1 & x_2 \end{pmatrix}$.

A continuación extenderemos el concepto de longitud de un ciclo a una permutación cualquiera $\sigma \in \mathfrak{S}_n$

DEFINICIÓN 5.6. Sea $\sigma \in \mathfrak{S}_n$, $\sigma \neq \mathbf{e}$ y $\sigma = \sigma_1 \cdots \sigma_m$ su representación canónica como producto de ciclos disjuntos. Entonces, definimos la *longitud* de σ , como

$$(5.3) \quad l(\sigma) := \sum_{j=1}^m l(\sigma_j)$$

Obviamente $1 \leq l(\sigma) \leq n - 1$.

Si nosotros tenemos una permutación dada como producto de ciclos, no necesariamente disjuntos o producto de transposiciones, la suma de sus longitudes puede variar. Lo que no va a variar, como veremos más adelante, es el hecho de que la longitud sea un número par o impar, lo que define la *paridad* de la permutación. El concepto de paridad juega un papel muy importante en la teoría de determinantes y en el estudio de las álgebras externas. Dado que las transposiciones son ciclos de longitud 1, si la longitud de una permutación es par, ésta se descompondrá siempre en un número par de transposiciones y si la longitud es impar, entonces se descompondrá siempre en un número impar de transposiciones.

TEOREMA 5.16. Sea $\sigma \in \mathfrak{S}_n$ una permutación, $\begin{pmatrix} x & y \end{pmatrix} \in \mathfrak{S}_n$ una transposición. Entonces, si $\tau := \begin{pmatrix} x & y \end{pmatrix} \sigma$

$$l(\tau) - l(\sigma) = \begin{cases} 1 & \text{o,} \\ -1 & \end{cases}$$

DEMOSTRACIÓN. Si x, y no son afectados por σ , entonces $l(\tau) = l(\sigma) + 1$. Si x, y son afectados por σ , entonces sólo vale la pena considerar aquellos ciclos que afectan a x, y . A tal efecto es suficiente considerar los siguientes dos casos:

- a) x, y están en el mismo ciclo. $\sigma := \begin{pmatrix} x & \cdots & x_r & y & \cdots & y_s \end{pmatrix}$. Entonces $l(\sigma) = r+s-1$. Un simple cálculo nos muestra que $\tau = \begin{pmatrix} x & x_2 & \cdots & x_r \end{pmatrix} \begin{pmatrix} y & y_2 & \cdots & y_s \end{pmatrix}$, y $l(\tau) = r - 1 + s - 1 = r + s - 2 = l(\sigma) - 1$
- b) x, y están en diferentes ciclos disjuntos. $\sigma := \begin{pmatrix} x & x_2 & \cdots & x_r \end{pmatrix} \begin{pmatrix} y & y_2 & \cdots & y_s \end{pmatrix}$. Entonces en este caso $\tau = \begin{pmatrix} x & \cdots & x_r & y & \cdots & y_s \end{pmatrix}$ y $l(\sigma) = l(\tau) - 1$.

El caso en que sólo uno de los elementos x, y es afectado está incluido en el razonamiento anterior, haciendo $r = 1$ o $s = 1$. \square

Una de las consecuencias del teorema 5.16 es que si la longitud de σ es un número par (ímpar), entonces la longitud de τ es un número ímpar (par). También, en la demostración

queda claro que $\tau \neq \sigma$ y para recuperar σ partiendo de τ debemos multiplicar τ de nuevo por la misma transposición.

DEFINICIÓN 5.7. Decimos que una permutación $\sigma \in \mathfrak{S}_n$ es *par (impar)*, si $l(\sigma)$ es par (ímpar).

Entonces toda transposición es impar, mientras que todo 3-ciclo es par. En general todo m -ciclo es par, si m impar y viceversa.

TEOREMA 5.17. *Sea $\sigma := \sigma_1 \cdots \sigma_m \in \mathfrak{S}_n$ un producto de transposiciones. Entonces el número m de los factores es par Ssi $l(\sigma)$ es par.*

DEMOSTRACIÓN. Por inducción sobre m . En efecto, si $m = 1$, entonces $l(\sigma) = 1$ y ambos son impares. Sea ahora $m \geq 2$ y supongamos que el teorema sea válido para $m - 1$. Sea entonces $\hat{\sigma} := \sigma_2 \cdots \sigma_m$. Por teorema 5.16 $\hat{\sigma}$ es par Ssi σ es impar. Por hipótesis de inducción tenemos entonces que $\hat{\sigma}$ es par, o sea σ impar, Ssi $m - 1$ es par y esto Ssi m es impar. \square

DEFINICIÓN 5.8. La aplicación $\pi : \mathfrak{S}_n \rightarrow \{-1, 1\}$, definida por

$$(5.4) \quad \pi(\sigma) := \begin{cases} 1 & \text{si } \sigma \text{ par,} \\ -1 & \text{si } \sigma \text{ impar.} \end{cases}$$

se llama la *función de paridad*.

TEOREMA 5.18. *La función de paridad $\pi : \mathfrak{S}_n \rightarrow \{-1, 1\}$ es un homomorfismo entre el grupo de simetría \mathfrak{S}_n y el grupo multiplicativo $\{-1, 1\}$.*

DEMOSTRACIÓN. En efecto, si σ, τ son pares, entonces $\sigma\tau$ es par y $\pi(\sigma\tau) = 1 = \pi(\sigma)\pi(\tau)$. Si σ, τ son impares, entonces $\sigma\tau$ par y $\pi(\sigma\tau) = 1 = (-1)(-1) = \pi(\sigma)\pi(\tau)$. Si una es par y la otra impar, supongamos, sin limitación de la generalidad, que σ impar y τ par, entonces $\sigma\tau$ es impar y $\pi(\sigma\tau) = -1 = (-1)(1) = \pi(\sigma)\pi(\tau)$. \square

Consideremos

$$\mathfrak{A}_n := \{\sigma \in \mathfrak{S}_n \mid \sigma \text{ es par}\}$$

el conjunto de las permutaciones pares. Entonces se tiene el siguiente

TEOREMA 5.19. *\mathfrak{A}_n es un subgrupo normal de \mathfrak{S}_n , de orden $\frac{1}{2}n!$ e índice 2, para $n \geq 2$ y no abeliano para $n \geq 4$.*

DEMOSTRACIÓN. En efecto \mathfrak{A}_n es cerrado bajo el producto, ya que el producto de permutaciones pares es otra permutación par, por lo tanto, es un subgrupo de \mathfrak{S}_n , por ser \mathfrak{A}_n finito. Por otra parte \mathfrak{A}_n es el núcleo del homomorfismo de paridad π , por consiguiente normal y por el teorema de factorización e isomorfía $\mathfrak{S}_n/\mathfrak{A}_n$ es isomorfo al grupo $\{-1, 1\}$, de donde resulta que $i_{\mathfrak{S}_n}(\mathfrak{A}_n) = 2$ y $\circ(\mathfrak{A}_n) = \frac{1}{2}n!$.

Para $n \geq 4$, la siguiente ecuación nos muestra que \mathfrak{A}_n no puede ser abeliano. En efecto

$$\left(\begin{array}{ccc} x_1 & x_2 & x_4 \end{array} \right) \left(\begin{array}{ccc} x_1 & x_2 & x_3 \end{array} \right) \left(\begin{array}{ccc} x_1 & x_2 & x_4 \end{array} \right)^{-1} = \left(\begin{array}{ccc} x_2 & x_4 & x_3 \end{array} \right)$$

\square

DEFINICIÓN 5.9. El subgrupo $\mathfrak{A}_n \subseteq \mathfrak{S}_n$ se llama el *subgrupo alternante* de \mathfrak{S}_n .

A continuación daremos algunas propiedades importantes del grupo alternante, las cuales jugarán un papel muy importante en la teoría de Galois, que estudiaremos más adelante.

LEMA 5.20. *Todo elemento de \mathfrak{A}_n , $n \geq 3$ se puede escribir como producto de 3-ciclos.*

DEMOSTRACIÓN. Como todo elemento de \mathfrak{A}_n es producto de un número par de transposiciones, basta que mostremos el teorema para productos de dos transposiciones. Pueden darse tres casos:

a)

$$\begin{pmatrix} x_1 & x_2 \end{pmatrix} \begin{pmatrix} x_1 & x_2 \end{pmatrix} = \mathbf{e} = \begin{pmatrix} x_1 & x_2 & x_3 \end{pmatrix}^3$$

b)

$$\begin{pmatrix} x_1 & x_2 \end{pmatrix} \begin{pmatrix} x_3 & x_2 \end{pmatrix} = \begin{pmatrix} x_1 & x_2 & x_3 \end{pmatrix}$$

c)

$$\begin{aligned} \begin{pmatrix} x_1 & x_2 \end{pmatrix} \begin{pmatrix} x_3 & x_4 \end{pmatrix} &= \begin{pmatrix} x_1 & x_2 \end{pmatrix} \begin{pmatrix} x_3 & x_2 \end{pmatrix} \begin{pmatrix} x_3 & x_2 \end{pmatrix} \begin{pmatrix} x_3 & x_4 \end{pmatrix} \\ &= \begin{pmatrix} x_1 & x_2 & x_3 \end{pmatrix} \begin{pmatrix} x_2 & x_3 & x_4 \end{pmatrix} \end{aligned}$$

□

LEMA 5.21. *Todo 3-ciclo es un conmutador en \mathfrak{S}_n , $n \geq 3$.*

DEMOSTRACIÓN. En efecto

$$\begin{pmatrix} x_1 & x_2 & x_3 \end{pmatrix} = \begin{pmatrix} x_1 & x_3 & x_2 \end{pmatrix}^2 = \begin{pmatrix} x_1 & x_3 \end{pmatrix} \begin{pmatrix} x_2 & x_3 \end{pmatrix} \begin{pmatrix} x_1 & x_3 \end{pmatrix}^{-1} \begin{pmatrix} x_2 & x_3 \end{pmatrix}^{-1}$$

□

De los lemas 5.20 y 5.21 se obtiene el siguiente

TEOREMA 5.22. *El grupo alternante \mathfrak{A}_n es el subgrupo de conmutadores de \mathfrak{S}_n .*

DEMOSTRACIÓN. Para $n \leq 2$ el teorema es trivial, ya que $\mathfrak{A}_n\{\mathbf{e}\}$ y \mathfrak{S}_n abeliano. En efecto, de los lemas 5.20 y 5.21 resulta que $\mathfrak{A}_n \subseteq K(\mathfrak{S}_n)$, por otra parte como $\text{o}(\mathfrak{S}_n/\mathfrak{A}_n) = 2$, entonces $\mathfrak{S}_n/\mathfrak{A}_n$ es abeliano, lo que implica que

$$K(\mathfrak{S}_n) \subseteq \mathfrak{A}_n.$$

□

TEOREMA 5.23. *Para $n \geq 5$ son todos los 3-ciclos elementos conjugados de \mathfrak{A}_n .*

DEMOSTRACIÓN. Dados dos 3-ciclos

$$\sigma := \begin{pmatrix} x_1 & x_2 & x_3 \end{pmatrix} \quad \hat{\sigma} := \begin{pmatrix} y_1 & y_2 & y_3 \end{pmatrix}$$

éstos son semejantes y existe $\tau \in \mathfrak{S}_n$, tal que $\hat{\sigma} = \tau \sigma \tau^{-1}$, como $n \geq 5$, existe una transposición $\psi := \begin{pmatrix} u & v \end{pmatrix}$, que conmuta con σ . Sea $\tau_1 := \tau \psi$. Entonces $\tau_1 \sigma \tau_1^{-1} = \tau \psi \sigma \psi \tau^{-1} = \tau \sigma \tau^{-1}$, donde, ya sea $\tau \in \mathfrak{A}_n$, o $\tau_1 \in \mathfrak{A}_n$.

□

El siguiente teorema constituye el pilar fundamental para entender porqué, para $n \geq 5$, la ecuación general de grado n no posee solución por medio de un proceso de radicación.

TEOREMA 5.24. *Para $n \geq 5$ el grupo alternante \mathfrak{A}_n es simple.*

DEMOSTRACIÓN. Sea $n \geq 5$ y N un subgrupo normal de \mathfrak{A}_n no trivial. Vamos a mostrar que N contiene un 3-ciclo, entonces por el teorema 5.23, N contiene a todos los 3-ciclos, los cuales generan \mathfrak{A}_n . Por consiguiente $N = \mathfrak{A}_n$.

En efecto, sea $\sigma \in N \subseteq \mathfrak{A}_n$, entonces σ no es una transposición y mueve a por lo menos tres elementos de S_n . Si σ es un 3-ciclo, ya estamos. Entonces supongamos que σ mueve, al menos, cuatro elementos de S_n . Entonces se dan tres casos:

$$(5.5) \quad \sigma = (x_1 \ x_2 \ x_3 \ x_4 \ \cdots)$$

$$(5.6) \quad \sigma = (x_1 \ x_2 \ x_3)(x_4 \ x_5 \ \cdots)$$

$$(5.7) \quad \sigma = (x_1 \ x_2)(x_3 \ x_4)$$

Supongamos primero el caso (5.5) y sea $\tau := (x_1 \ x_2 \ x_3) \in \mathfrak{A}_n$, entonces $\sigma\tau\sigma^{-1} = (x_2 \ x_3 \ x_4) \in \mathfrak{A}_n$. Como N normal en \mathfrak{A}_n , $\tau\sigma^{-1}\tau^{-1} \in N$, por lo que $\sigma(\tau\sigma^{-1}\tau^{-1}) \in N$. Entonces

$$\sigma(\tau\sigma^{-1}\tau^{-1}) = (\sigma\tau\sigma^{-1})\tau^{-1} = (x_2 \ x_3 \ x_4)(x_3 \ x_2 \ x_1) = (x_1 \ x_4 \ x_2) \in N$$

Supongamos ahora el caso (5.6) y sea $\tau := (x_1 \ x_2 \ x_4)$, entonces

$$\sigma\tau\sigma^{-1} = (x_2 \ x_3 \ x_5)$$

y

$$(\sigma\tau\sigma^{-1})\tau^{-1} = (x_2 \ x_3 \ x_5)(x_4 \ x_2 \ x_1) = (x_1 \ x_4 \ x_3 \ x_5 \ x_2) \in N$$

obteniendo el caso (5.5).

Finalmente tratemos el caso (5.7). Como $n \geq 5$ existe $x_5 \in S_n$, distinto de x_1, x_2, x_3, x_4 y sea $\tau := (x_1 \ x_3 \ x_5)$. Entonces tenemos dos casos posibles: $\sigma(x_5) = x_5$ o $\sigma(x_5) \neq x_5$.

Si $\sigma(x_5) = x_5$, entonces

$$\sigma\tau\sigma^{-1} = (x_2 \ x_4 \ x_5)$$

y

$$(\sigma\tau\sigma^{-1})\tau^{-1} = (x_2 \ x_4 \ x_5)(x_5 \ x_3 \ x_1) = (x_1 \ x_2 \ x_4 \ x_5 \ x_3) \in N$$

obteniendo nuevamente el caso (5.5).

Si $\sigma(x_5) \neq x_5$, entonces:

$$\sigma\tau\sigma^{-1} = (x_2 \ x_4 \ \sigma(x_5))$$

y

$$(\sigma\tau\sigma^{-1})\tau^{-1} = (x_2 \ x_4 \ \sigma(x_5))(x_5 \ x_3 \ x_1) = (x_1 \ x_5 \ x_3)(x_r \ \sigma(x_5) \ \cdots) \in N$$

obteniendo el caso (5.6). \square

DEFINICIÓN 5.10. Decimos que un subgrupo G de \mathfrak{S}_n es transitivo, si para cada par de elementos $x, y \in S_n$, existe $\sigma \in G$, tal que $\sigma(x) = y$.

Dados $x, y \in S_n$, decimos que x es equivalente respecto de G a y , $x \sim_G y$ y Ssi: $x = y$ o $(x \ y) \in G$.

LEMA 5.25. *La relación \sim_G es una relación de equivalencia sobre S_n .*

La demostración la dejamos al lector como un ejercicio.

TEOREMA 5.26. *Si un subgrupo transitivo $G \subseteq \mathfrak{S}_n$ contiene transposiciones y n es un número primo, entonces $G = \mathfrak{S}_n$.*

DEMOSTRACIÓN. Como G contiene transposiciones, por ejemplo $\begin{pmatrix} x & y \end{pmatrix}$, la clase de equivalencia \bar{x} de x contiene más de un elemento. Si $\sigma \in G$, entonces $\begin{pmatrix} \sigma(x) & \sigma(y) \end{pmatrix} = \sigma \begin{pmatrix} x & y \end{pmatrix} \sigma^{-1} \in G$, lo que implica que $\sigma[\bar{x}] \subseteq \overline{\sigma(x)}$. Por otra parte, si aplicamos el mismo argumento a σ^{-1} y a la clase $\overline{\sigma(x)}$ obtenemos que las clases \bar{x} y $\overline{\sigma(x)}$ poseen el mismo número de elementos. Si $z \in S_n$ es otro elemento cualquiera, por la transitividad de G , existe $\sigma \in G$, tal que $\sigma(x) = z$, por consiguiente, todas las clases de equivalencia respecto de \sim_G poseen el mismo número de elementos, digamos m y $m \mid n$. Como $m \geq 2$ y n primo, resulta que $m = n$, lo que implica que todos los elementos de S_n son equivalentes respecto de G y G contiene a todas las transposiciones de \mathfrak{S}_n . Por lo tanto $G = \mathfrak{S}_n$. \square

En los teoremas precedentes mostramos, entre otros resultados, que toda permutación de \mathfrak{S}_n , se descompone, de forma única, salvo orden de sus factores, en un producto de m n_μ -ciclos, $\mu = 1, \dots, m$, disjuntos, donde consideraremos también los ciclos de longitud 0. Como cada elemento de S_n está en uno y sólamente un ciclo, vale que

$$(5.8) \quad n = \sum_{\mu=1}^m n_\mu.$$

Este resultado está relacionado con la llamada *partición* de un número entero n , de gran importancia en la teoría de números y otras áreas de las matemáticas. Decimos que una sucesión finita de enteros n_1, \dots, n_m , tales que $1 \leq n_1 \leq n_2 \leq \dots \leq n_m \leq n$, es una *partición* del número entero n , si

$$(5.9) \quad n = \sum_{\mu=1}^m n_\mu.$$

Un problema clásico de la teoría de números es la determinación del número de particiones posibles, $p(n)$, para un entero n dado. El lector comprobará, sin mucha dificultad, que $p(1) = 1$, $p(2) = 2$, $p(5) = 7$, $p(6) = 11$. Para números grandes el problema se dificulta grandemente.

De la ecuación (5.8) se deduce que los órdenes de todos los ciclos, obtenidos en la descomposición de un elemento de \mathfrak{S}_n , es una partición de n y por el teorema 5.11, todas las permutaciones semejantes o conjugadas dan lugar a la misma partición de n . Por consiguiente se tiene el siguiente resultado que expresamos en el

TEOREMA 5.27. *El número de clases conjugadas en \mathfrak{S}_n es igual a $p(n)$, el número de particiones de n .*

En los siguientes ejemplos daremos una aplicación de los resultados arriba obtenidos en combinación con el teorema 4.26.

EJEMPLOS 5.8.

1. ¿Cuántas permutaciones comutan con una transposición $\sigma := \begin{pmatrix} i & j \end{pmatrix}$ dada? y ¿cuáles son éstas?

El número de permutaciones que comutan con σ viene dado por el orden del normalizador de σ , $N(\sigma)$. Por teorema 4.26 sabemos que $\circ(N(\sigma)) = \frac{\circ(\mathfrak{S}_n)}{c_\sigma}$, donde c_σ es el número de elementos que posee la clase de conjugación $C(\sigma)$.

Como todas las transposiciones son elementos conjugados de cualquier otra, tenemos que c_x es igual al número total de transposiciones en \mathfrak{S}_n que en total son $\frac{n(n-1)}{2}$, entonces $\circ(N(\sigma)) = \frac{\circ(\mathfrak{S}_n)}{c_\sigma} = 2(n-2)!$.

Para determinar cuáles son las permutaciones que comutan con σ procedemos de la siguiente manera: Primeramente todas aquellas permutaciones que no afectan a i, j comutan con σ . De éstas existen $(n-2)!$. Por otra parte, si τ es una permutación que no afecta a i, j , entonces $\sigma\tau$ comuta con σ , ya que $\sigma\tau\sigma = \tau$, por teorema 5.11. En total tenemos ya $2(n-2)!$ permutaciones que comutan con σ . Así pues, las permutaciones que comutan con σ son aquellas de la forma $\sigma^\mu\tau$, $\mu = 1, 2$ y τ cualquier permutación que deja fijos i, j .

2. Por un razonamiento análogo se muestra que el orden del normalizador del n -ciclo $\sigma := (1 \ 2 \ \cdots \ n)$ es n y por consiguiente σ comunica únicamente con sus potencias.
3. En general para calcular el número de m -ciclos diferentes, $m \leq n$ consideramos el número total de combinaciones de n elementos tomados de m en m , importando el orden, lo cual nos da $\frac{n!}{(n-m)!}$, donde m van a representar la misma permutación, por consiguiente tendremos $\frac{n!}{m(n-m)!}$ m -ciclos distintos, los cuales son to-

dos conjugados, por teorema 5.11. Entonces dado un m -ciclo σ , $c_\sigma = \frac{n!}{m(n-m)!}$ y obtenemos $\circ(N(\sigma)) = m(n-m)!$. Si τ es una permutación que deja fijos todos los elementos que mueve σ , τ comunica con σ y tenemos $(n-m)!$ posibilidades para τ . Por otra parte σ comunica con todas sus potencias y con cada elemento de la forma $\sigma^\mu\tau$, $1 \leq \mu \leq m$, donde τ deja fijos todos los elementos que mueve σ . En total obtenemos entonces $m(n-m)!$ permutaciones de la forma $\sigma^\mu\tau$, $1 \leq \mu \leq m$.

TEOREMA 5.28 (Teorema de Cayley). *Todo grupo G es isomorfo, para un conjunto S apropiado, a un subgrupo de $\mathcal{A}(S)$, donde $\mathcal{A}(S)$ es el grupo de todas las biyecciones sobre S .*

DEMOSTRACIÓN. En efecto, sea G un grupo y definamos $S := G$, el conjunto de los elementos de G . Dado $g \in G$, definimos $\phi_g : S \rightarrow S$, por $\phi_g(x) := gx$, $\forall x \in S$, entonces, por la ley de cancelación, ϕ_g es inyectiva. Por otra parte, dado $y \in S$, $y = g(g^{-1}y) = \phi_g(g^{-1}y)$, por lo que ϕ_g es una biyección sobre S y $\phi_g \in \mathcal{A}(S)$. Vamos a mostrar que $\Psi : G \rightarrow \mathcal{A}(S)$ definida por $\Psi(g) := \phi_g$ es un homomorfismo inyectivo y que entonces G es isomorfo al subgrupo $\Psi[G] \subseteq \mathcal{A}(S)$. Por definición $\Psi(gh) = \phi_{gh}$, $\phi_{gh}(x) = (gh)x = g(hx) = \phi_g \circ \phi_h(x)$, $\forall x \in S$ y por consiguiente $\phi_{gh} = \phi_g \circ \phi_h$, lo que muestra que Ψ es un homomorfismo de grupos. Por otra parte si $\Psi(g)$ es la identidad en $\mathcal{A}(S)$, entonces $gx = x$, $\forall x \in S$, de donde $g = e$. Por lo tanto Ψ es inyectiva. \square

Si G es finito de orden n , entonces G es isomorfo a un subgrupo de permutaciones sobre el conjunto $S := G$. Sin embargo uno de los inconvenientes es que para n no tan pequeño, el grupo \mathfrak{S}_n posee $n!$ elementos, lo que hace que G no se visualice bien dentro de un grupo gigantesco. Lo ideal sería encontrar un conjunto S no tan grande, con el cual podamos visualizar mejor a G dentro de $\mathcal{A}(S)$. El siguiente teorema nos acerca un poco más a lo deseado.

TEOREMA 5.29. Si G es un grupo, H un subgrupo de G y S el conjunto de toda las clases laterales izquierdas de H en G , entonces existe un homomorfismo $\Phi : G \rightarrow \mathcal{A}(S)$ y $\ker \Phi$ es el subgrupo normal más grande de G que está contenido en H .

DEMOSTRACIÓN. Dado $g \in G$, sea $\phi_g : S \rightarrow S$, definida por $\phi_g(xH) := gxH$. Un argumento similar al empleado en la demostración del teorema 5.28, nos muestra que $\phi_g \in \mathcal{A}(S)$ y que $\phi_{gh} = \phi_g \circ \phi_h$. Entonces la aplicación $\Phi : G \rightarrow \mathcal{A}(S)$, definida por $\Phi(g) := \phi_g$ es un homomorfismo de grupos. Si $g \in \ker \Phi$, entonces $\Phi(g) = \phi_g$ es la identidad y $\forall x \in G$, $\phi_g(xH) = gxH = xH$, en particular si $x := e$, debe valer que $gH = H$, lo que implica que $g \in H$. Entonces $\ker \Phi \subseteq H$ y $\ker \Phi$ es un subgrupo normal en G de G contenido en H . Por otra parte, si N es otro subgrupo normal en G de G contenido en H , entonces $\forall x \in G$, $xN = Nx$ y dado $g \in N$, $\phi_g(xH) = gxH$ y por la normalidad de N en G , existe $\hat{g} \in N$, tal que $gx = x\hat{g}$. Entonces $gxH = x\hat{g}H = xH$, $\forall x \in G$, por consiguiente $g \in \ker \Phi$. Lo que muestra que $N \subseteq \ker \Phi$. \square

Si en el teorema 5.29, $H := \{e\}$, entonces $S = G$ y obtenemos el teorema de Cayley. Si por otra parte H es un subgrupo que no posee ningún subgrupo normal en G distinto de $\{e\}$, entonces $\ker \Phi = \{e\}$ y $\Phi : G \rightarrow \mathcal{A}(S)$ induce un isomorfismo de G sobre un subgrupo de $\mathcal{A}(S)$ y S , en el caso finito, es un conjunto más pequeño que S .

Como una consecuencia el teorema 5.29 se obtiene el siguiente

COROLARIO 5.30. Si G es un grupo finito y H un subgrupo propio de G , tal que $\circ(G) \nmid i_G(H)!$ Entonces H debe contener un subgrupo normal en G no trivial. En particular G no es simple.

DEMOSTRACIÓN. En efecto si $\circ(G) \nmid i_G(H)! = \circ(\mathcal{A}(S))$, por el teorema de Lagrange, $\mathcal{A}(S)$ no puede contener ningún subgrupo de orden $\circ(G)$, por consiguiente ningún subgrupo isomorfo a G . Como $\Phi[G] \subseteq \mathcal{A}(S)$ es subgrupo, éste no puede, entonces, ser isomorfo a G , por lo que Φ no puede ser inyectiva. Entonces $\ker \Phi \neq \{e\}$ es un subgrupo normal no trivial contenido en H que es normal en G . \square

5.0.9. Ejercicios y Complementos.

1. Dadas las permutaciones

$$\sigma := \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 1 & 2 & 5 & 6 & 7 & 8 & 4 \end{pmatrix} \quad \tau := \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 5 & 6 & 7 & 3 & 2 & 8 & 1 \end{pmatrix}$$

- a) Descomponer σ y τ en producto de ciclos disjuntos y dar longitud de cada uno de sus ciclos.
- b) Dar longitud de σ y τ
- c) Dar descomposición de σ y τ en producto de transposiciones
- d) Dar σ^{-1} y τ^{-1}
- e) Calcular $\sigma\tau\sigma^{-1}$ y $\tau\sigma\tau^{-1}$.

- 2. Mostrar que todo grupo cíclico de orden n es isomorfo al grupo cíclico generado por un n -ciclo.
- 3. Dar explícitamente \mathfrak{A}_3 y \mathfrak{A}_4 .
- 4. Mostrar el corolario 5.14
- 5. Mostrar que \mathfrak{A}_4 es generado por los 3-ciclos $\sigma := (1 \ 2 \ 3)$ y $\tau := (2 \ 3 \ 4)$.
- 6. Mostrar que el grupo de conmutadores de \mathfrak{A}_4 es el grupo obtenido a partir del conmutador $[\sigma, \tau]$, donde σ, τ como en el ejercicio precedente y que

$$K(\mathfrak{A}_4) = \{\mathbf{e}, (1 \ 2)(3 \ 4), (1 \ 3)(2 \ 4), (1 \ 4)(2 \ 3)\}$$

Este grupo se conoce con el nombre de “*Grupo de los Cuatro de Klein*” (Kleinsche Vierer Gruppe), que se suele denotar por \mathfrak{V}_4 y cuyo significado geométrico veremos más adelante.

7. Deducir del ejercicio precedente que \mathfrak{A}_4 no es simple y que posee un subgrupo normal de orden 4.
8. Mostrar que $K(\mathfrak{A}_4)$ es normal en \mathfrak{S}_4 y que $\mathfrak{S}_4/K(\mathfrak{A}_4)$ es un grupo de orden 6 isomorfo a \mathfrak{S}_3 .
9. Mostrar lema 5.25. Tomar en cuenta que

$$\begin{pmatrix} x & z \\ y & z \end{pmatrix} = \begin{pmatrix} y & z \\ x & y \end{pmatrix} \begin{pmatrix} x & y \\ y & z \end{pmatrix}$$

10. Mostrar que si un grupo G de orden 36 posee un subgrupo de orden 9, entonces H posee un subgrupo N , normal en G , no trivial, de orden 3 o 9, por lo que G no es simple.
11. Mostrar que todo subgrupo H , de orden 11, de un grupo G , de orden 99, es normal en G .
12. Mostrar que todo grupo no abeliano G , de orden 6, es isomorfo a \mathfrak{S}_3 .
13. Mostrar que todo grupo de orden p^2 , donde p es un número primo, posee un subgrupo normal de orden p .
14. Mostrar que en un grupo G , de orden p^2 , donde p es un número primo, todo subgrupo normal de orden p está contenido en $Z(G)$ y deducir de esto que todo grupo de orden p^2 es abeliano.
15. Dar las clases conjugadas en \mathfrak{S}_3 y encontrar, para cada σ , c_σ .
16. Dar las clases conjugadas en \mathfrak{S}_4 y encontrar, para cada σ , c_σ .
17. Dar $p(7)$, $p(8)$ y $p(9)$.

5.1. Aplicaciones a la Geometría y Teoría Musical

Los grupos de permutaciones sirven de modelo para representar grupos de operaciones geométricas, como rotaciones, reflexiones, etc., que actúan sobre elementos geométricos, como ejes cartesianos, polígonos y poliedros. En particular consideraremos movimientos geométricos que después de actuar sobre un determinado ente geométrico la posición de éste coincide con la posición original, que llamaremos movimientos de recubierta, ya que la imagen final recubre a la imagen inicial.

EJEMPLOS 5.9.

1. Consideremos el sistema coordenado cartesiano en el plano:

Los movimientos de recubrimiento, en este caso, son las rotaciones, alrededor del origen, en sentido de las agujas del reloj, en $\frac{\pi}{2}$, que llamaremos α , la reflexión β sobre el eje x y la reflexión γ sobre el eje y .

Como podemos observar la rotación α es de orden 4 y las dos reflexiones de orden 2. α puede ser identificada con el 4-ciclo $\alpha := \begin{pmatrix} x & -y & -x & y \end{pmatrix}$, la reflexión β la podemos identificar con la transposición $\beta := \begin{pmatrix} y & -y \end{pmatrix}$ y la reflexión γ , con la transposición $\gamma := \begin{pmatrix} x & -x \end{pmatrix}$. Cada una de estas operaciones generan subgrupos cíclicos del grupo total generado por las tres. Analicemos la

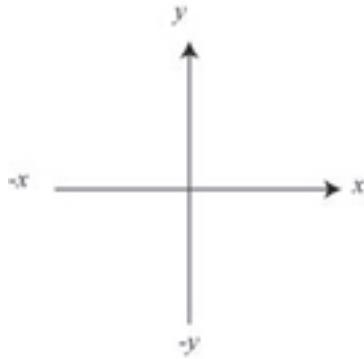


FIGURA 5.1. Plano xy

tabla de operaciones correspondiente

\circ	e	α	α^2	α^3	β	γ	$\alpha\beta$	$\alpha\gamma$
(5.10)	e	α	α^2	α^3	β	γ	$\alpha\beta$	$\alpha\gamma$
	α	α^2	α^3	e	$\alpha\beta$	$\alpha\gamma$	γ	β
	α^2	α^3	e	α	γ	β	$\alpha\gamma$	$\alpha\beta$
	α^3	α^3	e	α	α^2	$\alpha\gamma$	$\alpha\beta$	β
	β	β	$\alpha\gamma$	γ	$\alpha\beta$	e	α^2	α^3
	γ	γ	$\alpha\beta$	β	$\alpha\gamma$	α^2	e	β
	$\alpha\beta$	$\alpha\beta$	γ	$\alpha\gamma$	β	α	α^3	e
	$\alpha\gamma$	$\alpha\gamma$	γ	$\alpha\beta$	β	α^3	α	α^2

Notemos por $\hat{\mathcal{D}}_4$ al grupo generado por $\langle \alpha, \beta, \gamma \rangle$. Entonces $\hat{\mathcal{D}}_4$ es un subgrupo de \mathfrak{S}_4 de orden 8, que como veremos es isomorfo al grupo *diédrico* o *diedral*, \mathfrak{D}_r de todas las operaciones de recubrimiento del cuadrado. $\hat{\mathcal{D}}_4$ posee dos subgrupos de orden 4. Uno es el subgrupo cíclico $\langle \alpha \rangle$ de las rotaciones y el sugrupo $\hat{\mathfrak{V}}_4 := \{e, \alpha\gamma, \alpha\beta, \alpha^2\}$, que es isomorfo al grupo de los 4 de Klein. (ver ejercicio 5.0.9,6)). $\hat{\mathcal{D}}_4$ posee además 3 subgrupos de orden 2, generados respectivamente por β, γ y $\alpha^2 = \beta\gamma$.

2. Consideremos el sistema cartesiano 3-dimensional y las operaciones de recubrimiento consistentes en α, β, γ rotaciones, en sentido contrario a las agujas del reloj, al rededor de los ejes z, y, x , respectivamente, en π . En este caso podemos identificar estas rotaciones con las siguientes permutaciones

$$\alpha := \begin{pmatrix} x & -x \\ y & -y \end{pmatrix} \quad \beta := \begin{pmatrix} x & -x \\ z & -z \end{pmatrix} \quad \gamma := \begin{pmatrix} z & -z \\ y & -y \end{pmatrix}$$

y obtenemos la siguiente tabla de operaciones:

\circ	e	α	β	γ
(5.11)	e	α	β	γ
	α	α	e	β
	β	β	γ	e
	γ	γ	β	e

El subgrupo formado por $\{e, \alpha, \beta, \gamma\}$ es un subgrupo de \mathfrak{S}_6 isomorfo al grupo de los cuatro de Klein \mathfrak{V}_4 . Geométricamente, entonces, el grupo de Klein es

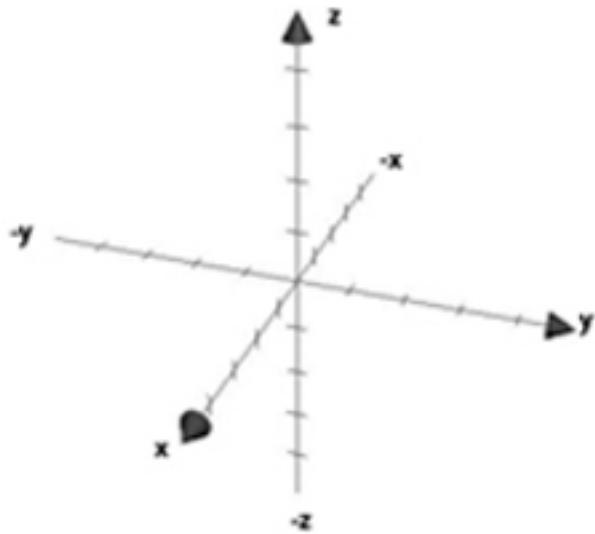


FIGURA 5.2. Sistema 3-dimensional

el grupo de las rotaciones, en π del sistema coordenado en tres dimensiones, alrededor de los ejes z , y , x , respectivamente.

3. El grupo de recubrimiento del triángulo equilátero. Consideremos el triángulo equilátero:

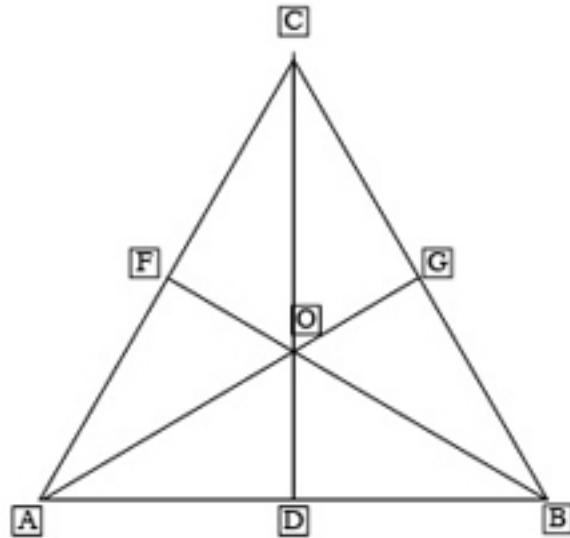


FIGURA 5.3. Triángulo equilátero

En el caso del triángulo equilátero tenemos las siguientes operaciones de recubrimiento: Las rotaciones alrededor de ‘O’ en $\frac{2\pi}{3}$, las reflexiones alrededor de los segmentos [CD],[BG] y [AF].

La rotación en $\frac{2\pi}{3}$ la podemos identificar con el 3-ciclo $\alpha := (A \ B \ C)$ y las reflexiones alrededor de los segmentos [CD],[BG],[AF] respectivamente con las transposiciones

$$\beta := (A \ B), \quad \gamma = (A \ C), \quad \tau := (B \ C)$$

y obtenemos la siguiente tabla de operaciones:

\circ	e	α	α^2	β	γ	τ
e	e	α	α^2	β	γ	τ
α	α	α^2	e	γ	τ	β
α^2	α^2	e	α	τ	β	γ
β	β	τ	γ	e	α^2	α
γ	γ	β	τ	α	e	α^2
τ	τ	γ	β	α^2	α	e

Este es un subgrupo de \mathfrak{S}_3 de orden 6 y por consiguiente es todo \mathfrak{S}_3 .

4. El grupo de recubrimiento del cuadrado. Consideremos el cuadrado:

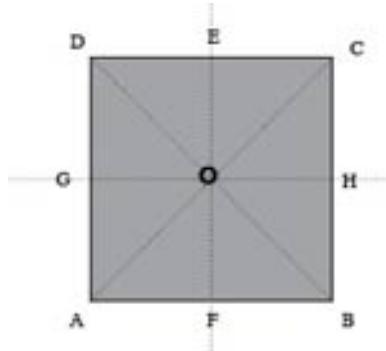


FIGURA 5.4. Cuadrado

En el caso del cuadrado tenemos las siguientes operaciones de recubrimiento: Las rotaciones alrededor de ‘O’ en $\frac{\pi}{2}$, la cual denotaremos por α , las reflexiones alrededor de las diagonales [AC] y [DB], las cuales denotaremos por β y γ respectivamente y las reflexiones alrededor de los segmentos [GH] y EF, las cuales denotaremos por σ y τ respectivamente.

Observemos que la rotación, en sentido contrario a las agujas del reloj, alrededor de ‘O’, en $\frac{\pi}{2}$ puede ser identificada con el 4-ciclo $\alpha := (A \ B \ C \ D)$, las reflexiones alrededor de las diagonales [AC],DB, respectivamente por las transposiciones:

$$\beta := (D \ B), \quad \gamma := (A \ C)$$

y las reflexiones alrededor de los segmentos [GH],[EF], con los productos de transposiciones:

$$\sigma := (A \ D)(B \ C), \quad \tau := (A \ B)(C \ D)$$

y obtenemos la siguiente tabla de operaciones:

\circ	e	α	α^2	α^3	β	γ	σ	τ
e	e	α	α^2	α^3	β	γ	σ	τ
α	α	α^2	α^3	e	τ	σ	β	γ
α^2	α^2	α^3	e	α	γ	β	τ	σ
α^3	α^3	e	α	α^2	σ	τ	γ	β
β	β	σ	γ	τ	e	α^2	α	α^3
γ	γ	τ	β	σ	α^2	e	α^3	α
σ	σ	γ	τ	β	α^3	α	e	α^2
τ	τ	β	σ	γ	α^2	α^3	α	e

Comparando esta tabla con la tabla (5.10), veremos que el grupo de todas las operaciones de recubrimiento del cuadrado no es más que el grupo diédrico o diedral $\mathfrak{D}_4 \subseteq \mathfrak{S}_4$, si en dicho cuadro identificamos σ con $\alpha\beta$ y τ con $\alpha\gamma$. El grupo de Klein $\mathfrak{V}_4 \subseteq \mathfrak{D}_4$ está dado por $\{\mathbf{e}, \alpha^2, \sigma, \tau\}$. Es decir que el grupo de los cuatro de Klein está formado por las reflexiones en π , alrededor del punto ‘O’ y las reflexiones alrededor de los segmentos [GH] y [EF]

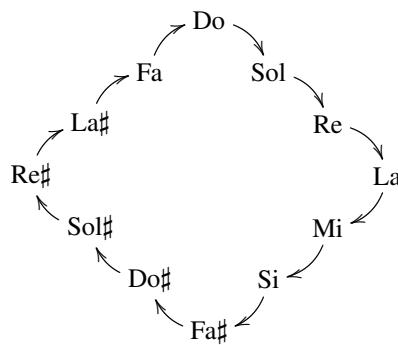
5. El siguiente ejemplo es de interés musical. La operación de asignarle a cada nota musical del conjunto de notas

$$\{\text{Do,Re,Mi,Fa,Sol,La,Si,Do\#,Re\#,Fa\#,Sol\#,La\#}\}$$

su quinta correspondiente, genera un grupo cíclico de orden 12 y puede ser representado por el 12-ciclo

$$\sigma := (\text{Do} \ Sol \ \text{Re} \ \text{La} \ \text{Mi} \ \text{Si} \ \text{Fa\#} \ \text{Do\#} \ \text{Sol\#} \ \text{Re\#} \ \text{La\#} \ \text{Fa\#})$$

perteneciente al grupo de simetría \mathfrak{S}_{12} , cuyo orden $\circ(\mathfrak{S}_{12}) = 12! = 479001600$. Por lo que las posibilidades de producir sonidos diferentes son, prácticamente, inagotables.



5.1.1. Ejercicios y Complementos.

1. Mostrar que los grupos $K(\mathfrak{A}_4)$, \mathfrak{V}_4 y $\hat{\mathfrak{V}}_4$ son isomorfos.
2. Mostrar que $\hat{\mathfrak{D}}_4$ es isomorfo a \mathfrak{D}_4 .
3. Mostrar que en \mathfrak{D}_4 , $K(\mathfrak{D}_4) = Z(\mathfrak{D}_4)$.
4. Mostrar que \mathfrak{D}_4 es un grupo transitivo de \mathfrak{S}_4 que contiene transposiciones.

5. Usar el ejercicio 5.0.9,5), para mostrar que \mathfrak{A}_4 no posee ningún subgrupo de orden 6, por lo que \mathfrak{A}_n puede también ser generado por un 3-ciclo de orden 3 y un elemento de orden 2, que en este caso es un producto de dos transposiciones..
6. Usar ejercicio precedente para mostrar que $\text{Aut}(\mathfrak{A}_4)$ posee como máximo $\circ(\mathfrak{S})_4 = 24$ elementos.
7. Dar la tabla de las operaciones de recubrimiento del tetraedro regular:

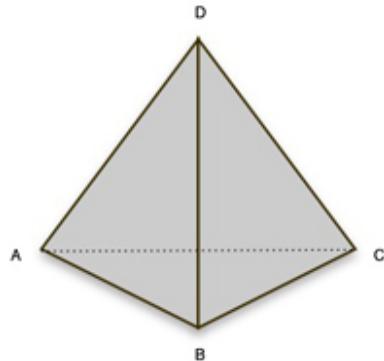


FIGURA 5.5. Tetraedro Regular

y describir el grupo correspondiente, generado por las rotaciones $\alpha, \beta, \gamma, \sigma$, en $\frac{2\pi}{3}$, alrededor de los ejes perpendiculares a las caras y pasando por los vértices A, B, C, D .

8. Mostrar que para $n \geq 3$, \mathfrak{S}_n es isomorfo al grupo $\mathcal{I}(\mathfrak{S}_n)$ de automorfismos internos.
9. Mostrar que para cualquier automorfismo interno, $\psi_\sigma : \mathfrak{S}_n \rightarrow \mathfrak{S}_n$, $\psi_\sigma[\mathfrak{A}_n] \subseteq \mathfrak{A}_n$. Mostrar que $\Phi : \mathcal{I}(\mathfrak{S}_n) \rightarrow \text{Aut}(\mathfrak{A}_n)$ definida por $\Phi(\psi_\sigma) := \psi_\sigma|_{\mathfrak{A}_n}$, es un homomorfismo inyectivo. Usar el resultado del ejercicio precedente para mostrar que $\Phi : \mathcal{I}(\mathfrak{S}_4) \rightarrow \text{Aut}(\mathfrak{A}_4)$ es un isomorfismo y por consiguiente $\text{Aut}(\mathfrak{A}_4)$ posee exactamente 24 elementos.
10. Dar tabla de las operaciones de recubrimiento del pentágono regular:

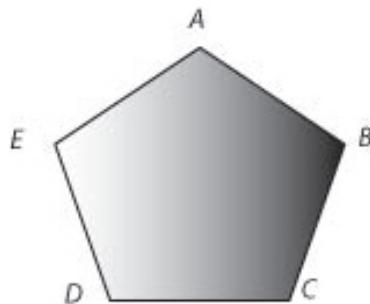


FIGURA 5.6. Pentágono Regular

11. Dar tabla de las operaciones de recubrimiento del hexágono regular:

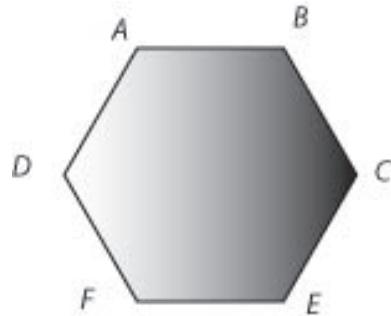


FIGURA 5.7. Hexágono Regular

12. Dar la tabla de las operaciones de recubrimiento del octaedro regular:

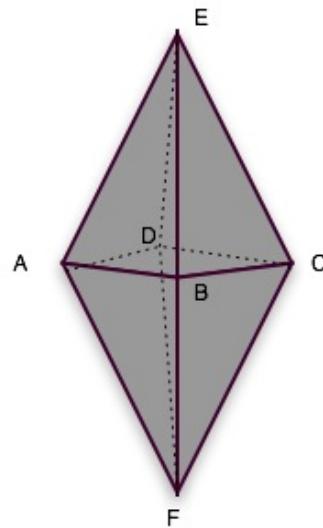


FIGURA 5.8. Octaedro Regular

Considerar que se tienen reflexiones que invierten la figura y que se ejecutan alrededor de las diagonales del cuadrado central y alrededor de rectas paralelas a los lados del cuadrado central que lo dividen por la mitad y rotaciones alrededor del eje perpendicular al centro del cuadrado central en $\frac{\pi}{2}$.

CAPÍTULO 6

TEOREMAS DE SYLOW, p -GRUPOS y GRUPOS SOLUBLES



FIGURA 6.1. Peter Ludwig Mejdell Sylow

En este capítulo estudiaremos grupos finitos, G y daremos algunos resultados concernientes a la existencia de subgrupos, cuyo orden sea un determinado divisor del orden de G . Por el teorema de Lagrange sabemos que el orden de cada subgrupo divide al orden de G . La pregunta, ahora, es, si dado un divisor m del orden de G , existe un subgrupo H de orden m . Veremos que en el caso abeliano la respuesta es positiva, mientras que en el caso general, deben cumplirse ciertas condiciones, las cuales son tratadas por los llamados teoremas de Sylow, en honor del matemático Noruego Peter Ludwig Mejdell Sylow.

Primero trataremos el caso abeliano, donde las demostraciones son bastante más sencillas que en el caso no abeliano.

6.1. Teoremas de Sylow

6.1.1. Caso Abeliano.

TEOREMA 6.1. *Sea G un grupo abeliano finito, de orden n . Si p es un número primo, tal que $p \mid n$, entonces G posee un subgrupo H de orden p .*

DEMOSTRACIÓN. Sea $n = pm$. Si G es cíclico, generado por un elemento g , entonces, como p es primo, $H := \langle g^m \rangle$ es un subgrupo de orden p y estamos listos. Sea, entonces, G un grupo abeliano no cíclico. Procederemos por inducción sobre m . Para $m = 1$, $n = p$ y no hay nada que mostrar, pues $H := G$ cumple con lo deseado. Supongamos, por hipótesis de inducción, que el teorema sea válido para todo grupo, cuyo orden sea menor que el orden de G y un múltiplo de p . Sea $g \in G$, $g \neq e$ y $N := \langle g \rangle$, entonces $N \neq G$ y $\circ(N) < \circ(G)$. Si $p \mid \circ(N)$, por hipótesis de inducción, estamos listos. Si $p \nmid \circ(N)$, entonces $p \mid i_G(N) = \circ(G/N) < \circ(G)$ y, por hipótesis de inducción, G/N posee un subgrupo de orden p el cual debe ser cíclico generado por una clase \bar{h} . Si $h \in G$ es un representante de \bar{h} y $\circ(h) = r$, entonces $(\bar{h})^r = \bar{e}$, por lo que $p \mid r$, entonces el grupo cíclico $H := \langle h \rangle$ posee un subgrupo de orden p . \square

Como corolario del teorema 6.1 se obtiene la siguiente generalización:

COROLARIO 6.2. *Si m es un divisor del orden del grupo abeliano finito G , entonces G posee un subgrupo de orden m .*

DEMOSTRACIÓN. Sea $n = mn_1$. Para $m = 1$, el subgrupo trivial cumple con lo deseado. Supongamos, por hipótesis de inducción, que el teorema sea válido para todo grupo de orden menor que n . Sea, entonces, $m > 1$ y p un primo, tal que $p \mid m$, entonces, por teorema 6.1, existe un subgrupo N de orden p y $\circ(G/N) = \frac{\circ(G)}{p} < \circ(G)$ y, por hipótesis de inducción, G/N posee un subgrupo \bar{H} de orden $\frac{m}{p}$, entonces $H := \pi^{-1}[\bar{H}]$, donde $\pi : G \rightarrow G/N$ es la proyección canónica, es un subgrupo de orden m de G . \square

También, como corolario del teorema 6.1, se obtiene, de forma inmediata, el llamado teorema de Cauchy para grupos abelianos:

COROLARIO 6.3 (Cauchy). *El grupo abeliano finito G posee un elemento de orden un número primo p Ssi $p \mid \circ(G)$.*

Como un caso particular del corolario 6.2, se obtiene el siguiente teorema de Sylow para grupos abelianos:

TEOREMA 6.4 (Teorema de Sylow para grupos abelianos). *Si G es un grupo abeliano de orden $\circ(G)$ y p un número primo, tal que $p^\alpha \mid \circ(G)$, pero $p^{\alpha+1} \nmid \circ(G)$, entonces G posee un subgrupo de orden p^α .*

El lector verificará fácilmente que si ponemos en el corolario 6.2, $m = p^\alpha$, se obtiene el teorema 6.4. Es más, obtenemos que G posee subgrupos de órdenes p, p^2, \dots, p^α . Sin embargo, más interesante es la siguiente versión más estricta del teorema de Sylow 6.4:

TEOREMA 6.5 (Sylow). *Si G es un grupo abeliano de orden $\circ(G)$ y p un número primo, tal que $p^\alpha \mid \circ(G)$, pero $p^{\alpha+1} \nmid \circ(G)$, entonces G posee un único subgrupo de orden p^α .*

DEMOSTRACIÓN. Supongamos que S, T son dos subgrupos de G de orden p^α . Como G abeliano, entonces ST es también, por teorema 4.12, subgrupo de G y aplicando ecuación (4.12) obtenemos:

$$(6.1) \quad \circ(ST) = \frac{\circ(S) \circ(T)}{\circ(S \cap T)} = \frac{p^\alpha p^\alpha}{\circ(S \cap T)}$$

como $S \neq T$, $\circ(S \cap T) < p^\alpha$, se obtiene de (6.1) que $\circ(ST) = p^\beta$, $\beta > \alpha$. Como $\circ(ST) \mid \circ(G)$, se tiene $p^\beta \mid \circ(G)$, en contradicción a la hipótesis de que $p^{\alpha+1} \nmid \circ(G)$. \square

El teorema 6.5, como veremos más adelante, no es válido en el caso no abeliano, como el lector comprobará fácilmente con el grupo \mathfrak{S}_3 . En efecto $\circ(\mathfrak{S}_3) = 6 = 2 \cdot 3$, pero \mathfrak{S}_3 posee tres subgrupos distintos de orden 2.

En el caso de grupos cíclicos finitos, se tiene la siguiente versión del corolario 6.2:

TEOREMA 6.6. *Sea G un grupo cíclico de orden $n := mq$. Entonces existe exactamente un único subgrupo H de G , de orden m e índice q . Si g es un generador de G , entonces $H = \langle g^q \rangle$. Viceversa, si G es un grupo finito de orden n y para cada divisor entero positivo m de n , existe, a lo sumo, un único subgrupo de orden m , en G , entonces G es cíclico.*

DEMOSTRACIÓN. En efecto, g^q genera un subgrupo H de G . Vamos a mostrar que $\circ(H) = m$. $(g^q)^m = g^n = e$, entonces $m \mid \circ(H)$. Por otra parte $(g^q)^{\circ(H)} = g^{q\circ(H)} = e$, entonces $n = mq \mid q \circ(H)$, de donde $m \mid \circ(H)$, por lo tanto $m = \circ(H)$.

Si H' es otro subgrupo de orden m , vamos a mostrar que $H' \subseteq H$, lo cual mostraría la igualdad. En efecto, como subgrupo de un grupo cíclico, H' es cíclico y sea $g^{q'}$ un generador de H' . Entonces $(g^{q'})^m = g^{q'm} = e$ y $qm = n \mid q'm$, lo que implica que $q \mid q'$. De aquí se deduce, entonces, que $q' = rq$, $r \in \mathbb{Z}^+$, por lo que $a^{q'} = a^{rq} = (a^q)^r \in H$. Por consiguiente $H' \subseteq H$.

Sea ahora G un grupo de orden n , y para cada divisor de n exista un único subgrupo de ese orden. Sean m_1, \dots, m_k los divisores de $\circ(G)$, ordenados ascendentemente, entonces $m_1 = 1$ y $m_k = n$. Para cada κ , $1 \leq \kappa \leq k$, sea N_κ el número de elementos de G que poseen exactamente el orden m_κ .

Si \tilde{G} es un grupo cíclico de orden n , consideremos \tilde{N}_κ el número de elementos de \tilde{G} de orden m_κ . Vamos a mostrar que $N_\kappa = \tilde{N}_\kappa$, $\forall \kappa$. En efecto:

$$(6.2) \quad n = \sum_{\kappa=1}^k N_\kappa = \sum_{\kappa=1}^k \tilde{N}_\kappa$$

Si g es un elemento de orden m_κ , sea $H := \langle g \rangle$, entonces, por hipótesis, todo elemento de orden m_κ está ya en H y generan a éste. Esto quiere decir, que N_κ es el número de elementos de orden m_κ en el grupo cíclico H . Como $m_\kappa \mid n = \circ(\tilde{G})$ y \tilde{G} es cíclico, existe un único subgrupo cíclico $\tilde{H} \subseteq \tilde{G}$ de orden m_κ , el cual es isomorfo a H . Entonces \tilde{G} posee, al menos, tantos elementos de orden m_κ como G , por lo que $N_\kappa \leq \tilde{N}_\kappa$. Por otra parte de la ecuación (6.2), resulta que $\forall \kappa$, $N_\kappa = \tilde{N}_\kappa$. Como, en particular, $N_k = \tilde{N}_k = n \neq 0$, resulta que G posee elementos de orden n . Por lo tanto G es cíclico. \square

Como consecuencia del teorema 6.6, se obtiene el siguiente

COROLARIO 6.7. *Si G es un grupo distinto del trivial y no posee ningún subgrupo propio distinto del trivial, entonces G es cíclico de orden primo.*

DEMOSTRACIÓN. Como $G \neq e$, existe $g \in G$, $g \neq e$ y, por hipótesis, $G = \langle g \rangle$, por lo que G es cíclico. G no puede ser infinito, ya que entonces sería isomorfo a \mathbb{Z} , el cual posee subgrupos propios. Entonces $\circ(G)$ debe ser finito. Si $\circ(G)$ no fuera primo, entonces, por el teorema 6.6, G tendría subgrupos propios no triviales, en contradicción a la hipótesis. \square

6.1.2. Caso General. Demostraremos ahora algunos resultados debidos a Sylow, para grupos en general, no necesariamente abelianos.

TEOREMA 6.8 (Sylow). *Sea G un grupo finito y p un número primo, tal que $p^m \mid \circ(G)$, entonces G posee un subgrupo H de orden p^m .*

DEMOSTRACIÓN. Para $m = 0$ no hay nada que demostrar. Sea entonces $m \geq 1$ y procedamos por inducción sobre el orden de G . Si $\circ(G) = p$, $H = G$ satisface lo deseado. Supongamos, por hipótesis de inducción, que el teorema vale para todo grupo de orden menor a $\circ(G)$. Si G es abeliano, entonces estamos listos. Sea, entonces, G no abeliano y $Z(G)$ su centro. Como G no es abeliano, $G \neq Z(G)$. Si $p \mid \circ(Z(G))$, entonces, como $Z(G)$ es abeliano, por teorema 6.1, $Z(G)$ posee un subgrupo N de orden p , el cual, como subgrupo de $Z(G)$ es normal en G y podemos formar $\tilde{G} := G/N$. Como $\circ(\tilde{G}) < \circ(G)$, \tilde{G} satisface la hipótesis de inducción. Ahora bien, $\circ(\tilde{G}) = \frac{\circ(G)}{p} = \frac{p^m n_1}{p} = p^{m-1} n_1$. Por consiguiente \tilde{G} posee un subgrupo \tilde{H} de orden p^{m-1} , entonces $H := \pi^{-1}[\tilde{H}]$, donde $\pi : G \rightarrow \tilde{G}$ es la proyección canónica, es un subgrupo de G de orden p^m .

En el caso en que $p \nmid \circ(Z(G))$, aplicando la ecuación de clase (4.22) a G :

$$\circ(G) = \circ(Z(G)) + \sum_{c_x > 1} c_x$$

resulta que debe existir al menos un $x \in G$, tal que $p \nmid c_x$. Si $N(x)$ es el normalizador de x , entonces $c_x = i_G(N(x))$. Como $p^m \mid \circ(G) = \circ(N(x))i_G(N(x))$ y $p \nmid i_G(N(x))$ resulta, entonces, que $p^m \mid \circ(N(x))$, como $G \neq N(x)$ y $\circ(N(x)) < \circ(G)$, $N(x)$ satisface la hipótesis de inducción y, por lo tanto, posee un subgrupo de orden p^m . \square

Al igual que en el caso abeliano, resulta, como corolario al teorema 6.8, el siguiente teorema de Cauchy:

TEOREMA 6.9 (Cauchy). *Un grupo finito G posee un elemento de orden un número primo p Ssi $p \mid \circ(G)$.*

DEFINICIÓN 6.1. Decimos que G es un p -grupo, donde p es un número primo, si el orden de cualquier elemento de G es una potencia de p .

Del teorema de Cauchy 6.9, se obtiene el siguiente

COROLARIO 6.10. *G es un p -grupo Ssi el orden de G es una potencia del número primo p .*

DEMOSTRACIÓN. En efecto, si $q \neq p$ fuese otro número primo, que divide al orden de G , entonces, por el teorema de Cauchy 6.9, G tendría un elemento de orden q , en contradicción a la hipótesis de que G es un p -grupo. \square

DEFINICIÓN 6.2. Sea p un número primo. Un subgrupo $H \subseteq G$ se llama un p -subgrupo de Sylow de G , si H es un p -grupo y cualquier otro p -grupo que contiene a H , coincide con H .

Si no hay confusión respecto de cual primo H es un p -subgrupo de Sylow, diremos simplemente que H es un subgrupo de Sylow.

El teorema 6.8, también lo podemos escribir de la siguiente forma

TEOREMA 6.11 (Sylow). *Si p es un número primo, tal que $p^m \mid \circ(G)$, pero $p^{m+1} \nmid \circ(G)$, entonces G contiene un p -subgrupo H de orden p^m , el cual es un p -subgrupo de Sylow.*

Obviamente H contiene subgrupos de órdenes p^μ , $\forall \mu \leq m$.

En forma análoga a como definimos la relación de conjugación para elementos de un grupo G , se puede definir la siguiente relación para subgrupos de G :

DEFINICIÓN 6.3. Decimos que dos subgrupos H, K , de un grupo G son *conjugados*, si existe $g \in G$, tal que $H = gKg^{-1}$.

El lector comprobará fácilmente que la relación de ser subgrupos conjugados es una relación de equivalencia sobre el conjunto de todos los subgrupos de G . Por $C(H)$, denotaremos la clase de conjugación del subgrupo H :

$$(6.3) \quad C(H) := \{gHg^{-1} \mid g \in G\}$$

y, en el caso en que $C(H)$ sea un conjunto finito, denotaremos por c_H el número de elementos de $C(H)$.

Dado un subgrupo H de G , $gHg^{-1} = H$ Ssi $g \in N(H)$, donde $N(H)$ es el normalizador de H .

El siguiente teorema nos da información sobre el número de elementos conjugados de un subgrupo H dado:

TEOREMA 6.12. *Sea H un subgrupo del grupo finito G . Entonces $c_H = i_G(N(H))$, donde $N(H)$ es el normalizador de H en G .*

DEMOSTRACIÓN. En efecto, $gHg^{-1} = xHx^{-1}$ Ssi $(x^{-1}g)H(g^{-1}x) = H$ Ssi $x^{-1}g \in N(H)$ Ssi $x \equiv g \pmod{N(H)}$. Por consiguiente existirán tantos elementos distintos en $C(H)$, como clases distintas $\pmod{N(H)}$. Por lo tanto $c_H = i_G(N(H))$. \square

El siguiente lema nos será útil para la demostración del teorema de Sylow enunciado más abajo.

LEMA 6.13. *Sean G un grupo y H, S subgrupos de G . Dados $x, y \in G$, entonces vale*

$$HxS = HyS \quad o \quad HxS \cap HyS = \emptyset$$

DEMOSTRACIÓN. En efecto, supongamos que existen $h \in H, g \in S$, tales que $hxg \in HxS \cap HyS$, entonces se tiene $HxS = (Hh)x(S) = H(hxg)S \subseteq H(HyS)S = (HH)y(S)S = HyS$, en forma similar se obtiene $HyS \subseteq HxS$, de donde $HxS = HyS$. \square

En el caso de los grupos abelianos, el teorema 6.5, nos dice que para un número primo dado p que divide al orden del grupo G , existe un único p -subgrupo de Sylow. Sin embargo en el caso general se tiene el siguiente

TEOREMA 6.14 (Sylow). *Sea G un grupo finito de orden $n := p^m q$, donde p es un número primo que no divide a q . Sea S un subgrupo de G de orden p^m . Entonces, si H es un p -subgrupo de G , H está contenido en un subgrupo conjugado de S . Es decir que existe $g \in G$, tal que $H \subseteq gSg^{-1}$.*

DEMOSTRACIÓN. En efecto, por el lema 6.13 existe un número minimal de elementos $x_1, \dots, x_n \in G$, tales que

$$G = \bigcup_{v=1}^n Hx_v S, \quad y \quad Hx_v S \cap Hx_\mu S = \emptyset, \text{ para } v \neq \mu, 1 \leq v, \mu \leq n$$

Sea q_v el número de clases laterales izquierdas, respecto de S , de los elementos de Hx_v , entonces se tiene la ecuación

$$(6.4) \quad q = i_G(S) = \sum_{v=1}^n q_v$$

Como $p \nmid q$, debe de existir, al menos un v , tal que $p \nmid q_v$. Esto quiere decir, que existe, al menos, un elemento x , tal que el número q_x de clases laterales de Hx en S no es divisible por p . Consideremos el homomorfismo $\phi_{x^{-1}} : HxS \rightarrow G$, definido por $\phi_{x^{-1}}(hxs) := hxsx^{-1} \in h(xSx^{-1})$, $\phi_{x^{-1}}$ es inyectivo y mapea HxS sobre $H(xSx^{-1})$, y la clase $(hx)S$ en la clase $h(xSx^{-1})$. Entonces H posee r clases distintas en xSx^{-1} .

Por el teorema 4.16 tenemos la ecuación

$$(6.5) \quad \circ(H(xSx^{-1})) = \frac{\circ(H) \circ (xSx^{-1})}{\circ(H \cap (xSx^{-1}))}$$

y para el número de clases de H en xSx^{-1} , $q_x = i_H(xSx^{-1})$, tenemos

$$(6.6) \quad q_x = \frac{\circ(H)}{\circ(H \cap (xSx^{-1}))}$$

Entonces, como divisor del orden del p -subgrupo H , q_x debe de ser 1, ya que $p \nmid q_x$. Esto significa, entonces, que $\circ(H) = \circ(H \cap (xSx^{-1}))$, lo que implica que $H \subseteq xSx^{-1}$. \square

Del teorema 6.14, se obtienen las siguientes consecuencias:

1. Todo p -subgrupo está contenido en un subgrupo de orden p^m .
2. Todos los p -subgrupos de Sylow son conjugados.
3. Si G es abeliano, el teorema 6.14 coincide con el teorema 6.5.

A continuación daremos un criterio de cómo determinar el número de posibles subgrupos de Sylow de un grupo finito G . Veremos que éste número debe ser un divisor de $\circ(G)$ y que va a depender del número primo p .

Mostremos primero el siguiente

LEMA 6.15. *Sea S un p -subgrupo de G y S_1, \dots, S_r los p -subgrupos distintos obtenidos de S por conjugación, tales que $S_\rho \neq S$, $\forall \rho = 1, \dots, r$. Entonces la relación \sim , definida por $S_v \sim S_\mu$ si existe $g \in S$, tal que $S_v = gSg^{-1}$ es una relación de equivalencia sobre el conjunto*

$$\tilde{C}(S) := \{S_1, \dots, S_r\}$$

Por otra parte, dados $g, h \in S$, $gS_\rho g^{-1} = hS_\rho h^{-1}$ si $g \equiv h$, (mód $N(S_\rho) \cap S$), donde $N(S_\rho)$ es el normalizador de S_ρ . Entonces, el número \tilde{c}_ρ de elementos en cada clase $[S_\rho]$, respecto de la relación \sim , es el índice en S de $N(S_\rho) \cap S$.

DEMOSTRACIÓN. El lector comprobará fácilmente que \sim es una relación de equivalencia en el conjunto de todos los subgrupos de G . Falta mostrar que \sim es una relación de equivalencia sobre $\tilde{C}(S)$. En efecto si S_ρ es un p -subgrupo de Sylow, también lo será $gS_\rho g^{-1}$, $\forall g \in S$. Debemos entonces mostrar que $S \neq gS_\rho g^{-1}$, $\forall g \in S$. En efecto si para algún ρ , $S = gS_\rho g^{-1}$, $g \in S$, tendríamos $S_\rho = g^{-1}Sg = S \notin \tilde{C}(S)$. Por consiguiente \sim es una relación de equivalencia sobre $\tilde{C}(S)$.

Del teorema 6.12, sabemos que si $gS_\rho g^{-1} = hS_\rho h^{-1}$, $g \equiv h$, (mód $N(S_\rho)$). Como $g, h \in S$, se tiene, entonces, que $g \equiv h$, (mód $N(S_\rho) \cap S$). Entonces existirán tantos elementos distintos en la clase $[S_\rho]$, como elementos tenga $S/(N(S_\rho) \cap S)$, es decir $\tilde{c}_\rho = i_S(N(S_\rho) \cap S)$. \square

TEOREMA 6.16 (Sylow). *El número de subgrupos de Sylow de un grupo finito G es un divisor de $\circ(G)$ y de la forma particular $1 + mp$, donde m es un entero mayor o igual a 0.*

DEMOSTRACIÓN. Si G posee un único subgrupo de Sylow, no hay nada que mostrar, pues $m = 0$ cumple la condición. Supongamos, entonces, que S, S_1, \dots, S_r sean los subgrupos de Sylow de G . Como, por teorema 6.14, éstos son conjugados, resulta del teorema 6.12, que el número de éstos es el índice, en G , del normalizador de S , es decir $1 + r = i_G(N(S))$. Entonces $(1 + r) \mid \circ(G)$. Vamos a mostrar que $p \mid r$.

Por el lema 6.15

$$r = \sum_{[S_\rho]} \tilde{c}_\rho \quad \text{ya que} \quad \tilde{C}(S) = \bigcup_{\rho} [S_\rho]$$

Si mostramos que $\forall \rho, p \mid \tilde{c}_\rho$, entonces habremos mostrado que $p \mid r$. En efecto, nuevamente por lema 6.15, $\tilde{c}_\rho = i_S(N(S_\rho) \cap S)$, el cual es un divisor de $\circ(S)$. Si mostramos que $\tilde{c}_\rho \neq 1$, $\forall \rho$, entonces debe valer que $p \mid \tilde{c}_\rho$ y estamos listos.

En efecto, $\forall \rho, S_\rho$ es normal en $N(S_\rho)$, por lo que S_ρ es el único p -subgrupo de Sylow de $N(S_\rho)$. Si $i_S(N(S_\rho) \cap S) = 1$, entonces tendríamos que $S = N(S_\rho) \cap S$ y S sería también un p -subgrupo de Sylow de $N(S_\rho)$, distinto de S_ρ . Lo cual no puede ser. Por consiguiente $p \mid r$ y existe un entero positivo m , tal que $r = mp$. \square

Como una consecuencia de los teoremas de Sylow y del teorema 6.6 se obtiene el siguiente

COROLARIO 6.17. *Sean p, q dos números primos $q < p$. Si G es un grupo de orden $n := p \cdot q$, entonces G posee un único p -subgrupo de Sylow de orden p , el cual es normal en G . Por otra parte, si q no divide a $(p-1)$, entonces G posee también un único q -subgrupo de Sylow de orden q , el cual es también normal y en este caso G es un grupo cíclico y por consiguiente abeliano.*

DEMOSTRACIÓN. En efecto, por teorema 6.16, el número de p -subgrupos de Sylow es de la forma $1+mp$ y $1+mp \mid p \cdot q$, lo que implica que $1+mp \mid q$. Como, por hipótesis, $q < p$, resulta que la única posibilidad es $m = 0$, por lo que únicamente existe un p -subgrupo de Sylow de orden p , el cual, por teorema 6.14, debe ser normal en G . Si $q \nmid (p-1)$, entonces, el número de q -subgrupos de Sylow es, por 6.16, de la forma $1+mq$ y debe dividir a p , lo cual sólo es posible si $q \mid (p-1)$ o $m = 0$. Como, por hipótesis, $q \nmid (p-1)$, debe valer $m = 0$ y G posee entonces un único q -subgrupo de Sylow de orden q , el cual, nuevamente por teorema 6.14, es normal. Del teorema 6.6, resulta ahora, que G es un grupo cíclico. \square

Vamos a dar un procedimiento para encontrar, primeramente, un subgrupo de Sylow del grupo \mathfrak{S}_{p^k} , para un número primo p . Para ésto determinaremos primero cuál es la potencia $n(k)$ más grande de p que divide a $(p^k)!$.

LEMA 6.18. *Dado un número primo p , entonces la potencia más grande de p que divide a $(p^k)!$ viene dada por*

$$(6.7) \quad n(k) = \sum_{\kappa=0}^{k-1} p^\kappa$$

DEMOSTRACIÓN. Si $k = 1$, es claro que $p \mid p!$, pero $p^2 \nmid p!$, por lo que $k(1) = 1$ y satisface la ecuación (6.7). En $(p^k)!$ los términos que contribuyen a que una potencia de p lo dividan son únicamente los múltiplos de p . Entonces $n(k)$ debe ser la potencia de p que divida a

$$(6.8) \quad p(2p)(3p) \cdots p^{k-1}p = p^{p^{k-1}}(p^{k-1})!$$

Entonces de (6.8), resulta que $p^{n(k)} \mid p^{p^{k-1}}(p^{k-1})!$. Pero la potencia máxima de p que divide a $(p^{k-1})!$ es $n(k-1)$. Por consiguiente tenemos la siguiente fórmula recursiva para $n(k)$:

$$(6.9) \quad n(k) = p^{k-1} + n(k-1)$$

la cual nos lleva a

$$\begin{aligned} n(k) - n(k-1) &= p^{k-1} \\ n(k-1) - n(k-2) &= p^{k-2} \\ &\vdots \\ n(2) - n(1) &= p \\ n(1) &= 1 \end{aligned}$$

Sumando se obtiene entonces (6.7). \square

EJEMPLO 6.1. Sea $p = 3$, entonces la potencia máxima de $p = 3$ que divide al orden de \mathfrak{S}_9 , considerando que $9 = 3^2$, $k = 2$ es

$$n(2) = 1 + 3 = 4$$

o sea que el orden de los 3-subgrupos de Sylow de \mathfrak{S}_9 es $3^4 = 81$.

A continuación describiremos un proceso inductivo para construir un p -subgrupo de Sylow de \mathfrak{S}_{p^k} a partir de un p -subgrupo de Sylow de $\mathfrak{S}_{p^{k-1}}$. Por los teoremas de Sylow sabemos que \mathfrak{S}_{p^k} debe poseer un p -subgrupo de Sylow de orden $p^{n(k)}$ y $\mathfrak{S}_{p^{k-1}}$ un subgrupo de Sylow de orden $p^{n(k-1)}$. Notemos que

$$(6.10) \quad pn(k-1) + 1 = p \sum_{\kappa=0}^{k-2} p^\kappa + 1 = \sum_{\kappa=0}^{k-1} p^\kappa = n(k)$$

entonces a partir de un subgrupo de orden $p^{n(k-1)}$ vamos a construir un grupo de orden $p^{n(k)}$. Primeramente dividamos los elementos del conjunto

$$S_{p^k} := \{1, 2, \dots, p^k\}$$

en p conjuntos disjuntos:

$$\{1, 2, \dots, p^{k-1}\}, \{p^{k-1} + 1, \dots, 2p^{k-1}\}, \dots, \{(p-1)p^{k-1}, \dots, p^k\}$$

y definamos la permutación

$$\begin{aligned} \sigma := & \left(\begin{array}{cccccc} 1 & p^{k-1} + 1 & 2p^{k-1} + 1 & \cdots & (p-1)p^{k-1} + 1 \end{array} \right) \cdots \\ & \left(\begin{array}{cccccc} j & p^{k-1} + j & 2p^{k-1} + j & \cdots & (p-1)p^{k-1} + j \end{array} \right) \cdots \\ & \left(\begin{array}{cccccc} p^{k-1} & 2p^{k-1} & \cdots & (p-1)p^{k-1} & p^k \end{array} \right) \end{aligned}$$

Como σ es producto de ciclos disjuntos de orden p , es también de orden p y $\sigma^p = e$. Dada una permutación τ que deja fijos todos los elementos $i > p^{k-1}$, es decir que sólo afecta a los elementos del conjunto

$$\{1, 2, \dots, p^{k-1}\}$$

entonces $\sigma\tau\sigma^{-1}$ sólo mueve a los elementos de

$$\{p^{k-1} + 1, \dots, 2p^{k-1}\}$$

y $\sigma^j\tau\sigma^{-j}$ sólo mueve a los elementos de

$$\{jp^{k-1} + 1, \dots, (j+1)p^{k-1}\}$$

Si

$$A := \{\tau \in \mathfrak{S}_{p^k} \mid \tau(i) = i, \forall i > p^{k-1}\}$$

Entonces A es un subgrupo de \mathfrak{S}_{p^k} y es isomorfo a $\mathfrak{S}_{p^{k-1}}$. Sea \tilde{S}_1 un subgrupo de Sylow de A de orden $p^{n(k-1)}$ y formemos el grupo

$$T := \tilde{S}_1\sigma\tilde{S}_1\sigma^{-1}\sigma^2\tilde{S}_1\sigma^{-2}\cdots\sigma^{(p-1)}\tilde{S}_1\sigma^{-(p-1)} =: \tilde{S}_1\cdots\tilde{S}_p$$

Como cada \tilde{S}_j , $1 \leq j \leq p$ actúa sobre conjuntos disjuntos, el producto de todos ellos commuta y T es un subgrupo de \mathfrak{S}_{p^k} . Por otra parte $\tilde{S}_i \cap \tilde{S}_j = \{e\}$ si $i \neq j$ y $\circ(T) = \circ(\tilde{S}_1)^p = p^{pn(k-1)}$. Como $\sigma \notin T$ y $\sigma T \sigma^{-1} = T$, el grupo cíclico $\langle\sigma\rangle$ commuta con T y $S := \langle\sigma\rangle T$ es un subgrupo de \mathfrak{S}_{p^k} de orden $p \circ(T) = pp^{pn(k-1)} = p^{pn(k-1)+1} = p^{n(k)}$. Por lo tanto S es un subgrupo de Sylow de \mathfrak{S}_{p^k} . ([12]).

EJEMPLOS 6.2.

- Tomemos como ejemplo un grupo G de orden $n := 6 = 2 \cdot 3$. ¿Cuáles son las posibilidades para los 2-Subgrupos de Sylow y los 3-subgrupos de Sylow? Por el teorema 6.16, sabemos que el número de los p -subgrupos de Sylow posible es un divisor del orden de G y de la forma $1 + mp$, $m \in \mathbb{N}$. Entonces para el caso de $p = 2$, el número posible es de la forma $1 + 2m$, donde $1 + 2m \mid 3$ y en el caso de $p = 3$, de la forma $1 + 3m$, donde $1 + 3m \mid 2$. Para el caso $p = 3$, la única posibilidad es $m = 0$, por lo que sólo existe un único 3-subgrupo de Sylow S_3 , de orden 3, el cual debe ser normal por ser único. Para $p = 2$, se tienen dos posibilidades $m = 0$ y $m = 1$, lo que nos da que podrían haber 3 2-subgrupos de Sylow o un único 2-subgrupo de Sylow. El lector comprobará que la unicidad del 2-subgrupo de Sylow se da si G es abeliano. Como vimos en el ejercicio 5.0.9,12), Si G no es abeliano es isomorfo a \mathfrak{S}_3 y posee 3 2-subgrupos de Sylow, cada uno generado por las únicas tres transposiciones existentes en este grupo.

2. Sea G un grupo de orden $11^2 \cdot 13^2$. Vamos a analizar cuáles podrían ser sus 11-subgrupos de Sylow y sus 13-subgrupos de Sylow. El número de los 11-subgrupos de Sylow es de la forma $1 + 11m$ y debe dividir a $\circ(G) = 11^2 \cdot 13^2$, como $1 + 11m \nmid 11^2$ debe valer entonces que $1 + 11m \mid 13^2$, lo cual es posible sólo si $m = 0$, por lo que sólo existe un único 11-subgrupo de Sylow que lo designaremos por \tilde{S}_{11} y éste debe ser normal, por ser único. De forma análoga, el número de los 13-subgrupos de Sylow es de la forma $1 + 13m$, el cual debe dividir a 11^2 , lo cual sólo es posible si $m = 0$, por lo que también sólo existe un único 13-subgrupo de Sylow, \tilde{S}_{13} , el cual también es normal.

Como el orden de \tilde{S}_{11} y de \tilde{S}_{13} es el cuadrado de un número primo, éstos son subgrupos abelianos de G . $\tilde{S}_{11} \cap \tilde{S}_{13} = \{e\}$ y por la normalidad $\tilde{S}_{11}\tilde{S}_{13} = \tilde{S}_{13}\tilde{S}_{11} = G$, ya que $\circ(\tilde{S}_{11}\tilde{S}_{13}) = \circ(\tilde{S}_{11}) \cdot \circ(\tilde{S}_{13}) = 11^2 \cdot 13^2 = \circ(G)$. Entonces G es el producto de dos subgrupos normales abelianos y disjuntos. G es abeliano: En efecto consideremos el conmutador $ghg^{-1}h^{-1}$, $g \in \tilde{S}_{11}$, $h \in \tilde{S}_{13}$. $ghg^{-1}h^{-1} = g(hg^{-1}h^{-1}) \in \tilde{S}_{11}$, ya que \tilde{S}_{11} es normal. Por otra parte, considerando la normalidad de \tilde{S}_{13} , $ghg^{-1}h^{-1} = (ghg^{-1})h^{-1} \in \tilde{S}_{13}$ y como $\tilde{S}_{11} \cap \tilde{S}_{13} = \{e\}$, debe valer que $ghg^{-1}h^{-1} = e$, lo que implica que G es abeliano. Entonces todo grupo de orden $11^2 \cdot 13^2$ es abeliano.

3. Sea G un grupo de orden $72 = 2^3 \cdot 3^2$. El número de 3-subgrupos de Sylow es de la forma $1 + 3m$ y debe dividir a $2^3 = 8$, lo cual sólo vale si $m = 0$ o si $m = 1$, por lo que G puede poseer uno o cuatro 3-subgrupos de Sylow. En el primer caso el 3-subgrupo de Sylow debe ser normal y G no es simple. En el segundo caso, vimos que el número de 3-subgrupos de Sylow es el índice del normalizador $N(\tilde{S}_3)$, donde \tilde{S}_3 es un 3-subgrupo de Sylow. Como $i_G(N(\tilde{S}_3)) = 4$ y $72 = \circ(G) \nmid 4!$, por corolario 5.30, $N(\tilde{S}_3)$ debe poseer un subgrupo, normal en G , no trivial. Por consiguiente todo grupo de orden 72 no es simple.
4. Vamos a construir un 2-subgrupo de Sylow de $\mathfrak{S}_4 = \mathfrak{S}_{2^2}$, usando el procedimiento arriba indicado. Nuestro conjunto

$$S_4 := \{1, 2, 3, 4\}$$

lo dividimos en

$$\{1, 2\} \quad \{3, 4\}$$

entonces

$$\sigma := \begin{pmatrix} 1 & 3 \\ 2 & 4 \end{pmatrix}$$

Sean

$$\tilde{S}_1 := \langle \begin{pmatrix} 1 & 2 \end{pmatrix} \rangle \quad \tilde{S}_2 := \sigma \tilde{S}_1 \sigma^{-1} = \langle \begin{pmatrix} 3 & 4 \end{pmatrix} \rangle$$

entonces

$$T := \tilde{S}_1 \tilde{S}_2 = \{e, \begin{pmatrix} 1 & 2 \end{pmatrix}, \begin{pmatrix} 3 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 2 \end{pmatrix} \begin{pmatrix} 3 & 4 \end{pmatrix}\}$$

Entonces nuestro 2-subgrupo de Sylow, es el subgrupo de orden 8 dado por

$$\langle \sigma \rangle T$$

Dado un número $x \in \mathbb{R}^+$, definimos $[x]$ como el mayor entero positivo m , tal que $m \leq [x] < m + 1$. Así, por ejemplo, si $x = 3.457 \dots$, $[x] = 3$, si $x = 0.324$, $[x] = 0$. Dado un entero n y un número primo $p \leq n$ queremos determinar cuál sería la máxima potencia $\alpha(n)$ de p , tal que $p^{\alpha(n)} \mid n!$. La respuesta nos la da el siguiente

TEOREMA 6.19. *Dado un número entero n y un número primo $p \leq n$, entonces la máxima potencia $\alpha(n)$ de p que divide a $n!$, viene dada por*

$$(6.11) \quad \alpha(n) = \sum_{k=1}^k \left[\frac{n}{p^k} \right]$$

donde k es tal que $p^k \leq n < p^{k+1}$

DEMOSTRACIÓN. La demostración es similar a la del lema 6.18. El lector comprobará fácilmente que (6.11) se satisface para $n = 2$ y $n = 3$. Sea $n > 3$ y supongamos, por hipótesis de inducción que (6.11) vale para todo entero positivo $m < n$. Si p es un número primo, tal que $p \leq n$, entonces el número de factores de p que aparecen en $n!$

es $\left[\frac{n}{p} \right]$.

$$n! = 1 \cdot 2 \cdots p \cdots 2p \cdots \left[\frac{n}{p} \right] \cdots n$$

entonces $p^{\alpha(n)}$ debe dividir a

$$p \cdots 2p \cdots \left[\frac{n}{p} \right] = p^{\left[\frac{n}{p} \right]} \left[\frac{n}{p} \right]!$$

como $\left[\frac{n}{p} \right] < n$, por hipótesis de inducción

$$\alpha\left(\left[\frac{n}{p} \right]\right) = \sum_{k=1}^{k-1} \left[\frac{n}{p^{k+1}} \right]$$

□

entonces

$$\alpha(n) = \left[\frac{n}{p} \right] + \sum_{k=1}^{k-1} \left[\frac{n}{p^{k+1}} \right]$$

que no es otra cosa que (6.11).

6.1.3. Ejercicios y Complementos.

1. Si S_p, \tilde{S}_p son dos p -subgrupos de Sylow de un grupo G , Mostrar que sus normalizadores correspondientes son conjugados.
2. Mostrar que todo grupo de orden 15 posee un único 3-subgrupo de Sylow de orden 3 y un único 5-subgrupo de Sylow de orden 5. Deducir de ésto que todo grupo de orden 15 es cíclico y por consiguiente abeliano.
3. Mostrar que todo grupo de orden 77 es cíclico.
4. Sean p, q dos números primos y G un grupo de orden $p \cdot q^2$. Mostrar
 - a) Si $p > q^2$, entonces el p -subgrupo de Sylow de G es normal en G .
 - b) Si $q > p$, entonces el q -subgrupo de Sylow de G es normal en G .
 - c) Si $p > q$, pero $p < q^2$, entonces uno de sus subgrupos de Sylow debe ser normal en G
5. Sea G un grupo de orden 18, 20, 28, 42, 44, 50, 52 o 54. Mostrar que si p es el mayor primo que divide al orden de G , entonces el p -subgrupo de Sylow es normal en G .
6. Mostrar que en todo grupo de orden 40 o 45 el 5-subgrupo de Sylow es normal.
7. Analizar qué posibilidades existen para un grupo de orden $3^2 \cdot 5^2$.

8. Mostrar que si G es un grupo de orden 56, entonces uno de sus subgrupos de Sylow debe ser normal en G .
9. Sea G un grupo de orden 36. Mostrar que G posee un 3-subgrupo (no necesariamente de Sylow) normal, no trivial. (Ver corolario 5.30).
10. Sea G un grupo de orden $2^m \cdot 3$, $m \geq 2$. Mostrar que G posee un 2-subgrupo normal, no trivial (no necesariamente de Sylow). (Ver corolario 5.30).
11. Sea G un grupo de orden $n = 30$.
 - a) Mostrar que todos los subgrupos de Sylow son cíclicos y por consiguiente abelianos
 - b) Describir las diferentes posibilidades que podrían darse para los 2-subgrupos, 3-subgrupos y 5-subgrupos de Sylow.
 - c) Mostrar que en el caso de que exista un único 2-subgrupo de Sylow, entonces existen subgrupos H_{10} y H_6 de orden 10 y de orden 6, respectivamente.
 - d) Bajo las mismas condiciones que en el inciso precedente, mostrar que H_{10} contiene un 5-subgrupo de Sylow, S_5 , de G y que éste es normal en H_{10} . Deducir de esto, que el normalizador de S_5 debe contener a H_{10} y que, por consiguiente, S_5 es normal en G .
 - e) Mostrar que si S_5 es normal, entonces existe un subgrupo H_{15} de orden 15, el cual es cíclico y normal en G .
 - f) Mostrar que si G posee un subgrupo de orden 15, entonces existe un único 3-subgrupo de Sylow S_3 y por consiguiente S_3 es normal en G . (Usar fórmula (4.12)).
 - g) En el caso en que G posee tres 2-subgrupos de Sylow, mostrar que el normalizador de éstos es un subgrupo de orden 10 y contiene un único 5-subgrupo de Sylow el cual debe ser normal en G y por consiguiente G posee un subgrupo normal de orden 15. Deducir que también G posee un único 3-subgrupo de Sylow, el cual es normal en G .
 - h) Mostrar que en el caso en que G posee cinco 2-subgrupos de Sylow, entonces existe un único 3-subgrupo de Sylow, el cual debe ser normal y deducir que también en este caso existe un subgrupo normal de orden 15 y que, por consiguiente, debe existir un único 5-subgrupo de Sylow normal en G .
 - i) Mostrar que en el caso en que G posee quince 2-subgrupos de Sylow, si S_3 o S_5 no fueran normales, existirían más de treinta elementos distintos en G . Concluir que tanto S_3 , como S_5 deben ser normales en G .
 - j) De lo anteriormente expuesto deducir que en todo grupo de orden 30, los 5-subgrupos y los 3-subgrupos de Sylow son siempre normales y únicos.
12. Usar los resultados obtenidos en los ejercicios precedentes para mostrar que todo grupo simple de orden ≤ 59 es cíclico de orden primo. (Listar los números del 1 al 59, dar su descomposición primaria y aplicar los resultados de los ejercicios precedentes y el corolario 5.30. Tener en cuenta también que todo grupo de orden p^2 , donde p es un número primo es abeliano y que todo subgrupo de índice 2 es normal). Esto quiere decir, en particular, que todo grupo no abeliano de orden ≤ 59 no es simple y que posee, al menos un subgrupo normal, no trivial, tal que $\circ(N) < \circ(G)$ y $\circ(G/N) < \circ(G)$.
13. Sea G un grupo no abeliano, de orden p^3 , donde p es un número primo. (Usar como ilustración el ejercicio 5.1.1,3).
 - a) Mostrar que el centro $Z(G)$ es un subgrupo propio de G , no trivial.
 - b) Mostrar que el grupo $K(G)$ de comutadores de G no es trivial.

- c) Mostrar que el grupo $G/Z(G)$ debe ser un grupo abeliano.
 - d) Deducir de c) que $K(G) \subseteq Z(G)$, por lo que $K(G) \neq G$ y $K(G)$ es abeliano.
 - e) Si $g, h \in G$ son dos elementos, tales que $gh \neq hg$, mostrar que sus normalizadores $N(g), N(h)$ son distintos.
 - f) Deducir del hecho que $Z(G) \subseteq N(g), \forall g \in G$, que $\circ(Z(G)) < \circ(N(g)) < \circ(G)$.
 - g) Concluir de lo mostrado en los incisos precedentes que $\circ(Z(G)) = p$ y por consiguiente $K(G) = Z(G)$.
14. Si G es un grupo abeliano que posee elementos de órdenes m y n respectivamente, mostrar que G posee un elemento, cuyo orden es el mínimo común múltiplo de m y n .
15. Si G es un grupo abeliano que posee subgrupos de órdenes m y n respectivamente, mostrar que G posee un subgrupo, cuyo orden es el mínimo común múltiplo de m y n .

6.2. Grupos Solubles

Sea G un grupo. Por $K(G)$ denotaremos el subgrupo de comutadores de G . Dado $n \in \mathbb{Z}^+$, definimos, de forma inductiva, $K_n(G) := K(K_{n-1}(G))$, donde $K_1(G) := K(G)$.

DEFINICIÓN 6.4. Decimos que el grupo G es *soluble*, si existe un entero $m \geq 1$, tal que $K_m(G) = \{e\}$.

EJEMPLOS 6.3.

1. Todo grupo abeliano es soluble, ya que $K(G) = \{e\}$.
2. Para $n \leq 3$, el grupo \mathfrak{S}_n es soluble, ya que $K(\mathfrak{S}_n) = \mathfrak{A}_n$, el cual es abeliano si $n \leq 3$. Por consiguiente, si $n \leq 3$, $K_2(\mathfrak{S}_n) = K(\mathfrak{A}_n) = \{e\}$.
3. El grupo \mathfrak{S}_4 es soluble, ya que $K(\mathfrak{A}_4) = \mathfrak{B}_4$, el grupo de los cuatro de Klein, el cual es abeliano por ser de orden 4.
4. Para $n \geq 5$, \mathfrak{A}_n no es abeliano y por teorema 5.24, es simple, por lo que no contiene ningún subgrupo normal propio no trivial. Entonces $K_m(\mathfrak{A}_n) = \mathfrak{A}_n \neq \{e\}$, $\forall m \in \mathbb{Z}^+$.

A continuación mostraremos una serie de propiedades de los grupos solubles.

LEMA 6.20. Si $\psi : H \rightarrow G$ es un homomorfismo de grupos, entonces $\psi[K(H)] \subseteq K(G)$ y $\psi|_{K(H)} : K(H) \rightarrow K(G)$.

DEMOSTRACIÓN. En efecto, si $ghg^{-1}h^{-1}$ es un comutador en H , $\psi(ghg^{-1}h^{-1}) = \psi(g)\psi(h)\psi(g^{-1})\psi(h^{-1}) = \psi(g)\psi(h)\psi(g)^{-1}\psi(h)^{-1} \in K(G)$. Por consiguiente $\psi[K(H)] \subseteq K(G)$. \square

Por aplicaciones sucesivas del lema 6.20, se obtiene el siguiente

COROLARIO 6.21. Todo homomorfismo de grupos $\psi : H \rightarrow G$, induce $\forall m \in \mathbb{Z}^+$ un homomorfismo $\psi|_{K^m(H)} : K_m(H) \rightarrow K_m(G)$.

TEOREMA 6.22. Todo subgrupo de un grupo soluble es soluble.

DEMOSTRACIÓN. En efecto, sea H un subgrupo del grupo soluble G . Consideremos la inclusión $\iota : H \rightarrow G$, donde $\iota(h) := h \in G, \forall h \in H$. ι es un homomorfismo de grupos y, por corolario 6.21, $K_m(H) = \iota[K_m(H)] \subseteq K_m(G)$. Por consiguiente, si G es soluble también lo será H . \square

Como consecuencia del teorema 6.22 se obtiene el siguiente

COROLARIO 6.23. *Si G es un grupo soluble, entonces existe un homomorfismo de todo subgrupo no trivial de G en un grupo abeliano.*

DEMOSTRACIÓN. En efecto, si G es soluble y $H \subseteq G$ es un subgrupo no trivial de G , entonces, por teorema 6.22, H es soluble y $K(H) \neq H$, entonces

$$\pi : H \rightarrow H/K(H)$$

es un homomorfismo de H en el grupo abeliano $H/K(H)$. \square

TEOREMA 6.24. *Si $\varphi : G \rightarrow H$ es un homomorfismo sobreyectivo del grupo soluble G sobre H , entonces H es soluble.*

DEMOSTRACIÓN. En efecto, por lema 6.20, $\varphi[K^m(G)] \subseteq K^m(H)$. Vamos a mostrar que si φ es sobreyectiva, entonces $K^m(H) \subseteq \varphi[K^m(G)]$. Como φ es sobreyectiva, dados $h_1, h_2 \in H$, existen $g_1, g_2 \in G$, tales que $\varphi(g_1) = h_1$ y $\varphi(g_2) = h_2$, entonces $[h_1, h_2] = [\varphi(g_1), \varphi(g_2)] = \varphi([g_1, g_2])$ y $\varphi[K(G)] = K(H)$. Entonces, siguiendo un proceso inductivo, resulta que $\varphi[K^m(G)] = K^m(H)$. Por consiguiente si G es soluble H es soluble. \square

Del teorema 6.24 se obtiene el siguiente

COROLARIO 6.25. *Si N es un subgrupo normal del grupo soluble G , entonces G/N es soluble.*

El siguiente teorema es una especie de inverso del corolario 6.25:

TEOREMA 6.26. *Si N es un subgrupo normal y soluble de G y G/N soluble, entonces G es soluble.*

DEMOSTRACIÓN. Sea $m \in \mathbb{Z}^+$, tal que $K^m(G/N) = \{\bar{e}\}$ y $K^m(N) = \{e\}$. Como la proyección canónica $\pi : G \rightarrow G/N$ es sobreyectiva, resulta que $\pi[K^m(G)] = K^m(G/N) = \{\bar{e}\}$, lo que implica que $K^m(G) \subseteq N$. Entonces $K^{2m}(G) \subseteq K^m(N) = \{e\}$. Por lo tanto G soluble. \square

TEOREMA 6.27. *Sea p un número primo, entonces todo p -grupo es soluble.*

DEMOSTRACIÓN. Si G es abeliano, entonces G es soluble. Sea G no abeliano y procedamos por inducción sobre el orden de G . Si $\circ(G) = p$, entonces G es abeliano y por consiguiente soluble. Supongamos, por hipótesis de inducción, que el teorema sea válido para todo p -grupo, cuyo orden sea menor a $\circ(G)$. Consideremos el centro $Z(G)$. Entonces, por teorema 4.28, $Z(G) \neq \{e\}$ y como $Z(G)$ es abeliano, $Z(G)$ es soluble. Entonces $\circ(G/Z(G)) < \circ(G)$ y, por hipótesis de inducción, $G/Z(G)$ es soluble. Entonces, por teorema 6.26, G es soluble. \square

6.2.1. Ejercicios y Complementos.

1. Sea G un grupo. Mostrar, por inducción sobre m , que $K_m(G)$ es normal en G .
2. Mostrar, por inducción sobre el orden, que todo grupo no abeliano de orden $n < 60$ es soluble.(Ver ejercicio 6.1.3,12)).
3. Sea G un grupo, N un subgrupo normal y soluble y H un subgrupo soluble cualquiera. Mostrar que HN es un subgrupo soluble.
4. Mostrar que todo grupo abeliano de orden p^3 , donde p es un número primo es soluble. (Ver ejercicio 6.1.3,13).
5. Si G es un grupo simple y H un grupo cualquiera, mostrar que un homomorfismo $\psi : G \rightarrow H$ o es inyectivo o el homomorfismo trivial que aplica G sobre $\{e\} \subseteq H$.

6. Sea G un grupo cualquiera. X un conjunto no vacío de subconjuntos no vacíos de G , tal que $M \in X \Rightarrow gMg^{-1} \in X, \forall g \in G$. Mostrar que todo homomorfismo interno φ_g de G induce una biyección $\sigma_g \in \mathcal{A}(X)$, donde $\sigma_g(M) := gMg^{-1}, \forall M \in X$ y que se tiene, entonces, un homomorfismo $\Phi : G \rightarrow \mathcal{A}(X)$, definido por $\Phi(g) := \sigma_g, \forall g \in G$.
7. Sea G un grupo simple, H un subgrupo cualquiera no trivial y

$$M := \{gHg^{-1} \mid g \in G\},$$

entonces el homomorfismo $\Phi : G \rightarrow \mathcal{A}(X)$ es inyectivo y G es isomorfo a un subgrupo de $\mathcal{A}(X)$. En particular si G es un grupo finito y M posee n elementos, G es isomorfo a un subgrupo de \mathfrak{S}_n .

8. Mostrar que el homomorfismo Φ , definido en el ejercicio 6), induce un homomorfismo $\hat{\Phi} : \mathcal{I}(G) \rightarrow \mathcal{A}(X)$ que hace commutar al diagrama:

$$\begin{array}{ccc} G & \xrightarrow{\Phi} & \mathcal{A}(X) \\ \pi \downarrow & & \hat{\Phi} \uparrow \\ G/Z(G) & \xrightarrow{\sim} & \mathcal{I}(G) \end{array}$$

9. Mostrar que \mathfrak{A}_n es el subgrupo más grande contenido en \mathfrak{S}_n .
10. Mostrar que para $n \geq 3$, ningún 2-subgrupo, de orden 2, de \mathfrak{S}_n es normal.
11. Mostrar que para $n \geq 5$ el único subgrupo normal, no trivial de \mathfrak{S}_n es \mathfrak{A}_n . (Asumir que existe un subgrupo normal N , $\circ(N) \geq 3$, aplicar la ecuación (4.12), para $\circ(N \cdot \mathfrak{A}_n)$ y el teorema 5.24).
12. Mostrar, usando el resultado en el ejercicio precedente, que no existe ningún homomorfismo de \mathfrak{S}_n sobre \mathfrak{S}_{n-1} .
13. Mostrar que \mathfrak{A}_5 es el único subgrupo de orden 60 en \mathfrak{S}_5 .
14. Sea G un grupo simple de orden 60.
- Mostrar, usando el resultado del corolario 5.30 y del hecho que todo subgrupo de índice 2 es normal, que G no puede contener ningún subgrupo de índice 2, 3 o 4.
 - Hacer ver que los 3-subgrupos de Sylow y los 5-subgrupos de Sylow no pueden ser únicos.
 - Mostrar que si H es un subgrupo de G de índice $i_G(H) < 15$, entonces $i_G(H) = 1$ y $H = G$.
 - Mostrar que si el normalizador del 2-subgrupo de Sylow de G fuera de índice 15, entonces el grupo H generado por dos 2-subgrupos de Sylow U, V es de índice $i_G(H) < 15$ y por consiguiente $H = G$.
 - Si $W := U \cap V$, U, V como en c), entonces W normal en U y en V y por consiguiente normal en H .
 - Deducir de e) y d) que $W = \{e\}$.
 - Deducir de f) y b) que, dado que existirían 15 2-subgrupos de Sylow cuyos elementos son todos distintos, se tendrían más de 60 elementos en G , por lo que esta situación no puede darse.
 - Deducir entonces que el índice del normalizador de un 2-subgrupo de Sylow debe de ser 5.
 - Si S_2 es un 2-subgrupo de Sylow y $X := \{gS_2g^{-1} \mid g \in G\}$, hacer ver que X posee cinco elementos distintos y que el homomorfismo $\Phi : G \rightarrow \mathcal{A}(X)$,

es inyectivo y puede ser visto como un homomorfismo $\Phi : G \rightarrow \mathfrak{S}_5$. Por consiguiente G es isomorfo a un subgrupo simple, de orden 60, de \mathfrak{S}_5 .

- j) Concluir que G es, entonces, isomorfo a \mathfrak{A}_5 .
- 15. Mostrar que \mathfrak{A}_5 es el único grupo simple, no abeliano, de orden ≤ 60 .
- 16. Mostrar que todo grupo no soluble, de orden 60, debe ser simple y por consiguiente isomorfo a \mathfrak{A}_5 .

6.3. Sucesiones Normales y Series de Composición

6.3.1. Sucesiones Normales.

DEFINICIÓN 6.5. Una sucesión finita,

$$(6.12) \quad \{G_0, \dots, G_m\},$$

de subgrupos de un grupo G , se llama una *sucesión normal* de G , si:

1. La sucesión (6.12), satisface una cadena descendente de inclusiones:

$$(6.13) \quad G = G_0 \supseteq G_1 \supseteq \dots \supseteq G_m = \{e\}$$

2. G_μ normal en $G_{\mu-1}$.

Los cocientes $G_{\mu-1}/G_\mu$ reciben el nombre de *cocientes de la sucesión*. Si $G_\mu \neq G_{\mu-1}$, $\forall \mu = 1, 2, \dots, m$, entonces se dice que la sucesión es *sin repeticiones*.

TEOREMA 6.28. *Un Grupo G es soluble Ssi posee una sucesión normal con cocientes abelianos.*

DEMOSTRACIÓN. Si G es soluble, entonces la sucesión

$$(6.14) \quad \{G, K(G), \dots, K^m(G)\}$$

es una sucesión normal con cocientes abelianos.

Supongamos ahora que G posea una sucesión normal, con cocientes abelianos. Vamos a mostrar, por inducción sobre la longitud de la sucesión, que G es soluble. En efecto, si $m = 1$, $G_0 \supseteq G_1 = \{e\}$ y G/G_1 abeliano implica que G es abeliano y por consiguiente soluble. Supongamos, por hipótesis de inducción que el teorema vale para todo grupo que posea una sucesión normal de longitud $< m$ y sea $m \geq 2$. Entonces si

$$G = G_0 \supseteq G_1 \supseteq \dots \supseteq G_m = \{e\}$$

es una sucesión normal de G de longitud m con coeficientes abelianos,

$$G_1 \supseteq \dots \supseteq G_m = \{e\}$$

es una sucesión normal de G_1 de longitud $m - 1$, con cocientes abelianos y por hipótesis de inducción G_1 es soluble. Como G/G_1 es abeliano y G_1 soluble, resulta, por teorema 6.26, que G es soluble. \square

6.3.2. Series de Composición.

DEFINICIÓN 6.6. Decimos que la sucesión normal

$$(6.15) \quad \{H_0, \dots, H_n\},$$

es un refinamiento de la sucesión normal

$$(6.16) \quad \{G_0, \dots, G_m\},$$

si cada elemento de la sucesión (6.16) está en la sucesión (6.15). Decimos que una sucesión normal es una *serie de composición* del grupo G , si es sin repeticiones y cualquier refinamiento de ella posee repeticiones..

TEOREMA 6.29. *Una sucesión normal es una serie de composición del grupo G Ssi sus cocientes son grupos simples no triviales.*

DEMOSTRACIÓN. La sucesión normal

$$(6.17) \quad \{G_0, \dots, G_m\},$$

es sin repeticiones Ssi $G_{\mu-1}/G_\mu$ es no trivial, $\forall \mu = 1, \dots, m-1$ y la sucesión (6.17) no posee refinamiento Ssi $G_{\mu-1}/G_\mu$ es simple, $\forall \mu = 1, \dots, m-1$. \square

TEOREMA 6.30. *Sea*

$$(6.18) \quad \{G_0, \dots, G_m\},$$

una serie de composición del grupo no trivial G . Entonces G es soluble Ssi todos los cocientes de la serie (6.18) son grupos cíclicos de orden primo.

DEMOSTRACIÓN. Si los cocientes de la serie (6.18), son cíclicos, entonces son abelianos y, por teorema 6.28, G es soluble.

Supongamos ahora que G es soluble. Sea $Q_\mu := G_{\mu-1}/G_\mu$, entonces, por teorema 6.29, Q_μ es simple y no trivial, Q_μ es soluble, ya que es cociente de dos grupos solubles. Por consiguiente $K(Q_\mu) \neq Q_\mu$. Como Q_μ simple, resulta que $K(Q_\mu) = \{\bar{e}\}$ y Q_μ es entonces un grupo abeliano, no trivial, que no posee ningún subgrupo propio no trivial. Entonces, por corolario 6.7, G es cíclico de orden primo. \square

Analicemos el resultado del teorema 6.30 para el caso de un grupo finito G , soluble, de orden $\circ(G) = n = p_1 \cdots p_k$, donde los p_κ , $\kappa = 1, \dots, k$ son números primos, no necesariamente distintos. Entonces si

$$(6.19) \quad \{G_0, \dots, G_m\},$$

es una serie de composición de G , por teorema 6.30, sus cocientes Q_μ son cíclicos de orden primo \tilde{p}_μ , $\forall \mu = 1, \dots, m$.

Como $G_m = \{e\}$, $\circ(Q_m) = \circ(G_{m-1}) = \tilde{p}_m$, $\circ(G_{m-2}) = \circ(Q_{m-1}) \cdot \circ(G_{m-1}) = \tilde{p}_{m-1} \cdot \tilde{p}_m, \dots, \circ(G_0) = \tilde{p}_1 \cdots \tilde{p}_m = \circ(G) = p_1 \cdots p_k$. Como la descomposición en números primos es única, salvo orden de los factores, resulta que $m = k$ y, luego de un posible reordenamiento, $\tilde{p}_\kappa = p_\kappa$. Esto quiere decir que la longitud de la serie de composición (6.19), está determinada por la descomposición en factores primos del orden de G .

Lo anteriormente expuesto lo podemos resumir en el siguiente

TEOREMA 6.31 (Teorema de Hölder para grupos finitos). *Todas las series de composición de un grupo finito G poseen la misma longitud y sus cocientes respecto del mismo primo son isomorfos.*

El teorema general de Hölder, del cual 6.31, es un caso particular es el siguiente

TEOREMA 6.32. *Los cocientes de dos series de composición cualesquiera de un grupo G son isomorfos, previo un reordenamiento adecuado.*

CAPÍTULO 7

CLASIFICACIÓN DE LOS GRUPOS ABELIANOS FINITAMENTE GENERADOS

En este capítulo estudiaremos los grupos abelianos *finitamente generados*. Es decir grupos abelianos que pueden ser generados por un número finito de elementos. Nuestra meta es mostrar que todo grupo abeliano, finitamente generado, puede ser representado como un producto directo de r copias del grupo de los enteros \mathbb{Z} , el cual determina el *rango* del grupo y de m copias de grupos finitos isomorfos a \mathbb{Z}_{q_μ} , donde q_μ es potencia de un número primo p_μ , $\forall \mu = 1, \dots, m$, el cual determina la parte de *torsión* del grupo. m o r pueden ser, según el caso, iguales a 0, pero no ambos 0 al mismo tiempo. Si G es un grupo abeliano finito, entonces $r = 0$ y m será igual al número mínimo de generadores de G . En el caso en que el grupo G sea libre de *torsión* entonces tendremos $m = 0$ y r igual al número mínimo de generadores de G . En general $m + r$ será el número mínimo de generadores de G .

7.1. Producto Directo de Subgrupos

Dado un grupo G y subgrupos G_1, \dots, G_n de G , al conjunto

$$(7.1) \quad \prod_{v=1}^n G_v = G_1 \cdots G_n := \{g \in G \mid g = g_1 \cdots g_n, g_v \in G_v\}$$

lo llamamos el *producto de los subgrupos* G_1, \dots, G_n .

Decimos que el producto es *consistente*, si

$$g_1 \cdots g_n = \tilde{g}_1 \cdots \tilde{g}_n \Rightarrow g_v = \tilde{g}_v, v = 1, \dots, n.$$

Es decir, que la representación de cada elemento $g \in \prod_{v=1}^n G_v$ es única.

TEOREMA 7.1. *El producto de dos subgrupos G_1, G_2 de un grupo G es consistente Ssi $G_1 \cap G_2 = \{e\}$.*

DEMOSTRACIÓN. Sea $G_1 \cdot G_2$ consistente. Si $g \in G_1 \cap G_2$, $g^{-1} \in G_1 \cap G_2$ y $e = g \cdot g^{-1} = e \cdot e$, por consiguiente $g = e$ y $G_1 \cap G_2 = \{e\}$.

Por otra parte si $G_1 \cap G_2 = \{e\}$ y $g_1, \tilde{g}_1 \in G_1$, $g_2, \tilde{g}_2 \in G_2$, tales que $g_1 \cdot g_2 = \tilde{g}_1 \cdot \tilde{g}_2$, entonces $\tilde{g}_1^{-1} g_1 = \tilde{g}_2 \cdot g_2^{-1} \in G_1 \cap G_2 = \{e\}$. Por consiguiente $g_1 = \tilde{g}_1$ y $g_2 = \tilde{g}_2$. \square

Recordamos al lector que, en general, el producto de subgrupos no es un grupo. Sin embargo si G es un grupo abeliano, entonces el producto de cualesquiera dos subgrupos, o más, sí es un subgrupo.

DEFINICIÓN 7.1. Decimos que el grupo abeliano G es *producto directo* de los subgrupos G_1, \dots, G_n , si

$$G = \prod_{v=1}^n G_v$$

y el producto es consistente.

TEOREMA 7.2. *Sea G un grupo abeliano y G_1, \dots, G_n subgrupos de G , tales que*

$$(7.2) \quad G = \prod_{v=1}^n G_v.$$

(7.2) *es un producto directo Ssi e posee una representación única, como producto de elementos de los G_v , $v = 1, \dots, n$.*

DEMOSTRACIÓN. En efecto, la condición es necesaria, por definición de producto directo.

Mostraremos que la condición es también suficiente. En efecto, sea $g_1 \cdots g_n = \tilde{g}_1 \cdots \tilde{g}_n$, entonces, como G es abeliano se tiene

$$(7.3) \quad e = (\tilde{g}_1 \cdot g_1^{-1}) \cdots (\tilde{g}_n \cdot g_n^{-1}).$$

Como, por hipótesis, e posee representación única, de (7.3), resulta que $g_v = \tilde{g}_v$, $\forall v = 1, \dots, n$. Por lo tanto (7.2) es producto directo. \square

OBSERVACIÓN. Si $G = G_1 \cdots G_n$, $n \geq 2$, definimos $\tilde{G}_v := G_1 \cdots \hat{G}_v \cdots G_n$, donde $\hat{}$ significa eliminación de este factor.

Como consecuencia del teorema 7.2, se obtiene el siguiente

TEOREMA 7.3. *El producto*

$$(7.4) \quad G = \prod_{v=1}^n G_v$$

es directo, Ssi

$$(7.5) \quad G_v \cap \tilde{G}_v = \{e\}, \quad v = 1, \dots, n.$$

DEMOSTRACIÓN. Si (7.4) es un producto directo, entonces $g \in G$ posee representación única como producto de elementos de los G_v , $v = 1, \dots, n$. Supongamos $g \in G_v \cap \tilde{G}_v$, entonces $g = g_v$ y $g = g_1 \cdots \hat{g}_v \cdots g_n$, serían dos representaciones distintas de g , salvo que $g = g_v = e$. Por consiguiente vale la ecuación (7.5).

Por otra parte, si (7.5) vale, sea $g = g_1 \cdots g_n = g_v \tilde{g}_v = g'_1 \cdots g'_n = g'_v \cdot \tilde{g}'_v$. Entonces $\tilde{g}_v \cdot \tilde{g}'_v = g'_v \cdot g_v^{-1} \in G_v \cap \tilde{G}_v = \{e\}$. Por consiguiente $g'_v = g_v$, $\forall v = 1, \dots, n$ y (7.4) es producto directo. \square

TEOREMA 7.4. *Sea*

$$(7.6) \quad G = \prod_{v=1}^n G_v,$$

donde G es un grupo abeliano y para cada $v = 1, \dots, n$, G_v producto de subgrupos $G_{v\mu}$, $\mu = 1, \dots, m_v$,

$$(7.7) \quad G_v = \prod_{\mu=1}^{m_v} G_{v\mu}$$

Entonces

$$(7.8) \quad G = \prod_{v=1}^n G_v = \prod_{v=1}^n \prod_{\mu=1}^{m_v} G_{v\mu}$$

es producto directo de los $G_{v\mu}$, $v = 1, \dots, n$, $\mu = 1, \dots, m_v$. Si los productos (7.6) y (7.7) son directos.

DEMOSTRACIÓN. En efecto, si (7.8) es un producto directo, pero para algún v (7.7) no fuera un producto directo, entonces, para dicho v , e poseería dos representaciones distintas como producto de los subgrupos $G_{v\mu}$, lo cual nos daría, al menos, dos representaciones distintas, para G como producto de todos los subgrupos $G_{v\mu}$. Por consiguiente (7.7) debe ser un producto directo.

Por otra parte, si $e = g_1 \cdots g_n$, $g_v \in G_v$ y como cada $g_v = g_{v1} \cdots g_{vm_v}$, entonces $e = g_{11} \cdots g_{1m_1} \cdots g_{n1} \cdots g_{nm_n}$, donde todos los $g_{n\mu}$ son iguales a e . Por consiguiente $g_v = e$, $\forall v = 1, \dots, n$ y (7.6) es producto directo.

Si (7.7) y (7.6) son productos directos y $e = g_{11} \cdots g_{1m_1} \cdots g_{n1} \cdots g_{nm_n} = g'_1 \cdots g'_n$, donde $g'_v = g_{v1} \cdots g_{vm_v}$, entonces, por hipótesis $g'_v = e$, $\forall v = 1, \dots, n$ y cada $g_{v\mu} = e$, $\forall v = 1, \dots, n$, $\forall \mu = 1, \dots, m_v$. Por lo tanto (7.8) es producto directo. \square

7.2. Grupos Abelianos Finitamente Generados

En esta sección desarrollaremos, paso a paso, la teoría necesaria que nos conducirá a la clasificación de los grupos abelianos finitamente generados.

7.2.1. Grupos Abelianos Finitos.

TEOREMA 7.5. *Todo grupo abeliano finito es producto directo de sus subgrupos de Sylow.*

DEMOSTRACIÓN. Sea $\circ(G) = p_1^{\alpha_1} \cdots p_m^{\alpha_m}$, donde los p_μ son números primos distintos, $\mu = 1, \dots, m$. Por el teorema de Sylow para grupos abelianos 6.5, para cada p_μ existe un único p_μ -subgrupo de Sylow de orden $p_\mu^{\alpha_\mu}$, que lo designaremos por S_μ .

Vamos a mostrar que $S_\mu \cap \tilde{S}_\mu = \{e\}$. En efecto si G_1, G_2 son dos grupos de órdenes r, s , respectivamente, entonces $\circ(G_1 \cap G_2)$ divide a $\circ(G_1)$ y a $\circ(G_2)$. Entonces si $\text{MCD}(\circ(G_1), \circ(G_2)) = 1$, $G_1 \cap G_2 = \{e\}$. Como para el grupo de Sylow S_μ vale que $\text{MCD}(\circ(S_\mu), \circ(\tilde{S}_\mu)) = 1$, resulta que $S_\mu \cap \tilde{S}_\mu = \{e\}$. Por consiguiente el producto

$$\prod_{\mu=1}^m S_\mu$$

es directo.

De la ecuación

$$\circ(S_\mu \cdot \tilde{S}_\mu) = \frac{\circ(S_\mu) \cdot \circ(\tilde{S}_\mu)}{\circ(S_\mu \cap \tilde{S}_\mu)},$$

y del hecho que $S_\mu \cap \tilde{S}_\mu = \{e\}$, resulta que

$$\circ(S_1 \cdots S_m) = \circ(S_\mu \cdot \tilde{S}_\mu) = p_1^{\alpha_1} \cdots p_m^{\alpha_m} = \circ(G)$$

por consiguiente

$$(7.9) \quad G = \prod_{\mu=1}^m S_\mu,$$

donde (7.9) es un producto directo. \square

En particular si $G := \mathbb{Z}_n$ y $n = p_1^{r_1} \cdots p_m^{r_m}$ la descomposición de n en factores primos y $q_\mu := p_\mu^{r_\mu}$, $1 \leq \mu \leq m$, se tiene el siguiente

COROLARIO 7.6. $\mathbb{Z}_n \simeq \mathbb{Z}_{q_1} \times \cdots \times \mathbb{Z}_{q_m}$.

Para el grupo multiplicativo \mathbb{Z}_n^* de todos los elementos $(\text{mód } n)$ primos relativos con n se tiene también:

COROLARIO 7.7. $\mathbb{Z}_n^* \simeq \mathbb{Z}_{q_1}^* \times \cdots \times \mathbb{Z}_{q_m}^*$.

Este corolario es particularmente interesante para calcular la función de Euler $\phi(n)$. Como vimos anteriormente $\circ(\mathbb{Z}_n^*) = \phi(n) = \phi(q_1) \cdots \phi(q_m)$. Entonces, si conocemos el valor de $\phi(q_\mu) = \phi(p_\mu^{r_\mu})$, podemos calcular $\phi(n)$. Dado un número primo p y un entero positivo r ¿Cuántos números primos relativos con p^r , menores que p^r existen? Entre todos los números $0 \leq m < p^r$ debemos eliminar todos los múltiplos de p , es decir todos los números de la forma $0, p, 2p, \dots, (p^{r-1} - 1)p = p^r - p$, que en total son p^r elementos. Entonces $\phi(p^r) = p^r - p^{r-1}$. Con esto hemos demostrado el siguiente

LEMA 7.8. Si p es un número primo y r un entero positivo, entonces

$$\phi(p^r) = p^r \left(1 - \frac{1}{p}\right) = p^r - p^{r-1}.$$

Por otra parte si $p_1^{r_1} \cdots p_m^{r_m}$ es la descomposición en factores primos de un entero positivo n , entonces

$$\phi(n) = \phi(q_1) \cdots \phi(q_m) = \prod_{\mu=1}^m p_\mu^{r_\mu} \left(1 - \frac{1}{p_\mu}\right) = \prod_{\mu=1}^m (p_\mu - 1) p_\mu^{r_\mu - 1}.$$

DEFINICIÓN 7.2. Decimos que el grupo abeliano G es *directamente reducible* si puede ser expresado como un producto directo de subgrupos

$$G = \prod_{v=1}^n G_v, \quad n \geq 2.$$

En caso que $G \neq \{e\}$ no pueda ser expresado de esta forma, entonces se dice que es *directamente irreducible*.

Del teorema 7.5 se deduce el siguiente

COROLARIO 7.9. Todo subgrupo directamente irreducible de un grupo abeliano, finito G es un p -grupo.

DEMOSTRACIÓN. En efecto, si G no fuera un p -grupo, por teorema 7.5, G sería producto directo de sus subgrupos de Sylow, con $n \geq 2$. Por lo tanto G debe ser un p -grupo. \square

Sin embargo si G es un p -grupo, G puede ser directamente reducible, como lo muestra el siguiente

EJEMPLO 7.1. Si G es el grupo generado por las transposiciones

$$\{\begin{pmatrix} 1 & 2 \end{pmatrix}, \begin{pmatrix} 3 & 4 \end{pmatrix}\},$$

entonces $\circ(G) = 4$ y es un 2-grupo. Pero $G = G_1 \cdot G_2$, donde

$$\begin{aligned} G_1 &:= \{e, \begin{pmatrix} 1 & 2 \end{pmatrix}\} \\ G_2 &:= \{e, \begin{pmatrix} 3 & 4 \end{pmatrix}\} \end{aligned}$$

Sin embargo para grupos cíclicos se tiene el siguiente

TEOREMA 7.10.

- a) *Todo grupo cíclico infinito es directamente irreducible.*
- b) *Un grupo cíclico finito de orden $n \geq 2$ es directamente irreducible. Si es un p -grupo.*

DEMOSTRACIÓN.

- a) G es directamente irreducible si para cada par de subgrupos G_1, G_2 de G , $G_1 \cap G_2 \neq \{e\}$. Si G es un grupo cíclico infinito, entonces, por ejercicio 4.3.3, G es isomorfo al grupo aditivo de los enteros \mathbb{Z} . Vamos a mostrar que \mathbb{Z} es directamente irreducible. En efecto, por lema 4.19, los subgrupos de \mathbb{Z} son de la forma $m\mathbb{Z}$, donde $m \in \mathbb{Z}$. Dados $m, n \in \mathbb{Z}$ distintos de 1, entonces, por ejercicio 4.2.4.5), $m\mathbb{Z} \cap n\mathbb{Z} = \text{lcm}(m, n)\mathbb{Z} \neq \{0\}$. Por lo tanto \mathbb{Z} es directamente irreducible.
- b) Si G es un grupo cíclico finito, directamente irreducible, entonces, por corolario 7.9, G es un p -grupo.

Por otra parte, sea G un grupo cíclico de orden p^m , $m \geq 1$. Vamos a mostrar que si H_1, H_2 son dos subgrupos cualesquiera de G , entonces $H_1 \subseteq H_2$, o $H_2 \subseteq H_1$, por lo que $H_1 \cap H_2 \neq \{e\}$. En efecto, sin limitación de la generalidad, sea $\text{o}(H_1) = p^r$, $\text{o}(H_2) = p^{r+s}$, $r \geq 1$, $s \geq 1$, entonces, por teorema 6.6, H_2 posee un único subgrupo de orden p^r , el cual debe coincidir con H_1 .

□

TEOREMA 7.11. *Todo grupo cíclico es producto directo de subgrupos directamente irreducibles.*

DEMOSTRACIÓN. Si G es infinito, entonces G es isomorfo a \mathbb{Z} y no hay nada que demostrar. Si G es finito, entonces G es producto directo de sus subgrupos de Sylow, los cuales, por teorema 7.10, son directamente irreducibles. □

TEOREMA 7.12. *La representación de un grupo cíclico G , como producto de subgrupos directamente irreducibles, es, salvo orden de los factores, única.*

DEMOSTRACIÓN. Si G es infinito, entonces G es isomorfo a \mathbb{Z} y no hay nada que demostrar. Mostremos, entonces, que la aserción vale para el caso en que G es un grupo finito. En efecto, sea

$$G = \prod_{v=1}^n G_v$$

una representación de G como producto de subgrupos directamente irreducibles. Entonces los subgrupos G_1, \dots, G_n son p_v -grupos, donde p_v es un número primo que divide a $\text{o}(G)$. Para p_v dado, denotemos por $G^1 := G_v$, y por G^2, \dots, G^r los otros posibles p_v -grupos que aparecen en la descomposición. Por S_v denotaremos al p_v -grupo de Sylow correspondiente. Como S_v contiene a todos los p_v -subgrupos, entonces

$$(7.10) \quad \prod_{\rho=1}^r G^\rho \subseteq S_v.$$

Por otra parte, si $g \in S_v$, como elemento de G , posee una única representación $g = g_1 \cdots g_n$, $g_v \in G_v$, $v = 1, \dots, n$. Como $\circ(g) \mid \circ(S_v)$, $\circ(g)$ debe ser una potencia de p_v . Entonces, para un $1 \leq k \leq n$, tal que $p_v \neq p_k$, $g_k = e$, por lo que

$$(7.11) \quad S_v \subseteq \prod_{\rho=1}^r G^\rho.$$

Entonces de (7.10) y de (7.11), resulta

$$(7.12) \quad \prod_{\rho=1}^r G^\rho = S_v.$$

Como S_v es irreducible, vale, entonces, que $r = 1$ y $G_v = S_v$. \square

El siguiente paso es mostrar que si G es un grupo abeliano, generado por un número finito de elementos, entonces lo podemos representar como un producto directo de subgrupos cíclicos.

TEOREMA 7.13. *Si G es un grupo abeliano que posee un conjunto de n generadores, entonces G posee una representación como producto de, a lo sumo, n subgrupos cíclicos.*

DEMOSTRACIÓN. Por inducción sobre n . Si G posee un único generador, G es ya cíclico y el teorema vale. Sea, entonces, $n > 1$ y asumamos, por hipótesis de inducción, que el teorema sea válido para n y mostremos que es válido para $n + 1$.

Sea, entonces, G un grupo abeliano generado por exactamente $n + 1$ elementos. Sean estos g, g_1, \dots, g_n . Entonces $G = \langle g, g_1, \dots, g_n \rangle$. $g \notin \langle g_1, \dots, g_n \rangle$. Si $\forall m > 1$, $g^m \notin \langle g_1, \dots, g_n \rangle$, salvo, $g^m = e$, entonces $\langle g \rangle \cap \langle g_1, \dots, g_n \rangle = \{e\}$ y G es producto directo de $\langle g \rangle$ y $\langle g_1, \dots, g_n \rangle$, donde por hipótesis de inducción $\langle g_1, \dots, g_n \rangle$ es producto directo de, a lo sumo, n subgrupos cíclicos.

Supongamos que en toda representación de G como $\langle g, g_1, \dots, g_n \rangle$, existe siempre un entero $m > 1$, tal que $e \neq g^m \in \langle g_1, \dots, g_n \rangle$. Entonces escojamos aquella en que m es minimal entre todas las posibles representaciones y denotemos, luego de un reordenamiento adecuado, por g , al elemento para el cual m es minimal.

Estudiemos la relación $g^m \cdot g_1^{m_1} \cdots g_n^{m_n}$. Entonces, por el algoritmo de Euclides, para cada v , $1 \leq v \leq n$, existen enteros q_v, r_v , $0 \leq r_v < m$, tales que $m_v = q_v m + r_v$. Sea $\bar{g} := g \cdot g_1^{q_1} \cdots g_n^{q_n}$. Entonces $G = \langle \bar{g}, g_1, \dots, g_n \rangle$, ya que $g = \bar{g} \cdot g_1^{-q_1} \cdots g_n^{-q_n}$.

Como $\bar{g}^m = g^m \cdot g_1^{mq_1} \cdots g_n^{mq_n}$, entonces $\bar{g}^m \cdot g_1^{r_1} \cdots g_n^{r_n} = g^m \cdot g_1^{m_1} \cdots g_n^{m_n} = e$.

Supongamos que para algún v , $1 \leq v \leq n$, $r_v > 0$, entonces tendríamos que $g_v^{r_v}$ es generado por los elementos restantes, con $0 \leq r_v < m$, en contradicción a la escogencia de m y g . Por consiguiente $r_v = 0$, $\forall v$ y $\bar{g}^m = e$. Por lo tanto $\langle \bar{g} \rangle \cap \langle g_1, \dots, g_n \rangle = e$, lo que nos lleva al caso precedente. \square

Como una consecuencia inmediata de los teoremas 7.12 y 7.13, se obtiene el siguiente

COROLARIO 7.14. *Todo grupo abeliano, no trivial, finitamente generado, es producto directo de grupos cíclicos directamente irreducibles.*

TEOREMA 7.15. *Sea G un grupo abeliano. El conjunto*

$$T := \{g \in G \mid \circ(g) < \infty\}$$

es un subgrupo de G , llamado subgrupo de torsión. Si $T = \{e\}$, entonces se dice que G es libre de torsión. Si $G = T$, entonces se dice que G es un grupo de torsión. Los elementos de T reciben el nombre de elementos de torsión de G .

DEMOSTRACIÓN. Es claro que $e \in T$, por lo que $T \neq \emptyset$. Si $g \in T$, entonces existe $m > 0$, tal que $g^m = e$ y $(g^{-1})^m = e$, por consiguiente $g^{-1} \in T$. Dados $g, h \in T$, $m, n > 0$, tales que $g^m = e$ y $h^n = e$, entonces $(g \cdot h)^{mn} = e$, y $g \cdot h \in T$. Por lo tanto T es un subgrupo de G . \square

EJEMPLO 7.2. Todo grupo abeliano finito es de torsión, mientras que todo grupo cíclico infinito es libre de torsión.

LEMA 7.16. *Si el grupo abeliano G es producto de subgrupos G_1, \dots, G_n libres de torsión, entonces G es libre de torsión.*

DEMOSTRACIÓN. Supongamos que para $g \in G$, $g = g_1 \cdots g_n$, $g^m = e$, entonces $e = g_1^m \cdots g_n^m$ y $g_v^m = e$, $\forall v = 1, \dots, n$. Por consiguiente $g_v = e$, $\forall v = 1, \dots, n$. \square

TEOREMA 7.17. *Todo grupo abeliano, finitamente generado, es producto directo de su subgrupo de torsión, T , con un grupo libre de torsión F .*

DEMOSTRACIÓN. Por corolario 7.14, G es producto directo de grupos cíclicos directamente irreducibles

$$G = G_1 \cdots G_r \cdot H_1 \cdots H_s,$$

ordenados, tales que G_1, \dots, G_r son cíclicos infinitos y H_1, \dots, H_s cíclicos finitos.

El grupo

$$H := \prod_{\sigma=1}^s H_\sigma$$

es finito, y por consiguiente $H \subseteq T$. El grupo

$$F := \prod_{\rho=1}^r G_\rho$$

es, por lema 7.16, libre de torsión. Entonces G es producto directo de F y H . Vamos a mostrar que $H = T$. En efecto, ya vimos que $H \subseteq T$, mostremos que también $T \subseteq H$. Sea $g \in G$, $g = f \cdot h$, donde $f \in F$ y $h \in H$ y g un elemento de torsión. Entonces existe un entero $m > 0$, tal que $g^m = e$ y $g^m = f^m \cdot h^m = e$, como $f \in F$, $f^m = e \Rightarrow f = e$ y $g = h \in H$. Por lo tanto $H = T$. \square

7.2.2. Ejercicios y Complementos.

1. Sea G un grupo abeliano, $G = F \cdot H$, la descomposición de G como producto directo de un grupo libre de torsión F con su subgrupo de torsión T .
 - a) Mostrar que $\varphi : G \rightarrow F$, definido por $\varphi(g) := f$, donde $g = f \cdot h$, $f \in F$, $h \in T$, es un homomorfismo de grupos.
 - b) $\ker \varphi = T$
 - c) F es isomorfo a G/T , por lo que F es único, salvo isomorfismo.
2. Sea H un subgrupo del grupo abeliano G , para un entero $m \geq 1$, sea

$$H^m := \{h^m \mid h \in H\}.$$

Mostrar que H^m es un subgrupo de G .

3. Sea $\psi : G \rightarrow \tilde{G}$ un homomorfismo de grupos, $H \subseteq G$ un subgrupo. Si $\psi|_H : H \rightarrow \tilde{G}$ es la restricción de ψ sobre H , entonces:
 - a) $\ker \psi|_H = \ker \psi \cap H$.
 - b) $\psi[H]$ es isomorfo a $H/(\ker \psi \cap H)$.

4. Sean G, H grupos abelianos y

$$G \times H := \{(g, h) \mid g \in G, h \in H\},$$

provisto de una operación binaria, \cdot , definida por $(g, h) \cdot (\tilde{g}, \tilde{h}) := (g \cdot \tilde{g}, h \cdot \tilde{h})$.

- a) Mostrar que $(G \times H, \cdot)$ es un grupo abeliano.
- b) Mostrar que $G \times H$ es producto directo de G y H , donde G lo identificamos con el subgrupo $G \times \{e\}$ y H con el subgrupo $\{e\} \times H$.
- c) Generalizar los resultados en a), b) si

$$G := G_1 \times G_2 \times \cdots \times G_n := \{(g_1, \dots, g_n) \mid g_v \in G_v, v = 1, \dots, n\},$$

donde los $G_v, v = 1, \dots, n$ son grupos abelianos.

7.2.3. Teoremas de Clasificación.

LEMA 7.18. *Sea G un grupo abeliano, $m \geq 1$ un entero. Si*

$$(7.13) \quad G = \prod_{v=1}^n G_v,$$

donde (7.13) es producto directo, entonces

$$(7.14) \quad G^m = \prod_{v=1}^n G_v^m$$

y

$$(7.15) \quad G/G^m = \prod_{v=1}^n \tilde{G}_v,$$

donde (7.14), (7.15) son productos directos y \tilde{G}_v es isomorfo a G_v/G_v^m .

DEMOSTRACIÓN. Si $g \in G$, $g = g_1 \cdots g_n$, $g_v \in G_v$, entonces $g^m = g_1^m \cdots g_n^m$, donde $g_v^m \in G_v$. Como la representación es única, resulta que (7.14), es producto directo.

Si $g^m = g_1^m \cdots g_n^m \in G_v$, entonces $g_j^m = e$, si $j \neq v$ y $G_v \cap G^m = G_v^m$. Si $\tilde{G} := G/G^m$, y $\pi : G \rightarrow G/G^m$ es la proyección canónica, entonces, por ejercicio 7.2.2,3), $\pi[G_v]$ es isomorfo a G_v/G_v^m . De (7.13), se sigue que

$$(7.16) \quad \tilde{G} = \pi[G] = \prod_{v=1}^n \tilde{G}_v.$$

Vamos a mostrar que el producto (7.16), es directo. En efecto, si $\pi(g_1 \cdots g_n) = \tilde{g}_1 \cdots \tilde{g}_n = \tilde{e}$, $\tilde{g}_v \in \tilde{G}_v$, entonces $g_1 \cdots g_n \in G^m$ y, como (7.14), es producto directo, $g_1 \cdots g_n = g'_1 \cdots g'_n$, $g'_v \in G_v^m$, como la representación es única, resulta, entonces, que $g_v = g'_v \in G_v^m$, por consiguiente $\tilde{g}_v = \tilde{e}$, $\forall v = 1, \dots, n$. Por lo que el producto (7.16) es directo. \square

TEOREMA 7.19. *Sea $F \neq \{e\}$ un grupo abeliano, libre de torsión. Entonces F es producto directo de grupos cíclicos infinitos, cuyo número está únicamente determinado.*

DEMOSTRACIÓN. Del teorema 7.17, sabemos que F es producto directo de grupos cíclicos infinitos F_1, \dots, F_r , cada uno isomorfo a \mathbb{Z} . Por el lema 7.18 es F/F^2 producto de r

subgrupos isomorfos a $\mathbb{Z}/2\mathbb{Z}$, por lo que F/F_2 posee exactamente 2^r elementos. Número que sólo depende de F . Entonces

$$F \approx \underbrace{\mathbb{Z} \times \cdots \times \mathbb{Z}}_r$$

□

DEFINICIÓN 7.3. El número r , determinado en el teorema 7.19, se llama el *rango* de F . Para un grupo abeliano cualquiera, finitamente generado, se define el *rango* como el rango de G/T .

TEOREMA 7.20. Si

$$G = G = \prod_{v=1}^n G_v,$$

es una descomposición del grupo abeliano, finito G , como producto directo de grupos cíclicos directamente irreducibles, entonces los números $q_v := \circ(G_v)$ están únicamente determinados.

DEMOSTRACIÓN. Como cada G_v es un p -grupo, q_v es una potencia de un número primo p_v . Uniendo los factores que corresponden al mismo primo, se obtiene la descomposición única en subgrupos de Sylow de G . Basta mostrar, entonces, el teorema para G , tal que $\circ(G) = p^m$, $m \geq 1$. Entonces $q_v = p^{m_v}$, con $m_1 + \cdots + m_n = m$.

Procedamos por inducción sobre m . Para $m = 1$ el teorema es trivialmente válido. Sea $m > 1$ y supongamos, por hipótesis de inducción, que el teorema vale para todo p -grupo de orden $< p^m$. Como la potenciación por p disminuye el orden, $G^p \neq G$ y $\circ(G^p) < \circ(G)$.

Consideremos dos casos:

1. $G^p = \{e\}$. Entonces $\forall v = 1, \dots, n$, $G_v^p = \{e\}$ y $q_1 = q_2 = \cdots = q_n = p$, $n = m$ y estamos listos.
2. $G^p \neq \{e\}$.

Como $\circ(G^p) < \circ(G) = p^m$, entonces, por hipótesis de inducción, G^p posee una descomposición en el sentido del teorema.

Consideremos los grupos G_v^p , $1 \leq v \leq n$. El grupo cíclico G_v^p es un p -grupo y por teorema 7.10, G^p es irreducible o $G_v^p = \{e\}$.

Sean

$$I := \{v \mid G_v^p = \{e\}\}, \quad J := \{v \mid G_v^p \neq \{e\}\}.$$

Como G^p es producto directo de los grupos cíclicos irreducibles G_v^p , $v = 1, \dots, n$, por hipótesis de inducción los números $\circ(G_v^p)$ están únicamente determinados para $v \in J$. Como para $v \in I$

$$q_v = \circ(G_v) = i_{G_v}(G_v^p) \cdot \circ(G_v^p) = p \cdot \circ(G_v^p) \geq p^2,$$

resulta que q_v está también únicamente determinado. O sea que

$$\{q_v \mid v \in J\} = \{q_v \mid q_v \geq p^2\}$$

y

$$\{q_v \mid v \in I\} = \{q_v \mid q_v = p\}.$$

Entonces

$$\circ(G) = \circ(G_1) \cdot \circ(G_n) = i_G(G^p) \cdot \circ(G^p) = \circ(G_1/G_1^p \cdots G_n/G_n^p) \cdot \circ(G^p) = p^{l+s} \cdot \circ(G^p),$$

donde s es el número de elementos en J y l el número de elementos en I . Como s y $\circ(G_p)$ están únicamente determinados, entonces l está únicamente determinado. Lo que muestra el teorema. □

Del teorema 7.20 se deduce que cada factor irreducible G_v es isomorfo a $\mathbb{Z}/q_v\mathbb{Z}$.

Analicemos, brevemente, los resultados hasta ahora obtenidos:

Si G es un grupo abeliano finitamente generado, entonces por el teorema 7.17,

$$(7.17) \quad G = F \cdot T,$$

donde F es un grupo libre de torsión y T es el subgrupo de torsión de G .

Por el teorema 7.19

$$(7.18) \quad F \approx \underbrace{\mathbb{Z} \times \cdots \times \mathbb{Z}}_r,$$

donde r es el rango de G/T .

Resumiendo, de (7.17), (7.18) y teorema 7.20 obtenemos el

TEOREMA 7.21 (Teorema Fundamental para Grupos Abelianos Finitamente Generados). *Un grupo abeliano $G \neq \{e\}$ es finitamente generado Ssi existen potencias de números primos q_1, \dots, q_m , y un número $r \geq 0$, tales que $m + r > 0$ y*

$$(7.19) \quad G \approx (\mathbb{Z}/q_1\mathbb{Z} \times \cdots \times \mathbb{Z}/q_m\mathbb{Z}) \times \underbrace{\mathbb{Z} \times \cdots \times \mathbb{Z}}_r,$$

donde r , el rango de G , y los números q_μ , $\mu = 1, \dots, m$, están únicamente determinados.

CAPÍTULO 8

PRODUCTO Y SUMA DIRECTA DE FAMILIA DE GRUPOS. GRUPOS LIBRES

En este capítulo estudiaremos el producto sobre una familia cualquiera de grupos, el cual puede ser dotado de una estructura de grupo, llamado el grupo producto, así como la *suma directa* sobre dicha familia. Relacionados con estos dos grupos se tienen los llamados grupos libres sobre un conjunto no vacío S de cualquier cardinalidad.

En el capítulo precedente vimos que todo grupo abeliano finitamente generado G es producto directo de un subgrupo libre de torsión F y un subgrupo de torsión T . Nuestra meta es mostrar que dado un conjunto cualquiera, S , no vacío, siempre es posible construirnos un grupo G generado por S y libre de torsión, al cual llamaremos *el grupo libre* generado por S , ya que dicho grupo será único, salvo isomorfismo.

8.1. Producto Directo y Suma Directa Sobre Una Familia de Grupos

8.1.1. Grupo Producto.

Sea $(G_i)_{i \in I}$ una familia de grupos. Si

$$G := \prod_{i \in I} G_i$$

es el producto cartesiano de la familia de conjuntos $(G_i)_{i \in I}$. Dados $(g_i)_{i \in I}, (h_i)_{i \in I} \in G$, por medio de $(g_i)_{i \in I} \cdot (h_i)_{i \in I} := (g_i h_i)_{i \in I}$, se define un producto $\cdot : G \times G \rightarrow G$, tal que (G, \cdot) es un grupo y las proyecciones

$$p_i : G \rightarrow G_i$$

son homomorfismos de grupos, para todo $i \in I$. $(G, \cdot, p_i)_{i \in I}$ lo llamamos *el grupo producto directo* sobre la familia $(G_i)_{i \in I}$. El lector comprobará fácilmente que, en efecto, (G, \cdot) cumple con los axiomas de grupo y que las proyecciones p_i son homomorfismos de grupos.

El grupo producto $(G, \cdot, p_i)_{i \in I}$ posee la siguiente *propiedad universal*: Dado un grupo cualquiera H y una familia de homomorfismos

$$(\psi_i : H \rightarrow G_i)_{i \in I},$$

existe un único homomorfismo

$$\psi : H \rightarrow G,$$

tal que para todo $i \in I$, el diagrama

(8.1)

$$\begin{array}{ccc} H & \xrightarrow{\psi} & G \\ & \searrow \psi_i & \downarrow p_i \\ & & G_i \end{array}$$

es comunitativo.

En efecto $\psi : H \rightarrow G$, definido por $\psi(h) := (\psi_i(h))_{i \in I}$ es un homomorfismo de grupos y es el único que hace commutar al diagrama (8.1), como el lector comprobará fácilmente.

De la propiedad universal que satisface el grupo producto $(G, \cdot, p_i)_{i \in I}$, se deduce que si $(\tilde{G}, \cdot, \tilde{p}_i)_{i \in I}$, es otro grupo que satisface dicha propiedad, entonces G es isomorfo a \tilde{G} .

En efecto, por la propiedad universal, existe un único homomorfismo $\psi : \tilde{G} \rightarrow G$ y un único homomorfismo $\tilde{\psi} : G \rightarrow \tilde{G}$, tales que los diagramas

(8.2)

$$\begin{array}{ccc} \tilde{G} & \xrightarrow{\psi} & G \\ & \searrow \tilde{p}_i & \downarrow p_i \\ & & G_i \end{array}$$

y

(8.3)

$$\begin{array}{ccc} G & \xrightarrow{\tilde{\psi}} & \tilde{G} \\ & \searrow p_i & \downarrow \tilde{p}_i \\ & & G_i \end{array}$$

son comutativos.

Entonces el homomorfismo $(\tilde{\psi} \circ \psi) : \tilde{G} \rightarrow \tilde{G}$ hace comutar al diagrama

(8.4)

$$\begin{array}{ccc} \tilde{G} & \xrightarrow{\tilde{\psi} \circ \psi} & \tilde{G} \\ & \searrow \tilde{p}_i & \downarrow \tilde{p}_i \\ & & G_i \end{array}$$

y por la propiedad universal $(\tilde{\psi} \circ \psi) = 1_{\tilde{G}}$. Un argumento análogo nos muestra que también $(\psi \circ \tilde{\psi}) = 1_G$. Por consiguiente ψ es un isomorfismo de grupos.

EJEMPLO 8.1. Consideremos los grupos $(\mathbb{Z}, +)$, $(\mathbb{R}, +)$, $(GL(n), \cdot)$, entonces el grupo producto consta del conjunto $\mathbb{Z} \times \mathbb{R} \times GL(n)$, dotado de la operación binaria $\cdot : (\mathbb{Z} \times \mathbb{R} \times GL(n)) \times (\mathbb{Z} \times \mathbb{R} \times GL(n)) \rightarrow (\mathbb{Z} \times \mathbb{R} \times GL(n))$, definida por $\cdot((n, \alpha, A), (m, \beta, B)) = (n, \alpha, A) \cdot (m, \beta, B) := (n + m, \alpha + \beta, A \cdot B)$.

8.1.2. Producto Fibrado. Relacionada con el producto directo está el llamado producto fibrado de grupos. Éste resulta como un subgrupo del producto directo de dos grupos.

Sean G, G_1, G_2 grupos y

$$\varphi_1 : G_1 \rightarrow G, \quad \varphi_2 : G_2 \rightarrow G$$

homomorfismos. Definimos el *producto fibrado* sobre G , de los grupos G_1, G_2 , como el grupo $(G_1 \times_G G_2, \cdot, p_1, p_2)$, donde $G_1 \times_G G_2$ es el subgrupo de $G_1 \times G_2$:

$$G_1 \times_G G_2 := \{(g_1, g_2) \in G_1 \times G_2 \mid \varphi_1(g_1) = \varphi_2(g_2)\}$$

y p_1, p_2 son las restricciones de las proyecciones sobre G_1 y G_2 respectivamente.

Se tiene entonces el siguiente diagrama comutativo:

(8.5)

$$\begin{array}{ccccc} & & G_1 & & \\ & \swarrow \varphi_1 & & \searrow p_1 & \\ G & & G_1 \times_G G_2 & & \\ & \uparrow \varphi_2 & & \downarrow p_2 & \\ & & G_2 & & \end{array}$$

El producto fibrado posee la siguiente propiedad universal: Dado un grupo H y homomorfismos ψ_1, ψ_2 , tales que el diagrama

(8.6)

$$\begin{array}{ccc} & H & \\ \swarrow \psi_1 & & \searrow \psi_2 \\ G_1 & & G_2 \\ \downarrow \varphi_1 & & \downarrow \varphi_2 \\ G & & \end{array}$$

sea comutativo, entonces existe un único homomorfismo

$$\psi : H \rightarrow G_1 \times_G G_2$$

que hace commutar al diagrama

(8.7)

$$\begin{array}{ccccc} & & G_1 & & \\ & \swarrow \varphi_1 & & \searrow p_1 & \\ G & & G_1 \times_G G_2 & & H \\ & \uparrow \varphi_2 & & \downarrow \psi & \\ & & G_2 & & \end{array}$$

Se suele decir que

(8.8)

$$\begin{array}{ccc} & G_1 & \\ & \swarrow p_1 & \\ G_1 \times_G G_2 & & \\ & \searrow p_2 & \\ & G_2 & \end{array}$$

es el “Pull-Back” de

(8.9)

$$\begin{array}{ccc} G_1 & & G_2 \\ \swarrow \varphi_1 & & \searrow \varphi_2 \\ G & & \end{array}$$

El lector comprobará que, por la propiedad universal, dado un diagrama de la forma (8.9), el pull-back correspondiente es único, salvo isomorfismo. Por consiguiente el producto fibrado es único, salvo isomorfismo.

8.1.3. Suma Directa de Grupos Abelianos. Sea $(A_i)_{i \in I}$ una familia de grupos abelianos. Por simplicidad denotaremos por $+$ la operación en cada grupo A_i y por 0 el elemento neutro respectivo. Si

$$A = \prod_{i \in I} A_i$$

es el producto directo de la familia $(A_i)_{i \in I}$, consideremos el subgrupo

$$\bigoplus_{i \in I} A_i$$

formado por los elementos $g = (g_i)_{i \in I} \in A$, tal que $g_i = 0$, salvo para un número finito de índices $i \in I$. Para cada índice $j \in I$, sea

$$\lambda_j : A_j \rightarrow \bigoplus_{i \in I} A_i$$

la aplicación tal que la j -componente de $\lambda_j(g) = g$ y el resto de las componentes es 0 , entonces λ_j es un homomorfismo de grupos, $\forall j \in I$.

$$\left(\bigoplus_{i \in I} A_i, +, \lambda_i \right)_i \in I$$

Se llama *la suma directa* de la familia de grupos abelianos $(A_i)_{i \in I}$.

En forma análoga al producto directo, la suma directa posee la siguiente propiedad universal:

Dada una familia de homomorfismos de grupos abelianos

$$(\psi_i : A_i \rightarrow H)_{i \in I},$$

existe un único homomorfismo

$$\psi : \bigoplus_{i \in I} A_i \rightarrow H,$$

tal que, $\forall i \in I$, el diagrama

$$(8.10) \quad \begin{array}{ccc} A_i & \xrightarrow{\lambda_i} & \bigoplus_{i \in I} A_i \\ \psi_i \downarrow & \nearrow \psi & \\ H & & \end{array}$$

es comutativo.

En efecto, el lector comprobará fácilmente que la aplicación

$$\psi : \bigoplus_{i \in I} A_i \rightarrow H$$

definida por

$$\psi(g) := \sum_{i \in I} \psi_i(g_i)$$

es un homomorfismo y que es el único que hace comutativo al diagrama (8.10).

Dada una familia de homomorfismos de grupos abelianos

$$(\varphi_i : A_i \rightarrow G)_{i \in I}$$

tal que

$$(G, +, \varphi_i)_{i \in I}$$

posee la propiedad universal arriba indicada, entonces

$$(G, +, \varphi_i)_{i \in I}$$

es isomorfo a

$$\left(\bigoplus_{i \in I} A_i, +, \lambda_i \right)_{i \in I}$$

Esto quiere decir que la suma directa es única, salvo isomorfismo. Dejamos al lector la demostración de esta propiedad, ya que es similar a la demostración de la unicidad del producto directo.

Si I es un conjunto finito de índices, entonces la suma directa y el producto directo coinciden, como el lector comprobará fácilmente.

8.1.4. Suma Fibrada. Dual al producto fibrado se tiene para grupos abelianos la llamada suma fibrada, obtenida como cociente de la suma directa con un subgrupo determinado.

Sean A, A_1, A_2 grupos abelianos y

$$\varphi_1 : A \rightarrow A_1, \quad \varphi_2 : A \rightarrow A_2$$

homomorfismos. Al grupo $(A_1 \oplus_A A_2, +, i_1, i_2)$, donde $A_1 \oplus_A A_2$ es el grupo cociente

$$A_1 \oplus_A A_2 := (A_1 \oplus A_2)/W,$$

donde W es el subgrupo de $A_1 \oplus A_2$ generado por los elementos de la forma $(\varphi_1(g_1), \varphi_2(g_2))$, i_1, i_2 son los homomorfismos inducidos por los homomorfismos φ_1, φ_2 respectivamente, lo llamamos la *suma fibrada* sobre A , de los grupos A_1, A_2 . Se tiene, entonces, el siguiente diagrama comutativo:

(8.11)

$$\begin{array}{ccccc} & & A_1 & & \\ & \varphi_1 \nearrow & & \searrow i_1 & \\ A & & & & A_1 \oplus_A A_2 \\ & \varphi_2 \searrow & & \nearrow i_2 & \\ & & A_2 & & \end{array}$$

La suma fibrada posee la siguiente propiedad universal: Dado un grupo abeliano H y homomorfismos ψ_1, ψ_2 , tales que el diagrama

(8.12)

$$\begin{array}{ccccc} & & H & & \\ & \psi_1 \nearrow & & \searrow \psi_2 & \\ A_1 & & & & A_2 \\ & \varphi_1 \swarrow & & \nearrow \varphi_2 & \\ & & A & & \end{array}$$

sea comutativo, entonces existe un único homomorfismo

$$\psi : A_1 \oplus_A A_2 \rightarrow H,$$

que hace conmutar al diagrama

(8.13)

$$\begin{array}{ccccc}
 & & A_1 & & \\
 & \varphi_1 \nearrow & \swarrow i_1 & \psi_1 \searrow & \\
 A & & A_1 \oplus_A A_2 & \xrightarrow{\psi} & H \\
 & \varphi_2 \searrow & \swarrow i_2 & \psi_2 \nearrow & \\
 & & A_2 & &
 \end{array}$$

También se dice que el diagrama

(8.14)

$$\begin{array}{ccc}
 A_1 & & \\
 & \searrow i_1 & \\
 & A_1 \oplus_A A_2 & \\
 & \swarrow i_2 & \\
 A_2 & &
 \end{array}$$

es un “Push-Out” del diagrama

(8.15)

$$\begin{array}{ccc}
 A_1 & & A_2 \\
 & \swarrow \varphi_1 & \nearrow \varphi_2 \\
 A & &
 \end{array}$$

En forma análoga al pull-back, por la propiedad universal, el push-out del diagrama (8.15) es único salvo isomorfismo, por lo que, en consecuencia, la suma fibrada es única salvo isomorfismo.

8.2. Grupos Libres

En esta sección estudiaremos la construcción de los llamados grupos libres. Estos son grupos que tienen como “base” los elementos de un conjunto dado S . Los grupos libres juegan un papel muy importante en la lingüística matemática, así como en la topología y geometría algebraicas.

Empezaremos esta sección con la construcción del grupo libre abeliano sobre un conjunto cualquiera, no vacío S , por ser más sencilla que la construcción del grupo libre en el caso no abeliano. A partir del grupo libre abeliano construiremos también el llamado K -grupo de Grothendieck.

8.2.1. Grupo Libre Abeliano. Sea S un conjunto no vacío y

$$\varphi : S \rightarrow \mathbb{Z}$$

una aplicación, tal que $\varphi(s) = 0$, salvo un número finito de elementos de S . Entonces, si

$$\mathbf{s}_j : S \rightarrow \mathbb{Z}$$

es la aplicación, tal que $\mathbf{s}_j(s) = 0$, si $s \neq s_j$ y $\mathbf{s}_j(s_j) = 1$, entonces φ se puede escribir de la forma

$$\varphi = k_1 \mathbf{s}_1 + \cdots + k_n \mathbf{s}_n,$$

donde los $k_\nu \in \mathbb{Z}$, $\forall \nu = 1, \dots, n$.

De forma más general podemos escribir

$$\varphi = \sum_{s \in S} k_s \mathbf{s},$$

donde $k_s = 0$, salvo para un número finito de elementos $s \in S$, y

$$\mathbf{s} : S \rightarrow \mathbb{Z}$$

la aplicación tal que

$$\mathbf{s}(x) = \begin{cases} 1 & \text{si } x = s, \\ 0 & \text{de lo contrario.} \end{cases}$$

φ admite una única representación de esta forma. En efecto, supongamos que

$$\varphi = \sum_{s \in S} k_s \mathbf{s} = \sum_{s \in S} k'_s \mathbf{s}$$

entonces

$$0 = \sum_{s \in S} (k_s - k'_s) \mathbf{s}$$

y por consiguiente $k_s = k'_s$, $\forall s \in S$.

Sea

$$\mathbb{Z}\langle S \rangle := \{\varphi : S \rightarrow \mathbb{Z} \mid \varphi(s) = 0, \text{ salvo un número finito de elementos } s \in S\}$$

entonces $(\mathbb{Z}\langle S \rangle, +)$, donde $+$ es la adición usual de aplicaciones sobre \mathbb{Z} , es un grupo abeliano.

Por medio de la aplicación inyectiva

$$f : S \rightarrow \mathbb{Z}\langle S \rangle$$

definida por $f(s) := \mathbf{s}$, podemos identificar a S como un subconjunto de $\mathbb{Z}\langle S \rangle$ y el grupo $\mathbb{Z}\langle S \rangle$ está generado por $f[S]$.

$(\mathbb{Z}\langle S \rangle, +, f)$ se llama el *grupo libre abeliano* generado por el conjunto S ,

Usualmente se suele identificar S con $f[S]$ en $\mathbb{Z}\langle S \rangle$ y representar los elementos de $\mathbb{Z}\langle S \rangle$, como las “sumas formales”

$$\sum_{s \in S} k_s s.$$

El grupo libre abeliano $(\mathbb{Z}\langle S \rangle, +, f)$ posee la siguiente propiedad universal:

Dada una aplicación

$$g : S \rightarrow A,$$

donde A es un grupo abeliano, entonces existe un único homomorfismo

$$g_* : \mathbb{Z}\langle S \rangle \rightarrow A,$$

tal que el diagrama

$$(8.16) \quad \begin{array}{ccc} S & \xrightarrow{f} & \mathbb{Z}\langle S \rangle \\ g \downarrow & \nearrow g_* & \\ A & & \end{array}$$

es comunitativo.

En efecto

$$g_* : \mathbb{Z}\langle S \rangle \rightarrow A$$

definida por

$$g_* \left(\sum_{s \in S} k_s s \right) := \sum_{s \in S} k_s g(s)$$

es el único homomorfismo que hace commutar al diagrama.

De la propiedad universal resulta, como el lector podrá comprobar, la unicidad, salvo isomorfismo, del grupo abeliano libre.

TEOREMA 8.1. *Si $g : S \rightarrow S'$ es una aplicación entre dos conjuntos y $(\mathbb{Z}\langle S \rangle, +, f)$, $(\mathbb{Z}\langle S' \rangle, +, f')$ los respectivos grupos libres abelianos, entonces existe un único homomorfismo de grupos $g_* : \mathbb{Z}\langle S \rangle \rightarrow \mathbb{Z}\langle S' \rangle$, tal que el diagrama*

$$(8.17) \quad \begin{array}{ccc} S & \xrightarrow{f} & \mathbb{Z}\langle S \rangle \\ g \downarrow & & \downarrow g_* \\ S' & \xrightarrow{f'} & \mathbb{Z}\langle S' \rangle \end{array}$$

es commutativo y si g es sobreyectiva también lo será g_* .

DEMOSTRACIÓN. En efecto, tenemos una aplicación

$$(f' \circ \lambda) : S \rightarrow \mathbb{Z}\langle S' \rangle$$

y por la propiedad universal existe un único homomorfismo $\lambda_* := (f' \circ \lambda)_*$ que hace commutar al diagrama (8.16), con $A := \mathbb{Z}\langle S' \rangle$ y el cual hace commutar también al diagrama (8.17).

□

En el caso en que S es un conjunto finito de n elementos, el lector comprobará facilmente que

$$\mathbb{Z}\langle S \rangle \approx \underbrace{\mathbb{Z} \times \cdots \times \mathbb{Z}}_n \approx \underbrace{\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}}_n$$

que es la parte libre de torsión de un grupo abeliano finitamente generado, como vimos en el capítulo precedente.

En la topología y geometría algebraicas juegan un papel muy importante los grupos de ciclos, que son grupos libres abelianos generados por el conjunto de caminos cerrados sobre un espacio topológico o sobre una variedad topológica o algebraica. También son de mucha importancia los grupos libres abelianos sobre el conjunto de los llamados simplicios singulares sobre un espacio topológico, los cuales dan origen a los llamados grupos de homología y cohomología en la topología y geometría algebraicas.

8.2.2. Grupo de Grothendieck. Otro grupo importante, construido a partir de un grupo libre abeliano, es el *K-grupo de Grothendieck*, el cual da origen a la llamada *K-teoría*. Este grupo se construye a partir de un semigrupo abeliano (A, \cdot) y el grupo libre abeliano $(\mathbb{Z}\langle A \rangle, +, f)$. Si $E\langle A \rangle$ es el subgrupo de $\mathbb{Z}\langle A \rangle$, generado por los elementos de la forma $\mathbf{a} + \mathbf{b} - \mathbf{a} \cdot \mathbf{b}$, $a, b \in A$, entonces se define el *K-grupo de Grothendieck*, como el grupo $(K\langle A \rangle, +, \hat{f})$, donde $K\langle A \rangle$ es el grupo cociente

$$K\langle A \rangle := \mathbb{Z}\langle A \rangle / E\langle A \rangle.$$

y $\hat{f} := (\pi \circ f)$.

$(K\langle A \rangle, +, \hat{f})$ posee la siguiente propiedad universal: Dado un homomorfismo de semigrupos abelianos

$$\varphi : A \rightarrow G,$$

donde G es un grupo abeliano, existe un único homomorfismo de grupos abelianos

$$\varphi_* : K\langle A \rangle \rightarrow G$$

tal que el diagrama

(8.18)

$$\begin{array}{ccc} A & \xrightarrow{\varphi} & G \\ \hat{f} \downarrow & \nearrow \varphi_* & \\ K\langle A \rangle & & \end{array}$$

es comutativo.

Además, en analogía al grupo libre abeliano, si (B, \cdot) es otro semigrupo y

$$\psi : A \rightarrow B$$

un homomorfismo de semigrupos, entonces existe un único homomorfismo de grupos

$$\psi_* : K\langle A \rangle \rightarrow K\langle B \rangle$$

tal que el diagrama

(8.19)

$$\begin{array}{ccc} A & \xrightarrow{\hat{f}} & K\langle A \rangle \\ \psi \downarrow & & \downarrow \psi_* \\ B & \xrightarrow{\hat{g}} & K\langle B \rangle \end{array}$$

es comutativo y si ψ es sobreyectiva también lo será ψ_* .

En la K -teoría topológica, el semigrupo (A, \oplus) consiste de todas las clases de equivalencia de los fibrados vectoriales sobre un espacio topológico X , donde \oplus es la operación inducida por la suma de Whitney de dos fibrados vectoriales. Ver, por ejemplo, [3].

8.2.3. Grupo Libre (caso general). Haremos la construcción del grupo libre, en el caso general, no necesariamente comutativo, siguiendo la construcción de Jaques Tits y transcrita por Serge Lang en [15]. Esta construcción es bastante abstracta, pero es aplicable para cualquier conjunto S de cualquier cardinalidad.

Nuestro objetivo es, dado un conjunto cualquiera S , construirnos un grupo $F\langle S \rangle$ y una aplicación

$$f_S : S \rightarrow F\langle S \rangle$$

inyectiva, que satisfaga la siguiente propiedad universal: Dada una aplicación

$$g : S \rightarrow G$$

donde G es un grupo cualquiera, exista un único homomorfismo de grupos

$$g_* : F\langle S \rangle \rightarrow G$$

que haga commutar al diagrama

(8.20)

$$\begin{array}{ccc} S & \xrightarrow{f_S} & F\langle S \rangle \\ g \downarrow & \nearrow g_* & \\ G & & \end{array}$$

$(F\langle S \rangle, \cdot, f_S)$ lo llamaremos el *grupo libre* sobre el conjunto S , el cual será único salvo isomorfismo, por satisfacer la propiedad universal arriba indicada. Dejamos al lector la confirmación de esta afirmación. Empecemos con un lema:

LEMA 8.2. *Existe un conjunto I y una familia de grupos $(G_i)_{i \in I}$, tales que si $g : S \rightarrow G$ es una aplicación de un conjunto S en un grupo G y G es generado por $g[S]$, entonces G es isomorfo a algún G_i .*

DEMOSTRACIÓN. Sea T un conjunto infinitamente contable si S es finito y de la misma cardinalidad de S si S es infinito. Para cada subconjunto $H \subseteq T$, $H \neq \emptyset$, sea Γ_H el conjunto de todas las estructuras de grupo sobre H . Para cada $\gamma \in \Gamma_H$, H_γ representará al conjunto H dotado de la estructura de grupo γ . (Dos estructuras γ, γ' serán consideradas iguales, si H_γ es isomorfo a $H_{\gamma'}$). Entonces la familia $(H_\gamma)_{\gamma \in \Gamma_H}$, donde H recorre todos los elementos de $\mathcal{P}(T) \setminus \{\emptyset\}$ es la familia buscada. \square

Construcción de $F\langle S \rangle$:

Sea $(G_i)_{i \in I}$ una familia de grupos, satisfaciendo las condiciones del lema 8.2 y, para cada $i \in I$, sea M_i el conjunto de todas las aplicaciones de S en G_i . Para cada $\phi \in M_i$, sea $G_{i,\phi} := G_i \times \{\phi\}$, de modo tal que $G_{i,\phi}$ no es otra cosa que el grupo G_i indizado por ϕ . Sea

$$F_0 := \prod_{i \in I} \prod_{\phi \in M_i} G_{i,\phi}$$

El grupo producto de los $G_{i,\phi}$. Definimos una aplicación

$$f_0 : S \rightarrow F_0$$

como la aplicación tal que la componente (i, ϕ) es $(f_0(s))_{i,\phi} := \phi(s)$, $\phi \in M_i$. f_0 es inyectiva, ya que si $s \neq s'$, para un G_i con más de dos elementos, siempre existirá un $\phi \in M_i$, tal que $\phi(s) \neq \phi(s')$. Vamos a mostrar que, dada una aplicación

$$g : S \rightarrow G,$$

donde G es un grupo, existe un homomorfismo de grupos

$$\psi_* : F_0 \rightarrow G$$

tal que el diagrama

$$(8.21) \quad \begin{array}{ccc} S & \xrightarrow{f_0} & F_0 \\ g \downarrow & \nearrow \psi_* & \\ G & & \end{array}$$

es comutativo. Sin limitación de la generalidad podemos asumir que G está generado por $g[S]$, restringiendo nuestra atención, en caso contrario al subgrupo de G generado por $g[S]$. Entonces por el lema 8.2, para algún $i \in I$ existe un isomorfismo

$$\lambda : G \rightarrow G_i$$

y $\psi := (\lambda \circ g) \in M_i$. Si $\pi_{i,\phi}$ es la proyección sobre la componente (i, ϕ) y $\psi_* := (\lambda^{-1} \circ \pi_{i,\phi})$, se obtiene el siguiente diagrama comutativo:

$$(8.22) \quad \begin{array}{ccc} S & \xrightarrow{f_0} & F_0 \\ g \downarrow & \nearrow \psi_* & \downarrow \pi_{i,\phi} \\ G & \xrightarrow[\lambda]{} & G_{i,\phi} \end{array}$$

Si definimos $F\langle S \rangle$ como el subgrupo de F_0 generado por $f_0[S]$, $f_S := f_0$ y g_* como la restricción de ψ_* a $F\langle S \rangle$, entonces $(F\langle S \rangle, \cdot, f_S)$ cumple con la propiedad universal deseada y g_* es el único homomorfismo que hace commutar al diagrama (8.20).

El lector comprobará facilmente que, en forma análoga al grupo libre abeliano, si

$$\lambda : S \rightarrow S'$$

es una aplicación entre dos conjuntos S y S' , entonces existe un único homomorfismo de grupos

$$\lambda_* : F\langle S \rangle \rightarrow F\langle S' \rangle$$

tal que el diagrama

$$(8.23) \quad \begin{array}{ccc} S & \xrightarrow{f_S} & F\langle S \rangle \\ \lambda \downarrow & & \downarrow \lambda_* \\ S' & \xrightarrow{f_{S'}} & F\langle S' \rangle \end{array}$$

es comutativo y si λ es sobreyectiva, también lo será λ_* .

Si G es un grupo y S el mismo conjunto que G desprovisto de la estructura de grupo, se tiene la aplicación identidad

$$1_G : S \rightarrow G$$

la cual es una biyección e induce un homomorfismo de grupos sobreyectivo

$$1_* : F\langle S \rangle \rightarrow G.$$

Por consiguiente todo grupo G es cociente de un grupo libre.

8.2.4. Coproducto de Grupos. Dada una familia de grupos no abelianos, $(G_i)_{i \in I}$, buscamos un grupo

$$\coprod_{i \in I} G_i$$

y una familia de homomorfismos

$$(\lambda_i : G_i \rightarrow \coprod_{i \in I} G_i)_{i \in I}$$

que posea la siguiente propiedad universal: dada una familia de homomorfismos de grupos

$$(\psi_i : G_i \rightarrow H)_{i \in I}$$

exista un único homomorfismo

$$\psi : \coprod_{i \in I} G_i \rightarrow H$$

tal que, $\forall i \in I$, haga commutar al diagrama

$$(8.24) \quad \begin{array}{ccc} G_i & \xrightarrow{\lambda_i} & \coprod_{i \in I} G_i \\ \psi_i \downarrow & \nearrow \psi & \\ H & & \end{array}$$

Vamos a mostrar que dicho grupo existe y a

$$(\coprod_{i \in I} G_i, \cdot, \lambda_i)_{i \in I}$$

lo llamaremos el *coproducto* de la familia $(G_i)_{i \in I}$. Como el lector habrá notado, la propiedad universal que cumple el coproducto de una familia de grupos no abelianos es la misma que la que satisface la suma directa de una familia de grupos abelianos.

La construcción, en el caso general, es similar a la construcción del grupo libre y es bastante abstracta. Sin embargo, en el caso finito, veremos una construcción más intuitiva, tanto del coproducto como del grupo libre.

Dada una familia de grupos $(G_i)_{i \in I}$, para cada índice i , sea S_i un conjunto igual a G_i , si G_i es infinito y S_i un conjunto contable si G_i es finito. Sea S un conjunto de cardinalidad igual a la unión disjunta de todos los S_i . Sea Γ el conjunto de todas las estructuras de grupo sobre S y para cada $\gamma \in \Gamma$, sea Φ_γ el conjunto de todas las familias de homomorfismos

$$\varphi := \{\varphi_i : G_i \rightarrow S_\gamma\}.$$

Dado $\gamma \in \Gamma$, $\varphi \in \Phi_\gamma$, definimos $S_{\gamma, \varphi} := (S_\gamma, \varphi)$, es decir el grupo S_γ indizado por φ .

Sea

$$F_0 := \prod_{\gamma \in \Gamma} \prod_{\varphi \in \Phi_\gamma} S_{\gamma, \varphi}$$

y para cada i , definimos un homomorfismo

$$f_i : G_i \rightarrow F_0$$

por medio de $f_i(g_i)_{\gamma, \varphi} := \varphi_i(g_i)$, $\forall g_i \in G_i$.

Sea ahora $\psi := \{\psi_i : G_i \rightarrow H\}$ una familia de homomorfismos de grupos. Sin limitación de la generalidad supondremos que H es generado por las imágenes de ψ_i , (en caso contrario nos restringimos al subgrupo de H generado por estas imágenes), entonces $\text{card}(H) \leq \text{card}(S)$, ya que todo elemento de G es producto finito de imágenes de elementos de S . Nuevamente, sin limitación de la generalidad, podemos asumir que $\text{card}(H) = \text{card}(S)$, pues en caso contrario consideramos el grupo

$$\tilde{H} := H \times \mathbf{Z},$$

donde \mathbf{Z} es el producto de suficientes copias de \mathbb{Z} , hasta obtener la cardinalidad deseada. Vamos a mostrar que existe un homomorfismo

$$\psi_* : F_0 \rightarrow H$$

tal que, $\forall i$, el diagrama

$$(8.25) \quad \begin{array}{ccc} H & \xrightarrow{f_i} & F_0 \\ \downarrow \psi_i & \nearrow \psi_* & \\ H & & \end{array}$$

sea comutativo.

Como $\text{card } H = \text{card } S$, existe $\gamma \in \Gamma$, y un isomorfismo

$$\phi_0 : H \rightarrow S_\gamma,$$

Entonces $\phi := \{\phi_0 \circ \psi_i : G_i \rightarrow S_\gamma\} \in \Phi_\gamma$ y definimos ψ_* como la proyección de F_0 sobre $S_{\gamma, \phi}$.

Si definimos $\coprod_{i \in I} G_i$ como el subgrupo de F_0 generado por $\bigcup_{i \in I} f_i[G_i]$, y $\lambda_i := f_i$, $\forall i \in I$, entonces la restricción ψ de ψ_* sobre $\coprod_{i \in I} G_i$, es el único homomorfismo que hace commutar al diagrama (8.24).

8.2.5. Producto Libre y Producto Amalgamado. Dada una familia finita de grupos $\{G_1, \dots, G_n\}$, vamos a construir el llamado *producto libre* de éstos y el *producto amalgamado* de dos grupos como un grupo cociente del producto libre. Vamos a hacer ver que el producto libre de los grupos de la familia $\{G_1, \dots, G_n\}$, es isomorfo al coproducto $\coprod_{i=1}^n G_i$ y que el grupo libre sobre un conjunto finito S es isomorfo al producto libre de un número finito de grupos adecuados.

Sean G, H dos grupos, tales que $G \cap H = \{e\}$, vamos a construir un grupo $G * H$, que contenga a G y a H como subgrupos y tal que cada elemento distinto de e posea una única representación como un producto

$$a_1 \cdot a_2 \cdots a_n \quad (n \geq 1, a_v \neq e, \forall v),$$

donde $a_v \in G$ o $a_v \in H$, y tal que si $a_v \in G$, entonces $a_{v+1} \in H$ y si $a_v \in H$, entonces $a_{v+1} \in G$.

Sea $G * H$ el conjunto de todas las sucesiones finitas

$$\mathbf{a} := (a_1, \dots, a_n) \quad (n \geq 0)$$

tal que, ya sea que $n = 0$ y en tal caso la sucesión es vacía, o $n \geq 1$ y los elementos de la sucesión pertenecen, de forma alterna, a G o a H y son distintos de e .

Dadas dos sucesiones $\mathbf{a} := (a_1, \dots, a_n), \mathbf{b} := (b_1, \dots, b_m) \in G * H$, definimos

$$\mathbf{a} \cdot \mathbf{b} := \begin{cases} (a_1, \dots, a_n, b_1, \dots, b_m) & \text{si } a_n \in G, b_1 \in H, \text{o } a_n \in H, b_1 \in G \\ (a_1, \dots, a_n b_1, \dots, b_m) & \text{si } a_n, b_1 \in G, \text{o } a_n, b_1 \in H, a_n b_1 \neq e \\ (a_1, \dots, a_{n-1})(b_2, \dots, b_m) & \text{si } a_n, b_1 \in G, \text{o } a_n, b_1 \in H, a_n b_1 = e \end{cases}$$

La sucesión vacía será el elemento neutro en $G * H$ y obviamente

$$(a_1, \dots, a_n)(a_n^{-1}, \dots, a_1^{-1}) = e$$

Falta probar que el producto, así definido, es asociativo. Sea $\mathbf{c} := (c_1, \dots, c_r)$. El lector comprobará fácilmente que si $n = 0$ o $m = 0$ o $r = 0$, la asociatividad vale. Consideremos, entonces, el caso $m = 1$, es decir $\mathbf{b} = (x), x \in G$ y verifiquemos que en cada caso posible $(\mathbf{a} \cdot \mathbf{b}) \cdot \mathbf{c} = \mathbf{a} \cdot (\mathbf{b} \cdot \mathbf{c})$. Los casos son los siguientes:

$$\begin{aligned} (a_1, \dots, a_n, x, c_1, \dots, c_r) & \quad \text{si } a_n \in H, c_1 \in H \\ (a_1, \dots, a_n x, c_1, \dots, c_r) & \quad \text{si } a_n \in G, a_n x \neq e, c_1 \in H \\ (a_1, \dots, a_n, x c_1, \dots, c_r) & \quad \text{si } a_n \in H, c_1 \in G, x c_1 \neq e \\ (a_1, \dots, a_{n-1})(c_1, \dots, c_r) & \quad \text{si } a_n = x^{-1}, c_1 \in H \\ (a_1, \dots, a_n)(c_2, \dots, c_r) & \quad \text{si } a_n \in H, c_1 = x^{-1} \\ (a_1, \dots, a_n x c_1, \dots, c_r) & \quad \text{si } a_n, c_1 \in G, a_n x c_1 \neq e \\ (a_1, \dots, a_{n-2})(c_2, \dots, c_r) & \quad \text{si } a_n, c_1 \in G, a_n x c_1 = e \end{aligned}$$

En forma análoga si $x \in H$. Procedamos ahora, para $m \geq 2$, por inducción. Sea \mathbf{b} una sucesión de longitud m , entonces podemos escribir $\mathbf{b} = \mathbf{b}_1 \cdot \mathbf{b}_2$, donde \mathbf{b}_1 y \mathbf{b}_2 poseen longitudes menores que m . Entonces

$$\begin{aligned} (\mathbf{a} \cdot \mathbf{b}) \cdot \mathbf{c} &= (\mathbf{a} \cdot (\mathbf{b}_1 \cdot \mathbf{b}_2)) \cdot \mathbf{c} = ((\mathbf{a} \cdot \mathbf{b}_1) \cdot \mathbf{b}_2) \cdot \mathbf{c} = (\mathbf{a} \cdot \mathbf{b}_1) \cdot (\mathbf{b}_2 \cdot \mathbf{c}) \\ \mathbf{a} \cdot (\mathbf{b} \cdot \mathbf{c}) &= \mathbf{a} \cdot ((\mathbf{b}_1 \cdot \mathbf{b}_2) \cdot \mathbf{c}) = \mathbf{a} \cdot (\mathbf{b}_1 \cdot (\mathbf{b}_2 \cdot \mathbf{c})) = (\mathbf{a} \cdot \mathbf{b}_1) \cdot (\mathbf{b}_2 \cdot \mathbf{c}) \end{aligned}$$

lo que muestra la asociatividad.

Por otra parte se tienen inyecciones

$$i : G \rightarrow G * H \quad \text{y} \quad j : H \rightarrow G * H$$

definidas por $i(g) := (g)$ y $j(h) := (h)$

Al grupo $(G * H, \cdot, i, j)$ lo llamamos el *producto libre de G y H*

El lector comprobará facilmente la siguiente propiedad universal del producto libre:
Si se tienen homomorfismos de grupos

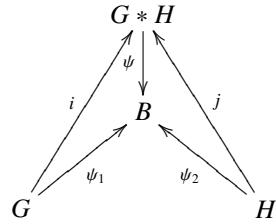
$$\psi_1 : G \rightarrow B \quad \psi_2 : H \rightarrow B$$

entonces existe un único homomorfismo

$$\psi : G * H \rightarrow B$$

que hace commutar al diagrama

(8.26)



donde ψ es el homomorfismo que a una sucesión a le aplica de forma alterna ψ_1, ψ_2 . Dejamos al lector la tarea de comprobar que, en efecto, ψ es un homomorfismo y que $G * H$ satisface la misma propiedad universal que $G \coprod H$, por lo que $G * H$ y $G \coprod H$ son isomorfos.

El producto libre se puede generalizar facilmente a una familia finita de grupos $\{G_1, \dots, G_n\}$, con $G_i \cap G_j = e$, si $i \neq j$, tomando como $G_1 * \dots * G_n$ el conjunto de todas las sucesiones finitas cuyos elementos son, de forma alterna, elementos de los G_i y el producto definido siguiendo el mismo esquema que describimos arriba. Tarea que también dejaremos al lector como ejercicio, así como la de demostrar que

$$G_1 * \dots * G_n \approx \coprod_{i=1}^n G_i$$

mostrando que con las inclusiones respectivas

$$\lambda_i : G_i \rightarrow G_1 * \dots * G_n,$$

donde $\lambda_i(g_i) := (g_i) \in G_1 * \dots * G_n$, el grupo $(G_1 * \dots * G_n, \cdot, \lambda_i)_{i=1, \dots, n}$ satisface la misma propiedad universal que el coproducto.

En analogía a la suma fibrada que definimos para grupos abelianos, definiremos ahora el llamado *producto amalgamado* o *suma amalgamada* de grupos.

Dados tres grupos G, G_1, G_2 y homomorfismos

$$\varphi_1 : G \rightarrow G_1 \quad \varphi_2 : G \rightarrow G_2$$

buscamos construir un grupo $G_1 *_G G_2$ y homomorfismos

$$i_1 : G_1 \rightarrow G *_G G_2 \quad i_2 : G_2 \rightarrow G *_G G_2$$

que haga commutativo al siguiente diagrama

(8.27)

$$\begin{array}{ccc} & G_1 & \\ \varphi_1 \nearrow & & \searrow i_1 \\ G & & G_1 *_G G_2 \\ \varphi_2 \searrow & & \nearrow i_2 \\ & G_2 & \end{array}$$

Si W es el subgrupo normal más pequeño de $G_1 * G_2$, que contiene al grupo generado por los todos los elementos de la forma $(\varphi_1(g), \varphi_2(g)^{-1})$, entonces el grupo $G_1 *_G G_2 := (G_1 * G_2)/W$ y los homomorfismos i_1, i_2 inducidos por las inclusiones respectivas de G_1 y G_2 en $G_1 * G_2$, hacen commutar al diagrama (8.27).

Al grupo $(G_1 *_G G_2, \cdot, i_1, i_2)$ lo llamamos el *producto amalgamado* o *suma amalgamada* sobre G de G_1, G_2 .

El producto amalgamado posee la siguiente propiedad universal: Dado un grupo H y homomorfismos ψ_1, ψ_2 , tales que el diagrama

(8.28)

$$\begin{array}{ccccc} & & H & & \\ & \swarrow \psi_1 & & \searrow \psi_2 & \\ G_1 & & & & G_2 \\ \varphi_1 \nearrow & & & & \searrow \varphi_2 \\ & G & & & \end{array}$$

sea commutativo, entonces existe un único homomorfismo

$$\psi : G_1 *_G G_2 \rightarrow H,$$

que hace commutar al diagrama

(8.29)

$$\begin{array}{ccccc} & G_1 & & & \\ \varphi_1 \nearrow & & \searrow i_1 & & \swarrow \psi_1 \\ G & & G_1 *_G G_2 & & H \\ \varphi_2 \searrow & & \nearrow i_2 & & \swarrow \psi_2 \\ & G_2 & & & \end{array}$$

Entonces el diagrama

(8.30)

$$\begin{array}{ccc} G_1 & & \\ & \searrow i_1 & \\ & G_1 *_G G_2 & \\ & \nearrow i_2 & \\ G_2 & & \end{array}$$

es un “Push-Out” del diagrama

$$(8.31) \quad \begin{array}{ccc} G_1 & & G_2 \\ \varphi_1 \swarrow & & \searrow \varphi_2 \\ & G & \end{array}$$

y por consiguiente es producto amalgamado es único salvo isomorfismo.

En el caso en que los grupos sean todos abelianos, entonces el producto amalgamado es isomorfo a la suma fibrada, pues serían push-outs del mismo diagrama.

El producto amalgamado juega un papel muy importante en la topología algebraica, en particular en la teoría de la homotopía, pues por el teorema de Van Kampen, el *grupo fundamental* $\pi_1(Z)$ de un espacio topológico Z que es unión de dos subconjuntos abiertos X_1, X_2 , tales que $A := X_1 \cap X_2$ sea no vacío y conexo por caminos, es el producto amalgamado de los grupos fundamentales de los X_i , $i = 1, 2$, $\pi_1(X_1), \pi_1(X_2)$ sobre el grupo fundamental de A , $\pi_1(A)$. Ver por ejemplo [25], [10], [8].

Vamos a hacer ver ahora, que si S es un conjunto finito de elementos

$$S := \{x_1, \dots, x_n\},$$

entonces el grupo libre $F\langle S \rangle$ es isomorfo al producto libre $G_1 * \dots * G_n$, donde G_i es el grupo cíclico infinito generado por x_i , $i = 1, \dots, n$.

Por construcción del grupo libre se tiene una inyección

$$f_S : S \rightarrow F\langle S \rangle$$

por lo que podemos identificar S con su imagen $f_S[S] \subseteq F\langle S \rangle$.

Mostremos primeramente el siguiente

LEMA 8.3. *Sea $F\langle S \rangle$ el grupo libre generado por el conjunto S y sean x_1, \dots, x_n elementos distintos de S . Sean v_1, \dots, v_r enteros $\neq 0$ y i_1, \dots, i_r enteros.*

$$1 \leq i_1, \dots, i_r \leq n$$

tales que $i_j \neq i_{j+1}$, para $j = 1, \dots, r-1$. Entonces, en $F\langle S \rangle$

$$x_{i_1}^{v_1} \cdots x_{i_r}^{v_r} \neq e$$

DEMOSTRACIÓN. Sean G_1, \dots, G_n los grupos cíclicos infinitos generados, respectivamente, por los elementos x_1, \dots, x_n y $G := G_1 * \dots * G_n$ y sea

$$g : S \rightarrow G$$

la aplicación definida por $g(x_i) := (x_i) \in G$ y $g(x) := e$, para $x \notin \{x_1, \dots, x_n\}$. Entonces por la propiedad universal del producto libre, g induce un único homomorfismo

$$g_* : F\langle S \rangle \rightarrow G,$$

tal que el diagrama (8.20) sea comutativo. Entonces $g_*(x_{i_1}^{v_1} \cdots x_{i_r}^{v_r}) = x_{i_1}^{v_1} \cdots x_{i_r}^{v_r} \neq e \in G$. Lo que muestra el lema, ya que g_* es un homomorfismo.. \square

Si

$$S := \{x_1, \dots, x_n\},$$

y

$$f : S \rightarrow H$$

una aplicación de S en un grupo H , el lector comprobará, fácilmente, que el homomorfismo

$$f_* : G \rightarrow H$$

definido por $f_*((x_i)) := f(x_i)$ es el único que hace comutar al diagrama

$$(8.32) \quad \begin{array}{ccc} S & \xrightarrow{g} & G \\ f \downarrow & \nearrow f_* & \\ H & & \end{array}$$

Esto quiere decir, que G satisface la misma propiedad universal que $F\langle S \rangle$, en el caso en que S es un conjunto finito y por consiguiente

$$g_* : F\langle S \rangle \rightarrow G_1 * \cdots * G_n$$

es un isomorfismo.

Por lo tanto, en el caso en que S es un conjunto finito el grupo libre sobre S lo obtenemos como el producto libre de los grupos cíclicos infinitos generados por cada elemento de S , lo que nos da una representación más intuitiva del grupo libre.

8.2.6. Ejercicios y Complementos.

1. Comprobar que la definición de grupo producto satisface todos los axiomas de un grupo y que las proyecciones son, en efecto, homomorfismos de grupos.
2. Mostrar que el homomorfismo ψ , que hace comutar al diagrama (8.1), es única.
3. Comprobar que la definición de suma directa satisface todos los axiomas de un grupo y que las inclusiones λ_i son, en efecto, homomorfismos de grupos.
4. Mostrar que el homomorfismo ψ que hace comutar al diagrama (8.10) es única.
5. Mostrar que el producto sobre una familia finita de grupos es isomorfo a la suma directa respectiva.
6. Mostrar que las definiciones de grupo de Groethendieck, producto fibrado, producto directo, suma fibrada, coproducto, producto amalgamado satisfacen los axiomas de un grupo y las propiedades universales respectivas.
7. Mostrar que, en efecto, si S es un conjunto finito, el grupo libre $F\langle S \rangle$ satisface la misma condición universal que el producto libre sobre todos los subgrupos cíclicos infinitos generados por cada elemento $s \in S$.
8. Sea S un conjunto. Siguiendo la terminología y la filosofía de la construcción del grupo abeliano libre, consideremos el conjunto

$$\mathbb{N}\langle S \rangle := \{\varphi : S \rightarrow \mathbb{N} \mid \varphi(s) = 0, \text{ salvo un número finito de elementos } s \in S\}$$

Mostrar que

- a) $(\mathbb{N}\langle S \rangle, +, f)$ es un monoide abeliano, llamado el *monoide libre abeliano*.
- b) El monoide libre abeliano $(\mathbb{N}\langle S \rangle, +, f)$ posee la siguiente propiedad universal:

Dada una aplicación

$$g : S \rightarrow A,$$

donde A es un monoide abeliano, entonces existe un único homomorfismo de monoídes

$$g_* : \mathbb{N}\langle S \rangle \rightarrow A,$$

tal que el diagrama

$$(8.33) \quad \begin{array}{ccc} S & \xrightarrow{f} & \mathbb{N}\langle S \rangle \\ g \downarrow & \nearrow g_* & \\ A & & \end{array}$$

es commutativo.

- c) Si $\lambda : S \rightarrow S'$ es una aplicación entre dos conjuntos y $(\mathbb{N}\langle S \rangle, +, f)$, $(\mathbb{N}\langle S' \rangle, +, f')$ los respectivos monoides libres abelianos, entonces existe un único homomorfismo de monoides $\lambda_* : \mathbb{N}\langle S \rangle \rightarrow \mathbb{N}\langle S' \rangle$, tal que el diagrama

$$(8.34) \quad \begin{array}{ccc} S & \xrightarrow{f} & \mathbb{N}\langle S \rangle \\ \lambda \downarrow & & \downarrow \lambda_* \\ S' & \xrightarrow{f'} & \mathbb{N}\langle S' \rangle \end{array}$$

es commutativo y si λ es sobreyectiva también lo será λ_* .

CAPÍTULO 9

INTRODUCCIÓN A LA TEORÍA DE ANILLOS E IDEALES



FIGURA 9.1. Emie Noether

En este capítulo estudiaremos las estructuras algebraicas con dos operaciones binarias llamadas anillos. En particular trataremos más ampliamente la teoría de los anillos conmutativos con unidad, es decir a anillos cuya segunda operación binaria es conmutativa y posee un elemento neutro.

Por simplicidad en la notación denotaremos la primera operación por ‘+’ y la segunda operación por ‘·’, salvo casos particulares y donde no haya lugar a confusión. Al elemento neutro de la primera operación lo denotaremos por 0 y al elemento *unidad* o elemento neutro de la segunda operación por 1.

9.1. Anillos

Recordamos al lector la definición de anillo dada en el primer capítulo, sección de estructuras algebraicas, definición 2.6, con dos operaciones binarias.

DEFINICIÓN 9.1. Decimos que la estructura algebraica con dos operaciones binarias $(A, +, \cdot)$ es un *anillo*, si $(A, +)$ es un grupo abeliano, (A, \cdot) un semigrupo y se cumplen las relaciones de distributividad siguientes:

$$(9.1) \quad a \cdot (b + c) = a \cdot b + a \cdot c, \text{ y } (a + b) \cdot c = a \cdot c + b \cdot c, \forall a, b, c \in A$$

Si además (A, \cdot) es un monoide, entonces se dice que $(A, +, \cdot)$ es un anillo con *unidad*, y si · es conmutativa, entonces se dice que es un *anillo conmutativo*.

Un elemento a de un anillo A se dice que es un *divisor de cero*, si existe $b \in A$, $b \neq 0$, tal que $a \cdot b = 0$. Si $a \neq 0$, entonces se dice que es un *divisor de cero propio*.

Un anillo conmutativo A , con unidad y sin divisores de cero propios se llama un *dominio entero* o de *integridad*.

Decimos que un elemento $a \in A \setminus \{0\}$ de un anillo con unidad A , es *invertible*, si existe un elemento $a^{-1} \in A$, tal que $a \cdot a^{-1} = a^{-1} \cdot a = 1$.

Decimos que un elemento a de un anillo A posee un *inverso por la derecha*, (*inverso por la izquierda*), si existe $b \in A$, tal que $a \cdot b = 1$, ($b \cdot a = 1$). Entonces un elemento invertible es aquel que posee tanto inverso por la izquierda como por la derecha.

Un anillo conmutativo, con unidad, en el cual todo elemento distinto de 0 es invertible, se llama un *campo* o *cuerpo*.

En un campo $(A, +, \cdot)$, son $(A, +)$ y $(A \setminus \{0\}, \cdot)$ grupos abelianos.

OBSERVACIÓN. En la literatura francesa y alemana se usa más el término de *cuerpo* (*corps*, en francés, *Körper*, en alemán), mientras que en la literatura anglosajona predomina el de *campo* (*field*). En la literatura española hay autores que utilizan indistintamente cualesquiera de los dos términos y otros que reservan el término de *cuerpo* al caso en que $(A \setminus \{0\}, \cdot)$ no es un grupo abeliano. Nosotros utilizaremos el de *campo*, por ser el más común en América Latina y el de *cuerpo* para el caso en que $(A \setminus \{0\}, \cdot)$ no es un grupo conmutativo.

EJEMPLOS 9.1.

1. El lector comprobará fácilmente que los conjuntos $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ con las operaciones de suma y producto usuales, son anillos conmutativos con unidad. Además $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ son campos.
2. El lector también comprobará fácilmente que el subconjunto de \mathbb{C}

$$\mathbb{Z}[i] := \{\alpha \in \mathbb{C} \mid \alpha := x + iy, x, y \in \mathbb{Z}\}$$

dotado de la suma y producto usuales de complejos, es un anillo conmutativo con unidad, llamado el anillo de los *enteros gaussianos*.

3. $(\mathbb{Z}_n, +, \cdot)$ el conjunto de las clases \pmod{n} , dotado de las operaciones binarias definidas por

$$\bar{x} + \bar{y} := \overline{x+y}, \quad \bar{x} \cdot \bar{y} := \overline{xy}, \quad \forall \bar{x}, \bar{y} \in \mathbb{Z}_n$$

es un anillo conmutativo con unidad, llamado el *anillo de las clases residuales* \pmod{n} . Si n no es un número primo, entonces \mathbb{Z}_n posee divisores de cero propios, pues si $n = qp$, entonces $\bar{q} \cdot \bar{p} = \overline{pq} = \bar{n} = \bar{0}$.

4. Sea

$$S := \{\alpha \in \mathbb{R} \mid \alpha := x + y\sqrt[3]{3} + z\sqrt[3]{9}, x, y, z \in \mathbb{Q}\}$$

dotado de las operaciones de suma y producto usuales de \mathbb{R} . Entonces $(S, +, \cdot)$ es un anillo conmutativo. En efecto las propiedades de conmutatividad, asociatividad y distributividad son heredadas de la suma y producto usuales de \mathbb{R} . 0 y 1 están en S y son los elementos neutros respectivos. Obviamente si $\alpha \in S$, también $-\alpha \in S$. Nos falta mostrar que dados dos elementos $\alpha, \beta \in S$, la suma y producto están en S . En efecto, si $\alpha := a + b\sqrt[3]{3} + c\sqrt[3]{9}$ y $\beta := d + e\sqrt[3]{3} + f\sqrt[3]{9}$, entonces:

$$\alpha + \beta = (a + d) + (b + e)\sqrt[3]{3} + (c + f)\sqrt[3]{9} \in S,$$

$$\alpha \cdot \beta = (ad + 3bf + 3ce) + (ae + bd + 3cf)\sqrt[3]{3} + (af + be + cd)\sqrt[3]{9} \in S$$

5. El orden en el cual aparecen las operaciones es importante, pues el lector comprobará fácilmente que $(\mathbb{Q}, +, \cdot)$ es un anillo, pero $(\mathbb{Q}, \cdot, +)$ no lo es, ya que (\mathbb{Q}, \cdot) no es un grupo.

6. Sea $A := \{a, b, c, d\}$ y $+, \cdot$ las operaciones definidas por las tablas:

$+$	a	b	c	d	\cdot	a	b	c	d
a	a	b	c	d	a	a	a	a	a
b	b	a	d	c	b	a	b	a	b
c	c	d	a	b	c	a	c	a	c
d	d	c	b	a	d	a	d	a	d

Entonces $(A, +, \cdot)$ es un anillo no conmutativo, como el lector lo comprobará como un ejercicio.

7. Sea $(G, +)$ un grupo Abeliano y $\text{End}(G)$ el conjunto de endomorfismos sobre G , dotado de la operación binaria

$$+ : \text{End}(G) \times \text{End}(G) \rightarrow \text{End}(G)$$

definida por $(\psi + \varphi)(g) := \psi(g) + \varphi(g), \forall \psi, \varphi \in \text{End}(G), \forall g \in G$. Entonces $(\text{End}(G), +)$ es un grupo abeliano.(Ver ejercicio 4.3.1,13). Por otra parte la composición \circ de endomorfismos sobre G es una operación binaria sobre $\text{End}(G)$ y $(\text{End}(G), \circ)$ es un semigrupo, incluso un monoide. Dados tres endomorfismos $\psi, \varphi, \sigma \in \text{End}(G)$,

$$\begin{aligned} \psi \circ (\varphi + \sigma)(g) &= \psi(\varphi(g) + \sigma(g)) = \psi(\varphi(g)) + \psi(\sigma(g)) = \psi \circ \varphi(g) + \psi \circ \sigma(g), \forall g \in G \\ \text{por consiguiente vale} \end{aligned}$$

$$\psi \circ (\varphi + \sigma) = \psi \circ \varphi + \psi \circ \sigma.$$

En forma análoga resulta

$$(\varphi + \sigma) \circ \psi = \varphi \circ \psi + \sigma \circ \psi$$

y las relaciones de distributividad (9.1) se satisfacen, por lo tanto $(\text{End}(G), +, \circ)$ es un anillo con unidad, no conmutativo, ya que la composición de endomorfismos no es conmutativa.

9.1.1. Ejercicios y Complementos.

1. En un anillo $(A, +, \cdot)$ valen las siguientes propiedades:

- a) $a \cdot 0 = 0 \cdot a = 0, \forall a \in A$.
- b) $a \cdot (-b) = (-a) \cdot b = -(a \cdot b), \forall a, b \in A$.
- c) $(-a) \cdot (-b) = a \cdot b, \forall a, b \in A$.
- d) $-(-a) = a, \forall a \in A$.
- e) $(a + b)^2 = a^2 + b^2 + a \cdot b + b \cdot a$

Si además A es un anillo con unidad, entonces:

- f) Existe un único elemento unidad.
- g) $(-1) \cdot a = -a, \forall a \in A$.

2. Mostrar que si $a \in A$ es un elemento invertible del anillo A , entonces a no puede ser un divisor de 0.

3. Mostrar que si $b, c \in A$ son inversos por la derecha, respectivamente por la izquierda de un elemento $a \in A$, entonces $b = c$ y a es, por consiguiente, invertible.

4. En general en un anillo A cualquiera no vale la implicación:

$$a \cdot b = a \cdot c \Rightarrow b = c, \forall a, b, c \in A.$$

Mostrar que si A es un dominio de integridad, entonces dicha implicación sí es válida $\forall a, b, c \in A$. Dar ejemplo de un anillo en el cual dicha implicación no vale.

5. Sea M_2 el conjunto de las matrices 2×2 , con términos enteros, dotado de la suma y producto habituales de matrices.
 - a) ¿Es $(M_2, +, \cdot)$ un anillo?
 - b) ¿Existen en M_2 elementos divisores de 0?
 - c) ¿Existen en M_2 elementos invertibles?
 - d) Dar condición para que un elemento sea invertible en M_2 .
6. Se dice que un anillo $(A, +, \cdot)$ es un *anillo Booleano* si $x^2 = x, \forall x \in A$. Mostrar que todo anillo booleano es commutativo y que $2x = 0, \forall x \in A$.
7. Sea $(A, +, \cdot)$ un anillo y

$$A^* := \{a \in A \mid a \text{ invertible}\}$$

Mostrar que (A, \cdot) es un grupo, llamado el *grupo de unidades o elementos invertibles* de A .

8. Sea E el conjunto de todas las sucesiones de números enteros $\mathbf{a} := (a_1, a_2, \dots)$, dotado de la adición definida por componentes. Sea

$$A := \{f : E \rightarrow E \mid f(\mathbf{a} + \mathbf{b}) = f(\mathbf{a}) + f(\mathbf{b})\}.$$

Si \circ es la composición de aplicaciones y $+$ la aplicación binaria sobre A definida por $(f + g)(\mathbf{a}) := f(\mathbf{a}) + g(\mathbf{a}), \forall \mathbf{a} \in A$, mostrar que

- a) $(A, +, \circ)$ es un anillo con unidad.
- b) El *operador deslizamiento* $T(a_1, a_2, \dots) := (0, a_1, a_2, \dots)$ es un elemento de A .
- c) T posee una inversa T' por la izquierda, pero no por la derecha. Describir T' .
9. Sea $(A, +, \cdot)$ un anillo. Decimos que un subconjunto $B \subseteq A$ es un *subanillo* de A , si $(B, +)$ es un subgrupo de $(A, +)$ y B es cerrado respecto del producto \cdot . Si A es anillo con unidad, entonces exigiremos que B contenga a la unidad. Mostrar que el *centro* del anillo A , definido como el subconjunto

$$Z(A) := \{a \in A \mid a \cdot x = x \cdot a, \forall x \in A\},$$

es un subanillo de A .

10. Sea $(A, +, \cdot)$ un anillo, $x, y_1, \dots, y_n \in A$. Mostrar, por inducción sobre n , que

$$x \cdot (y_1 + y_2 + \dots + y_n) = xy_1 + \dots + xy_n.$$

Si además se tienen elementos $x_1, \dots, x_m \in A$, mostrar que

$$\left(\sum_{i=1}^m x_i \right) \left(\sum_{j=1}^n y_j \right) = \sum_{i=1}^m \sum_{j=1}^n x_i y_j$$

11. Sea S un conjunto no vacío y $(A, +, \cdot)$ un anillo. Mostrar que si $\mathfrak{M}(S, A)$ es el conjunto de todas las aplicaciones de S en A , dotado de las operaciones binarias $+$ y \cdot , definidas por

$$(f + g)(s) := f(s) + g(s), \quad (f \cdot g)(s) := f(s) \cdot g(s), \quad \forall s \in S$$

entonces $(\mathfrak{M}(S, A), +, \cdot)$ es un anillo. Si A es un anillo con unidad, entonces $\mathfrak{M}(S, A)$ es un anillo con unidad. Además si A es un anillo commutativo, entonces también lo será $\mathfrak{M}(S, A)$.

9.2. Ideales, Homomorfismos, Anillos Cociente y Teorema de Isomorfía

9.2.1. Ideales. Sea A un anillo. Un subconjunto no vacío, $\alpha \subseteq A$, es un *ideal derecho* (izquierdo) de A si se cumplen las condiciones siguientes:

- a) $(\alpha, +)$ es un subgrupo de $(A, +)$.
- b) Dados $x \in A$, $a \in \alpha$, $a \cdot x \in \alpha$ ($x \cdot a \in \alpha$).

Si α es un ideal izquierdo y derecho, entonces se dice que es un *ideal bilátero* o simplemente, por abuso de lenguaje, un *ideal*.

OBSERVACIÓN. Si A es un anillo commutativo la distinción entre ideal izquierdo y derecho es irrelevante.

EJEMPLOS 9.2.

1. El anillo A y $\mathbf{0} := \{0\} = (0)$ son ideales. $\mathbf{0}$ se llama el *ideal cero*
2. Sea \mathbb{Z} el anillo de los números enteros con las operaciones usuales y n un entero.

Entonces

$$n\mathbb{Z} := \{nx \mid x \in \mathbb{Z}\}$$

es un ideal de \mathbb{Z} .

3. Si

$$\mathbb{Z}[i] := \{\alpha \in \mathbb{C} \mid \alpha := x + iy, x, y \in \mathbb{Z}\}$$

es el anillo de los *enteros gaussianos*, entonces el conjunto

$$\alpha := \{i\alpha \mid \alpha \in \mathbb{Z}[i]\}$$

es un ideal de $\mathbb{Z}[i]$.

4. Sea M_2 el conjunto de las matrices 2×2 con términos reales y $A \in M_2$, entonces

$$\alpha := \{AB \mid B \in M_2\}$$

es un ideal derecho de M_2 , mientras que

$$\beta := \{BA \mid B \in M_2\}$$

es un ideal izquierdo de M_2 . Sin embargo α , β no son ideales de M_2 .

5. Sea A un anillo, $a \in A$ un elemento fijo. Entonces los conjuntos

$$a \cdot A := \{a \cdot x \mid x \in A\} \quad A \cdot a := \{x \cdot a \mid x \in A\}$$

son, respectivamente, ideal derecho e ideal izquierdo de A , mientras que

$$a \cdot A \cdot a := \{x \cdot a \cdot x \mid x \in A\}$$

es un ideal de A . En el caso en que A es un anillo commutativo, entonces $a \cdot A = A \cdot a = A \cdot a \cdot A$ es un ideal de A .

Decimos que un ideal izquierdo (derecho) α es un *ideal principal izquierdo (derecho)* generado por $a \in A$, si $\alpha = A \cdot a$ ($\alpha = a \cdot A$). En forma análoga α es un *ideal principal* de A generado por $a \in A$ si $\alpha = A \cdot a \cdot A$, en tal caso escribiremos $\alpha = (a)$. Si A es un anillo con unidad, entonces $a \in \alpha$.

Si S es un subconjunto de elementos de un anillo A , sean

$$(S)_{(i)} := \left\{ \sum_{s \in S} x_s \cdot s \mid x_s \in A, x_s = 0, \text{ salvo para un número finito de elementos } s \in S \right\}$$

$$(S)_{(d)} := \left\{ \sum_{s \in S} s \cdot x_s \mid x_s \in A, x_s = 0, \text{ salvo para un número finito de elementos } s \in S \right\}$$

y

$$(S) := \left\{ \sum_{s \in S} x_s \cdot s \cdot y_s \mid x_s, y_s \in A, x_s = 0 = y_s, \text{ salvo para un número finito de elementos } s \in S \right\}$$

Entonces $(S)_{(i)}$, $(S)_{(d)}$, (S) son ideales por la izquierda, por la derecha y bilátero, respectivamente, llamados los ideales por la izquierda, por la derecha y bilátero generados por el conjunto S .

En el caso en que S es un conjunto finito formado por los elementos $s_1, \dots, s_n \in A$, entonces denotaremos por $(s_1, \dots, s_n)_{(i)}$, $(s_1, \dots, s_n)_{(d)}$, (s_1, \dots, s_n) los ideales correspondientes generados por s_1, \dots, s_n .

9.2.1.1. Operaciones entre Ideales. Sea $(\mathfrak{a})_{i \in I}$ una familia de ideales de un anillo $(A, +, \cdot)$, entonces

$$\mathfrak{a} := \bigcap_{i \in I} \mathfrak{a}_i$$

es un ideal (demostración!) de A , llamado el *ideal intersección* sobre la familia $(\mathfrak{a})_{i \in I}$. $\mathfrak{a} \neq \emptyset$, ya que $0 \in \mathfrak{a}$.

Como el lector podrá comprobar con facilidad, con algunos ejemplos, la unión de ideales no es, en general, un ideal. Sin embargo definimos la suma de ideales sobre una familia $(\mathfrak{a})_{i \in I}$ de ideales como

$$(9.3) \quad \sum_{i \in I} \mathfrak{a}_i := \left(\bigcup_{i \in I} \mathfrak{a}_i \right),$$

es decir como el ideal generado por la unión sobre la familia de ideales $(\mathfrak{a})_{i \in I}$. Al ideal (9.3) lo llamamos el *ideal suma* sobre la familia de ideales $(\mathfrak{a})_{i \in I}$.

Si A es un anillo comunitativo y $\mathfrak{a}_1, \dots, \mathfrak{a}_n$ ideales de A , entonces al ideal

$$\prod_{i=1}^n \mathfrak{a}_i := (S),$$

donde S es el conjunto

$$S := \{x_1 \cdots x_n \mid x_i \in \mathfrak{a}_i, i = 1, \dots, n\},$$

lo llamamos el *ideal producto* de los ideales $\mathfrak{a}_1, \dots, \mathfrak{a}_n$.

Decimos que el ideal \mathfrak{a} es un *ideal propio* del anillo A , si $\mathfrak{a} \neq A$, es decir \mathfrak{a} está propiamente contenido en A .

9.2.2. Ejercicios y Complementos.

1. Sea $(\mathbb{Z}, +, \cdot)$ el anillo de los números enteros. Mostrar que dados $m, n \in \mathbb{Z}$, el ideal $(m, n) = (D)$, donde D es el máximo común divisor de m y n .
2. Si $(A, +, \cdot)$ es un anillo con unidad, y $\mathfrak{a} := (a)$, entonces $a \in \mathfrak{a}$. Si \mathfrak{a} es un ideal, tal que $1 \in \mathfrak{a}$, mostrar que $\mathfrak{a} = A$ y que $a \in A$ un elemento invertible. Si el ideal $(a) = A$. Mostrar también que si un ideal \mathfrak{a} contiene un elemento invertible, entonces $\mathfrak{a} = A$.
3. Sean \mathfrak{a} un ideal izquierdo y \mathfrak{b} un ideal derecho de un anillo A . Mostrar que $\mathfrak{a} \cdot \mathfrak{b}$ es un ideal de A .

4. Sean $(A, +, \cdot)$ un anillo conmutativo con unidad, \mathfrak{a} , \mathfrak{b} ideales de A . Mostrar que

$$(\mathfrak{a} : \mathfrak{b}) := \{x \in A \mid x \cdot \mathfrak{b} \subseteq \mathfrak{a}\}$$

es un ideal de A , llamado el *ideal cociente*. Mostrar, además que el ideal cociente posee las siguientes propiedades:

- a) $\mathfrak{a} \subseteq (\mathfrak{a} : \mathfrak{b})$.
- b) $(\mathfrak{a} : \mathfrak{b}) \cdot \mathfrak{b} \subseteq \mathfrak{a}$.
- c) $((\mathfrak{a} : \mathfrak{b}) : \mathfrak{c}) = (\mathfrak{a} : (\mathfrak{b} \cdot \mathfrak{c})) = ((\mathfrak{a} : \mathfrak{c}) : \mathfrak{b})$.
- d) $(\bigcap_{i \in I} \mathfrak{a}_i : \mathfrak{b}) = \bigcap_{i \in I} (\mathfrak{a}_i : \mathfrak{b})$.
- e) $(\mathfrak{a} : \sum_{i \in I} \mathfrak{b}_i) = \bigcap_{i \in I} (\mathfrak{a} : \mathfrak{b}_i)$.

5. Sea \mathfrak{a} un ideal del anillo conmutativo con unidad A . Si

$$\text{Ann}(\mathfrak{a}) := \{x \in A \mid x \cdot \mathfrak{a} = \mathbf{0}\}$$

mostrar que $\text{Ann}(\mathfrak{a}) = (\mathbf{0} : \mathfrak{a})$, por lo que $\text{Ann}(\mathfrak{a})$ es un ideal de A , llamado el *anulador* de \mathfrak{a} .

6. Mostrar que un anillo conmutativo con unidad $(K, +, \cdot)$ es un campo Ssi sus únicos ideales son $\mathbf{0}$ y todo K .

9.2.3. Homomorfismos de Anillos. Sean A, B dos anillos. Decimos que la aplicación

$$\varphi : A \rightarrow B$$

es un *homomorfismo de anillos* si se cumplen las condiciones siguientes:

$$(9.4) \quad \varphi(x + y) = \varphi(x) + \varphi(y), \forall x, y \in A,$$

(es decir φ es un homomorfismo del grupo $(A, +)$ en el grupo $(B, +)$)

$$(9.5) \quad \varphi(x \cdot y) = \varphi(x) \cdot \varphi(y), \forall x, y \in A.$$

Si A y B son anillos con unidad, entonces debe valer además

$$(9.6) \quad \varphi(1_A) = 1_B$$

En forma análoga a los homomorfismos de grupos, al conjunto

$$\ker \varphi := \{x \in A \mid \varphi(x) = 0\}$$

lo llamamos el *núcleo* o *kernel* del homomorfismo φ .

En forma análoga a los homomorfismos de grupos, si φ es un homomorfismo de anillos inyectivo, sobreíectivo o biíyectivo, respectivamente, diremos, entonces que φ es un *monomorfismo*, *epimorfismo* o *isomorfismo* de anillos, respectivamente.

EJEMPLOS 9.3.

1. Sea A un anillo. La aplicación identidad

$$\mathbf{1} : A \rightarrow A$$

definida por $\mathbf{1}(x) := x, \forall x \in A$, es un homomorfismo de anillos, cuyo núcleo es $\mathbf{0}$.

2. Sea \mathfrak{C} el conjunto de todas las matrices de la forma

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \quad \text{donde } a, b \in \mathbb{Z}$$

dotado de las operaciones usuales de suma y producto de matrices. Entonces $(\mathbb{C}, +, \cdot)$ es un anillo conmutativo con unidad. Si \mathbb{Z} es el anillo de los enteros, entonces

$$\varphi : \mathbb{Z} \rightarrow \mathbb{C}$$

definido por

$$\varphi(a) := \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$$

es un homomorfismo inyectivo de anillos. $\ker \varphi = \mathbf{0}$

3. Sea $(\mathbb{Z}_n, +, \cdot)$ el anillo de las clases residuales $(\text{mód } n)$ y

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

la proyección canónica, definida por $\pi(x) := \bar{x}$, entonces π es un homomorfismo de anillos, cuyo núcleo $\ker \pi = n\mathbb{Z}$.

4. Sea $\mathbb{Z}[i]$ el anillo de los enteros gaussianos y \mathbb{C} el anillo definido en el ejemplo 9.3.2, entonces la aplicación

$$\varphi : \mathbb{Z}[i] \rightarrow \mathbb{C}$$

definida por

$$\varphi(a + bi) := \begin{pmatrix} a & b \\ -b & a \end{pmatrix}, \forall a + bi \in \mathbb{Z}[i]$$

es un isomorfismo de anillos.

TEOREMA 9.1. *El núcleo $\ker \varphi$ de un homomorfismo de anillos $\varphi : A \rightarrow B$ es un ideal de A . Además $\ker \varphi = \mathbf{0}$ Ssi φ es un monomorfismo.*

DEMOSTRACIÓN. Siendo $\ker \varphi$ el núcleo de un homomorfismo de anillos, es también el núcleo del homomorfismo φ en tanto que homomorfismo de grupos, entre el grupo $(A, +)$ y el grupo $(B, +)$. Del teorema 4.33 sabemos que $\ker \varphi$ es un subgrupo normal del grupo $(A, +)$. Por otra parte $\forall x \in A$ y $\forall a \in \ker \varphi$ se tiene

$$\varphi(x \cdot a) = \varphi(x) \cdot \varphi(a) = \varphi(x) \cdot 0 = 0 \quad y \quad \varphi(a \cdot x) = \varphi(a) \cdot \varphi(x) = 0 \cdot \varphi(x) = 0$$

por lo tanto $\ker \varphi$ es un ideal de A .

Supongamos ahora que $\ker \varphi = \mathbf{0}$, y φ no inyectiva. Entonces existen $x, y \in A$, $x \neq y$ tales que $\varphi(x) = \varphi(y)$. Como φ es un homomorfismo, vale entonces $0 = \varphi(x) - \varphi(y) = \varphi(x - y)$, entonces $x - y \in \ker \varphi$ y $x - y \neq 0$, en contradicción a que $\ker \varphi = \mathbf{0}$. Por lo tanto φ debe ser inyectiva. Por otra parte, si φ es inyectiva, entonces $\varphi(x) = 0 = \varphi(0)$ implica que $x = 0$, por lo que $\ker \varphi = \mathbf{0}$. \square

9.2.4. Anillos Cociente. Dado un anillo $(A, +, \cdot)$ y un ideal \mathfrak{a} de A , entonces \mathfrak{a} es un subgrupo normal del grupo $(A, +)$, la relación $a \sim b$ Ssi $(a - b) \in \mathfrak{a}$ es una relación de equivalencia sobre A y la operación binaria $+$ induce una operación binaria sobre A/\mathfrak{a} tal que $(A/\mathfrak{a}, +)$ es un grupo abeliano (Ver teorema 4.21).

TEOREMA 9.2. *La operación \cdot sobre A induce una operación binaria*

$$\cdot : A/\mathfrak{a} \times A/\mathfrak{a} \rightarrow A/\mathfrak{a}$$

definida de la siguiente forma:

$$\bar{x} \cdot \bar{y} := \overline{x \cdot y}$$

la cual está bien definida y tal que $(A/\mathfrak{a}, +, \cdot)$ es un anillo. Si $(A, +, \cdot)$ es conmutativo, también lo será $(A/\mathfrak{a}, +, \cdot)$ y si A es un anillo con elemento unidad 1, entonces la clase $\bar{1}$ es elemento unidad del anillo A/\mathfrak{a} .

DEMOSTRACIÓN. Debemos mostrar que \cdot está bien definida, es decir, que no depende de los representantes escogidos. En efecto, sean $x, u \in A$ dos representantes distintos de $\bar{x} \in A/\alpha$ y $y, v \in A$ dos representantes distintos de $\bar{y} \in A/\alpha$. Entonces $u - x \in \alpha$ y $v - y \in \alpha$ y existen $a, b \in \alpha$, tales que $u = x + a$ y $v = y + b$. Entonces

$$u \cdot v = (x + a) \cdot (y + b) = x \cdot y + x \cdot b + a \cdot y + a \cdot b,$$

de donde

$$u \cdot v - x \cdot y = (x \cdot b + a \cdot y + a \cdot b) \in \alpha.$$

Por consiguiente

$$\bar{u} \cdot \bar{v} = \overline{u \cdot v} = \overline{x \cdot y} = \bar{x} \cdot \bar{y},$$

por lo que \cdot está bien definida sobre A/α .

Por teorema 4.21 ($A/\alpha, +$) es un grupo abeliano. Nos queda por mostrar que \cdot es asociativa y que satisface las propiedades de distributividad (9.1)

\cdot es asociativa. En efecto, para todo $x, y, z \in A$

$$\bar{x} \cdot (\bar{y} \cdot \bar{z}) = \bar{x} \cdot (\overline{\bar{y} \cdot \bar{z}}) = \overline{x \cdot (y \cdot z)} = \overline{(x \cdot y) \cdot z} = (\bar{x} \cdot \bar{y}) \cdot \bar{z}.$$

De forma análoga resultan las propiedades distributivas:

$$\bar{x} \cdot (\bar{y} + \bar{z}) = \bar{x} \cdot \overline{(y + z)} = \overline{x \cdot (y + z)} = \overline{x \cdot y + x \cdot z} = \overline{x \cdot y} + \overline{x \cdot z} = \bar{x} \cdot \bar{y} + \bar{x} \cdot \bar{z}$$

y

$$(\bar{x} + \bar{y}) \cdot \bar{z} = \overline{(x + y)} \cdot \bar{z} = \overline{(x + y) \cdot z} = \overline{x \cdot z + y \cdot z} = \overline{x \cdot z} + \overline{y \cdot z} = \bar{x} \cdot \bar{z} + \bar{y} \cdot \bar{z}.$$

Por lo tanto hemos mostrado que $(A/\alpha, +, \cdot)$ es un anillo.

Si A es conmutativo, entonces un simple cálculo (ejercicio) nos muestra que A/α es conmutativo.

Si A es un anillo con unidad $1 \in A$, entonces

$$\bar{1} \cdot \bar{x} = \overline{1 \cdot x} = \bar{x} = \overline{x \cdot 1} = \bar{x} \cdot \bar{1}$$

por lo que $\bar{1}$ es el elemento unidad de A/α . □

El anillo $(A/\alpha, +, \cdot)$ se llama el *anillo cociente* de A por α .

Dejamos al lector, como un ejercicio, la sencilla demostración del siguiente

TEOREMA 9.3. *La aplicación canónica*

$$\pi : A \rightarrow A/\alpha$$

definida por $\pi(x) := \bar{x}$ es un homomorfismo de anillos, llamado el *homomorfismo canónico*.

9.2.5. Teoremas de Isomorfía. En forma análoga a la teoría de grupos, en la teoría de anillos también se tienen los llamados teoremas de isomorfía.

TEOREMA 9.4 (Primer Teorema de Isomorfía o Teorema de Factorización). *Sea*

$$\varphi : A \rightarrow B$$

un homomorfismo de anillos. Entonces φ induce un único homomorfismo de anillos

$$\hat{\varphi} : A/\ker \varphi \rightarrow B,$$

que hace comutar al diagrama

$$(9.7) \quad \begin{array}{ccc} A & \xrightarrow{\varphi} & B \\ \downarrow \pi & \nearrow \hat{\varphi} & \\ A/\ker \varphi & & \end{array}$$

$\hat{\varphi}$ es inyectiva y si φ es sobreyectiva, entonces $\hat{\varphi}$ es un isomorfismo.

DEMOSTRACIÓN. Consideremos, inicialmente, φ como el homomorfismo entre los grupos $(A, +)$ y $(B, +)$. Vimos en la demostración del teorema de factorización para grupos 4.35, que la aplicación $\hat{\varphi}$, definida por $\hat{\varphi}(\bar{x}) := \varphi(x)$ está bien definida, es un homomorfismo de grupos y es el único homomorfismo que hace comutar al diagrama (9.7). Además $\hat{\varphi}$ es inyectivo y si φ es sobreyectivo, entonces $\hat{\varphi}$ es un isomorfismo de grupos. Vamos a mostrar que $\hat{\varphi}$ es también un homomorfismo de anillos. En efecto, $\forall \bar{x}, \bar{y} \in A/\ker \varphi$

$$\hat{\varphi}(\bar{x} \cdot \bar{y}) = \varphi(x \cdot y) = \varphi(x) \cdot \varphi(y) = \hat{\varphi}(\bar{x}) \cdot \hat{\varphi}(\bar{y})$$

□

Sea \mathfrak{a} un ideal del anillo A y \mathfrak{b} un ideal del anillo B , decimos que una aplicación

$$\varphi : \mathfrak{a} \rightarrow \mathfrak{b}$$

es un *homomorfismo de ideales*, si φ es un homomorfismo de grupos entre el grupo $(\mathfrak{a}, +)$ y el grupo $(\mathfrak{b}, +)$ y $\forall x, y \in \mathfrak{a}$, $\varphi(x \cdot y) = \varphi(x) \cdot \varphi(y)$.

Si

$$\varphi : A \rightarrow B$$

es un homomorfismo de anillos, que mapea un ideal \mathfrak{a} de A en un ideal \mathfrak{b} de B , entonces la restricción

$$\varphi|_{\mathfrak{a}} : \mathfrak{a} \rightarrow \mathfrak{b}$$

es un homomorfismo de ideales, como el lector comprobará fácilmente. Dado un anillo A y un ideal \mathfrak{a} de A , denotaremos por $\mathfrak{J}(A)$ al conjunto de todos los ideales de A , y por $\mathfrak{J}_{\mathfrak{a}}(A)$ al conjunto de todos los ideales de A que contienen al ideal \mathfrak{a} .

TEOREMA 9.5 (Segundo Teorema de Isomorfía). *Sea*

$$\varphi : A \rightarrow B$$

un homomorfismo sobreyectivo de anillos, \mathfrak{b} un ideal de B . Entonces $\mathfrak{a} := \varphi^{-1}[\mathfrak{b}]$ es un ideal de A que contiene al núcleo $\ker \varphi$ y la restricción

$$\hat{\varphi}|_{\mathfrak{a}/\ker \varphi} : \mathfrak{a}/\ker \varphi \rightarrow \mathfrak{b}$$

es un isomorfismo de ideales. Por otra parte φ induce una biyección

$$\Phi : \mathfrak{J}(B) \rightarrow \mathfrak{J}_{\ker \varphi}(A)$$

por lo que los ideales de B están en correspondencia biunívoca con los ideales de A que contienen a $\ker \varphi$.

DEMOSTRACIÓN. \mathfrak{a} es un ideal de A . En efecto dados $x, y \in \mathfrak{a}$, $\varphi(x+y) = \varphi(x) + \varphi(y) \in \mathfrak{b}$, lo que implica que $(x+y) \in \mathfrak{a}$. Por otra parte, dados $x \in A$, $a \in \mathfrak{a}$, $\varphi(x \cdot a) = \varphi(x) \cdot \varphi(a) \in \mathfrak{b}$ lo que implica que $x \cdot a \in \mathfrak{a}$, en forma análoga se muestra que $a \cdot x \in \mathfrak{a}$. Por consiguiente \mathfrak{a} es un ideal de A . Por otra parte, como $0 \in \mathfrak{b}$, resulta que $\ker \varphi = \varphi^{-1}[\mathbf{0}] \subseteq \mathfrak{a}$.

Por el primer teorema de isomorfía 9.4, φ induce un isomorfismo

$$\hat{\varphi} : \mathfrak{a}/\ker \varphi \rightarrow \mathfrak{b}$$

cuya restricción

$$\hat{\varphi}|_{\mathfrak{a}/\ker \varphi} : \mathfrak{a}/\ker \varphi \rightarrow \mathfrak{b}$$

es un isomorfismo de ideales.

Vamos a mostrar ahora, que la aplicación

$$\Phi : \mathfrak{I}(B) \rightarrow \mathfrak{I}_{\ker \varphi}(A)$$

definida por $\Phi(\mathfrak{y}) := \varphi^{-1}[\mathfrak{y}], \forall \mathfrak{y} \in \mathfrak{I}(B)$ es una biyección. Φ es inyectiva: En efecto, como φ es sobreyectiva, se tiene que $\varphi[\varphi^{-1}[\mathfrak{y}]] = \mathfrak{y}, \forall \mathfrak{y} \in \mathfrak{I}(B)$. (Ver teorema 1.2), por consiguiente Φ es inyectiva. Φ es sobreyectiva: En efecto, sea $\mathfrak{x} \in \mathfrak{I}_{\ker \varphi}(A)$, como φ es sobreyectiva, $\varphi[\mathfrak{x}]$ es un ideal de B (ejercicio). Vamos a mostrar que $\mathfrak{x} = \varphi^{-1}[\varphi[\mathfrak{x}]]$. Por teorema 1.2, sabemos que $\mathfrak{x} \subseteq \varphi^{-1}[\varphi[\mathfrak{x}]]$, vamos a mostrar que, en este caso, también $\varphi^{-1}[\varphi[\mathfrak{x}]] \subseteq \mathfrak{x}$. Sea $x \in \varphi^{-1}[\varphi[\mathfrak{x}]]$, entonces $\varphi(x) \in \varphi[\mathfrak{x}]$, por lo que existe $a \in \mathfrak{x}$, tal que $\varphi(x) = \varphi(a)$, entonces $(x - a) \in \ker \varphi \subseteq \mathfrak{x}$ y $x = (a + (x - a)) \in \mathfrak{x}, \forall x \in \varphi^{-1}[\varphi[\mathfrak{x}]]$. Por consiguiente $\mathfrak{x} = \varphi^{-1}[\varphi[\mathfrak{x}]]$ \square

LEMA 9.6. *Si \mathfrak{a} es un ideal de un anillo A , contenido en el núcleo $\ker \varphi$ del homomorfismo de anillos*

$$\varphi : A \rightarrow B$$

entonces φ induce un homomorfismo de anillos

$$\hat{\varphi} : A/\mathfrak{a} \rightarrow B$$

que hace commutar al diagrama

(9.8)

$$\begin{array}{ccc} A & \xrightarrow{\varphi} & B \\ \downarrow \pi & \nearrow \hat{\varphi} & \\ A/\mathfrak{a} & & \end{array}$$

DEMOSTRACIÓN. Como vimos en la demostración del teorema 9.4, para que el diagrama (9.8) sea commutativo, debe valer $\hat{\varphi}(\bar{x}) := \varphi(x)$. $\hat{\varphi}$ está bien definida si, dados dos representantes x, y de la clase \bar{x} , $x - y \in \ker \varphi$, lo cual se cumple, ya que $\mathfrak{a} \subseteq \ker \varphi$. (Ver ejercicio 9.2.6,3). $\hat{\varphi}$ es un homomorfismo de anillos, como se demostró en el teorema 9.4. \square

TEOREMA 9.7 (Tercer Teorema de Isomorfía). *Sean*

$$\varphi : A \rightarrow B$$

un homomorfismo de anillos, \mathfrak{b} un ideal de B y \mathfrak{a} un ideal de A , tal que $\varphi[\mathfrak{a}] \subseteq \mathfrak{b}$. Entonces φ induce un único homomorfismo

$$\hat{\varphi} : A/\mathfrak{a} \rightarrow B/\mathfrak{b}$$

que hace commutar al diagrama

(9.9)

$$\begin{array}{ccc} A & \xrightarrow{\varphi} & B \\ \downarrow \pi_A & & \downarrow \pi_B \\ A/\mathfrak{a} & \xrightarrow{\hat{\varphi}} & B/\mathfrak{b} \end{array}$$

Si $\mathfrak{a} := \varphi^{-1}[\mathfrak{b}]$, entonces $\hat{\varphi}$ es inyectiva y si, además, φ es sobreyectiva, entonces $\hat{\varphi}$ es un isomorfismo.

DEMOSTRACIÓN. Consideremos el diagrama comutativo, por definición de $\tilde{\varphi}$

(9.10)

$$\begin{array}{ccc} A & \xrightarrow{\varphi} & B \\ & \searrow \tilde{\varphi} & \downarrow \pi_B \\ & & B/b \end{array}$$

como $\varphi[a] \subseteq b$, vale $a \subseteq \ker \varphi$ y, por lema 9.6, $\tilde{\varphi}$ induce un homomorfismo

$$\hat{\varphi} : A/a \rightarrow B/b$$

que completa al diagrama (9.10) en el diagrama comutativo

(9.11)

$$\begin{array}{ccc} A & \xrightarrow{\varphi} & B \\ \pi_A \downarrow & \swarrow \tilde{\varphi} & \downarrow \pi_B \\ A/a & \xrightarrow{\hat{\varphi}} & B/b \end{array}$$

Si $a := \varphi^{-1}[b]$, entonces $a = \ker \tilde{\varphi}$ y, por teorema 9.4, $\hat{\varphi}$ es inyectiva y si φ es sobreyectiva, también lo será $\tilde{\varphi}$ y por consiguiente $\hat{\varphi}$ es un isomorfismo. \square

Como consecuencia de los teoremas de isomorfía, se obtiene el siguiente

COROLARIO 9.8 (Teorema de Cancelación). *Sean A un anillo, a, b ideales de A , tales que $a \subseteq b$. Entonces existe un isomorfismo*

$$\hat{\pi} : (A/a)/(b/a) \rightarrow A/b$$

DEMOSTRACIÓN. En efecto, la proyección canónica

$$\pi : A \rightarrow A/b$$

induce, por lema 9.6, un homomorfismo

$$\tilde{\pi} : A/a \rightarrow A/b$$

cuyo núcleo es b/a y, por teorema 9.7, el homomorfismo

$$\hat{\pi} : (A/a)/(b/a) \rightarrow A/b$$

es un isomorfismo. \square

9.2.6. Ejercicios y Complementos.

1. Mostrar que si $\varphi : A \rightarrow B$ es un homomorfismo de anillos, entonces $\varphi[A]$ es un subanillo de B .
2. Sean A un anillo con unidad y \mathbb{Z} el anillo de los números enteros. Mostrar que la aplicación $\psi : \mathbb{Z} \rightarrow A$, definida por $\psi(m) := m \cdot 1 := \underbrace{1 + \dots + 1}_m$, $\forall m \in \mathbb{Z}$ es un homomorfismo de anillos. Mostrar, además, que A contiene un subanillo isomorfo a \mathbb{Z} o A contiene un subanillo isomorfo a un \mathbb{Z}_n , para algún $n \in \mathbb{Z}$.
3. Dados un homomorfismo de anillos $\varphi : A \rightarrow B$, y un ideal a de A , mostrar que la aplicación $\hat{\varphi} : A/a \rightarrow B$, definida por $\hat{\varphi}(\bar{x}) := \varphi(x)$, está bien definida. Si $a \subseteq \ker \varphi$.
4. Dados un anillo A y un ideal a de A , mostrar, usando el segundo teorema de isomorfía, que los ideales de A/a están en correspondencia biunívoca con los ideales de A que contienen al ideal a y que éstos son de la forma x/a , donde x es un ideal de A que contiene al ideal a .

5. Sea $A := \text{End}(\mathbb{Z}_n)$ el anillo de todos los endomorfismos sobre el grupo abeliano $(\mathbb{Z}_n, +)$. Si $\mathbf{1}$ es el endomorfismo identidad sobre \mathbb{Z}_n , entonces por ejercicio 9.2.6.2, la aplicación $\psi : \mathbb{Z} \rightarrow \text{End}(\mathbb{Z}_n)$, definida por $\psi(m) := m \cdot \mathbf{1}$ es un homomorfismo de anillos. Mostrar que ψ induce un isomorfismo $\hat{\psi} : \mathbb{Z}_n \rightarrow \text{End}(\mathbb{Z}_n)$.
6. Mostrar que si $\varphi : K \rightarrow E$ es un homomorfismo entre dos campos K, E , entonces φ es inyectivo. En particular, si K es un campo finito, entonces todo endomorfismo sobre K es un automorfismo.
7. Mostrar que el conjunto de los automorfismos sobre un campo K , $\text{Aut}(K)$, con la composición \circ forma un grupo. LLamado el *grupo de automorfismos* sobre el campo K .

9.3. Ideales Primos e Ideales Maximales

Sea A un anillo comunitativo con unidad. Decimos que el ideal \mathfrak{p} es un *ideal primo* del anillo A , si \mathfrak{p} es un ideal propio y

$$(9.12) \quad x \cdot y \in \mathfrak{p} \Rightarrow x \in \mathfrak{p} \vee y \in \mathfrak{p}.$$

TEOREMA 9.9. *Sea A un anillo comunitativo con unidad. Entonces el ideal \mathfrak{p} es un ideal primo Ssi el anillo A/\mathfrak{p} es un dominio entero.*

DEMOSTRACIÓN. A/\mathfrak{p} es dominio entero Ssi $\bar{x} \cdot \bar{y} = \bar{x} \cdot \bar{y} = \bar{0} \Rightarrow \bar{x} = \bar{0} \vee \bar{y} = \bar{0}$ Ssi $x \cdot y \in \mathfrak{p} \Rightarrow x \in \mathfrak{p} \vee y \in \mathfrak{p}$ Ssi \mathfrak{p} es ideal primo. \square

Sea A un anillo comunitativo con unidad. Al conjunto

$$\text{Spec } A := \{\mathfrak{p} \subseteq A \mid \mathfrak{p} \text{ es un ideal primo}\}$$

lo llamamos el *espectro primo* de A o *espectro* de A . Dado un ideal \mathfrak{a} de A , definimos

$$\text{Spec}_{\mathfrak{a}} A := \{\mathfrak{p} \in \text{Spec } A \mid \mathfrak{a} \subseteq \mathfrak{p}\}.$$

El conjunto $\text{Spec } A$ juega un papel muy importante en la geometría algebraica, donde se le dota de una topología, la llamada topología de Zariski. Ver teorema 9.18).

Como consecuencia del segundo teorema de isomorfía, teorema 9.5, se obtiene, para el caso de los ideales primos el siguiente

COROLARIO 9.10. *Sean*

$$\varphi : A \rightarrow B$$

un homomorfismo sobreyectivo de anillos y $\mathfrak{q} \in \text{Spec } B$. Entonces $\mathfrak{p} := \varphi^{-1}[\mathfrak{q}] \in \text{Spec}_{\ker \varphi} A$ y la restricción

$$\hat{\varphi}|_{\mathfrak{p}/\ker \varphi} : \mathfrak{p}/\ker \varphi \rightarrow \mathfrak{q}$$

es un isomorfismo de ideales. Por otra parte φ induce una biyección

$$\varphi^* : \text{Spec } B \rightarrow \text{Spec}_{\ker \varphi} A$$

definida por $\varphi^(\mathfrak{q}) := \varphi^{-1}[\mathfrak{q}]$, $\forall \mathfrak{q} \in \text{Spec } B$, por lo que los ideales primos de B están en correspondencia biunívoca con los ideales primos de A que contienen a $\ker \varphi$.*

DEMOSTRACIÓN. Únicamente falta mostrar que, en efecto, la imágen inversa de un ideal primo es también primo. Demostración que dejaremos, como ejercicio, al lector. \square

Sea A un anillo comunitativo con unidad. Decimos que el ideal \mathfrak{m} es un *ideal maximal* del anillo A , si \mathfrak{m} es un ideal propio y si \mathfrak{a} es un ideal que contiene a \mathfrak{m} , entonces $\mathfrak{a} = A$ o $\mathfrak{a} = \mathfrak{m}$. Es decir \mathfrak{m} no está contenido propiamente en ningún ideal propio.

TEOREMA 9.11. *Sea A un anillo conmutativo con unidad. Entonces el ideal \mathfrak{m} es un ideal maximal. Sí A/\mathfrak{m} es un campo.*

DEMOSTRACIÓN. Vamos a mostrar que los únicos ideales de A/\mathfrak{m} son $\bar{\mathbf{0}}$ y A/\mathfrak{m} y por ejercicio 9.2.2,6, A/\mathfrak{m} es un campo. En efecto, si $\bar{\mathfrak{a}}$ es un ideal de A/\mathfrak{m} , entonces, por ejercicio 9.2.6,4, $\bar{\mathfrak{a}} = \mathfrak{a}/\mathfrak{m}$, donde \mathfrak{a} es un ideal que contiene a \mathfrak{m} . Como \mathfrak{m} es ideal maximal sólo puede valer $\mathfrak{a} = \mathfrak{m}$ o $\mathfrak{a} = A$, es decir $\bar{\mathfrak{a}} = \bar{\mathbf{0}}$ o $\bar{\mathfrak{a}} = A/\mathfrak{m}$. \square

Dado que todo campo es un dominio de integridad, se tiene, de forma inmediata, el siguiente

COROLARIO 9.12. *Todo ideal maximal de un anillo conmutativo con unidad, es un ideal primo.*

Sea A un anillo conmutativo con unidad. Al conjunto

$$\Omega(A) := \{\mathfrak{m} \subseteq A \mid \mathfrak{m} \text{ es ideal maximal}\}$$

lo llamamos el *espectro maximal* de A . Dado un ideal \mathfrak{a} de A , definimos

$$\Omega_{\mathfrak{a}}(A) := \{\mathfrak{m} \in \Omega(A) \mid \mathfrak{a} \subseteq \mathfrak{m}\}.$$

Por corolario 9.12, se tiene

$$(9.13) \quad \Omega(A) \subseteq \text{Spec } A.$$

Como consecuencia del segundo teorema de isomorfía, teorema 9.5, se obtiene, para el caso de los ideales maximales el siguiente

COROLARIO 9.13. *Sean*

$$\varphi : A \rightarrow B$$

un homomorfismo sobreyectivo de anillos y $\mathfrak{n} \in \Omega(B)$. Entonces $\mathfrak{m} := \varphi^{-1}[\mathfrak{n}] \in \Omega_{\ker \varphi}(A)$ y la restricción

$$\hat{\varphi}|_{\mathfrak{m}/\ker \varphi} : \mathfrak{m}/\ker \varphi \rightarrow \mathfrak{n}$$

es un isomorfismo de ideales. Por otra parte φ induce una biyección

$$\varphi^* : \Omega(B) \rightarrow \Omega_{\ker \varphi}(A)$$

definida por $\varphi^(\mathfrak{n}) := \varphi^{-1}[\mathfrak{n}], \forall \mathfrak{n} \in \Omega(B)$, por lo que los ideales maximales de B están en correspondencia biunívoca con los ideales maximales de A que contienen a $\ker \varphi$.*

DEMOSTRACIÓN. Únicamente falta mostrar que, en efecto, la imagen inversa de un ideal maximal es también maximal. Demostración que dejaremos, como ejercicio, al lector. \square

Uno de los resultados más importantes en la teoría de anillos conmutativos con unidad, es la existencia de ideales maximales, cuya demostración utiliza el llamado lema de Zorn, 1.6.

TEOREMA 9.14. *Sea A un anillo conmutativo con unidad. Entonces A posee, al menos, un ideal maximal.*

DEMOSTRACIÓN. Sea \mathfrak{M} el conjunto de todos los ideales propios de A . Vamos a mostrar que \mathfrak{M} satisface las condiciones del lema de Zorn, 1.6, lo que mostraría que \mathfrak{M} posee, al menos, un elemento maximal. $\mathfrak{M} \neq \emptyset$, ya que $\mathbf{0} \in \mathfrak{M}$. Vamos a mostrar ahora que \mathfrak{M} está inductivamente ordenado (ver definición 1.19). En efecto, la inclusión \subseteq , induce una

relación de orden parcial sobre \mathfrak{M} . Sea \mathfrak{A} un subconjunto totalmente ordenado de \mathfrak{M} . Vamos a mostrar que \mathfrak{A} posee una cota superior en \mathfrak{M} . Sea

$$\mathfrak{s} := \bigcup_{\mathfrak{a} \in \mathfrak{A}} \mathfrak{a}$$

y mostremos que $\mathfrak{s} \in \mathfrak{M}$ y que es una cota superior de \mathfrak{A} . En efecto, por definición de \mathfrak{s} , $\mathfrak{a} \subseteq \mathfrak{s}, \forall \mathfrak{a} \in \mathfrak{A}$. Vamos a mostrar que \mathfrak{s} es un ideal propio de A . $\mathfrak{s} \neq A$, ya que $1 \notin \mathfrak{s}$, pues \mathfrak{s} es unión de ideales propios. Dados $a, b \in \mathfrak{s}$, existen $\mathfrak{a}, \mathfrak{b} \in \mathfrak{A}$, tales que $a \in \mathfrak{a}, b \in \mathfrak{b}$, como \mathfrak{A} está totalmente ordenado, vale entonces que $\mathfrak{a} \subseteq \mathfrak{b}$ o $\mathfrak{b} \subseteq \mathfrak{a}$. Sin limitación de la generalidad, supongamos que $\mathfrak{a} \subseteq \mathfrak{b}$, entonces $a, b \in \mathfrak{b}$ por lo que $(a + b) \in \mathfrak{b} \subseteq \mathfrak{s}$. Por otra parte, si $x \in A$ y $a \in \mathfrak{s}$, existe un ideal $\mathfrak{a} \in \mathfrak{A}$, tal que $a \in \mathfrak{a}$, entonces $x \cdot a = a \cdot x \in \mathfrak{a} \subseteq \mathfrak{s}$. Por consiguiente \mathfrak{s} es un ideal propio de A y es una cota superior de \mathfrak{A} . \square

Uno de los problemas ancestrales de la teoría de números enteros es el siguiente: Dados p_1, \dots, p_n números enteros primos relativos entre sí y x_1, \dots, x_n números enteros cualesquiera ¿Existe un número entero x , tal que

$$(9.14) \quad x = q_i p_i + x_i?$$

Es decir

$$(9.15) \quad x \equiv x_i \pmod{p_i}$$

Dicho problema es conocido como el problema del resto chino y en la teoría de anillos e ideales el siguiente teorema nos da una respuesta generalizada.

TEOREMA 9.15 (Teorema del Resto Chino). *Sea A un anillo conmutativo con unidad, $\mathfrak{a}_1, \dots, \mathfrak{a}_n$ ideales, tales que $\mathfrak{a}_i + \mathfrak{a}_j = A$, para todo $i \neq j$. Dados $x_1, \dots, x_n \in A$, existe, entonces, un $x \in A$, tal que $x \equiv x_i \pmod{\mathfrak{a}_i}$, para todo $i = 1, \dots, n$.*

DEMOSTRACIÓN. Por inducción sobre n . Para $n = 2$, se tiene

$$a_1 + a_2 = 1$$

para $a_1 \in \mathfrak{a}_1$ y $a_2 \in \mathfrak{a}_2$ adecuados. Entonces $x := x_1 \cdot a_2 + x_2 \cdot a_1$, satisface lo deseado.

Supongamos que el teorema valga para $n - 1$ ideales. Entonces para $i \geq 2$, existen elementos $a_i \in \mathfrak{a}_1, b_i \in \mathfrak{a}_i$, tales que

$$a_i + b_i = 1, \quad i \geq 2.$$

Entonces

$$1 = \prod_{i=2}^n (a_i + b_i) \in \mathfrak{a}_1 + \prod_{i=2}^n \mathfrak{a}_i.$$

Entonces

$$\mathfrak{a}_1 + \prod_{i=2}^n \mathfrak{a}_i = A.$$

Dados $x_1 = 1, x_2 = 0$, como el teorema vale para $n = 2$, existe $y_1 \in A$, tal que

$$y_1 \equiv 1 \pmod{\mathfrak{a}_1}$$

$$y_1 \equiv \left(\prod_{i=2}^n \mathfrak{a}_i \right)$$

Por hipótesis de inducción, para cada $j \geq 2$, $x_j = 1, x_i = 0, i \neq j$, existe $y_j \in A$, tal que

$$y_j \equiv 1 \pmod{\mathfrak{a}_j} \quad y \quad y_j \equiv 0 \pmod{\mathfrak{a}_i} \quad \text{para } i \neq j.$$

Entonces $x = x_1 y_1 + \dots + x_n y_n$ satisface lo deseado. \square

COROLARIO 9.16. *Sean A un anillo conmutativo con unidad, $\mathfrak{a}_1, \dots, \mathfrak{a}_n$ ideales de A , tales que $\mathfrak{a}_i + \mathfrak{a}_j = A$, para $i \neq j$. Sea*

$$f : A \rightarrow \prod_{i=1}^n A/\mathfrak{a}_i$$

el homomorfismo definido por $f(x) := (\pi_1(x), \dots, \pi_n(x))$, donde

$$\pi_i : A \rightarrow A/\mathfrak{a}_i$$

es la aplicación canónica. Entonces $\bigcap_{i=1}^n \mathfrak{a}_i$ es el núcleo de f y

$$\tilde{f} : A / \bigcap_{i=1}^n \mathfrak{a}_i \rightarrow \prod_{i=1}^n A/\mathfrak{a}_i$$

es un isomorfismo.

DEMOSTRACIÓN. Obviamente $\ker f = \bigcap_{i=1}^n \mathfrak{a}_i$. Vamos a mostrar que f es sobreyectiva. Dado $(\bar{x}_1, \dots, \bar{x}_n) \in \prod_{i=1}^n A/\mathfrak{a}_i$, por el teorema del resto chino 9.15, para los representantes $x_1, \dots, x_n \in A$, existe $x \in A$, tal que $x \equiv x_i \pmod{\mathfrak{a}_i}$. entonces $f(x) = (\bar{x}_1, \dots, \bar{x}_n)$. Por lo tanto f es sobreyectiva y \tilde{f} es un isomorfismo. \square

Un resultado interesante es el obtenido en el siguiente

LEMA 9.17. *Dados $\mathfrak{a}_1, \dots, \mathfrak{a}_n$, ideales de un anillo conmutativo con unidad A , tales que $A = \mathfrak{a}_1 + \dots + \mathfrak{a}_n$, entonces, si ν_1, \dots, ν_n , son enteros positivos, también vale $A = \mathfrak{a}^{\nu_1} + \dots + \mathfrak{a}^{\nu_n}$.*

DEMOSTRACIÓN. Procedamos por inducción sobre n . Para $n = 2$, existen $a_1 \in \mathfrak{a}_1$, $a_2 \in \mathfrak{a}_2$, tales que

$$a_1 + a_2 = 1$$

entonces para cualquier entero positivo ν_1 ,

$$(a_1 + a_2)^{\nu_1} = 1 = (a_1^{\nu_1} + \tilde{a}_2) \in \mathfrak{a}_1^{\nu_1} + \mathfrak{a}_2$$

y para cualquier entero positivo ν_2

$$1 = (a_1^{\nu_1} + \tilde{a}_2)^{\nu_2} = \tilde{a}_1 + \tilde{a}_2^{\nu_2} \in \mathfrak{a}_1^{\nu_1} + \mathfrak{a}_2^{\nu_2}.$$

Por consiguiente $\mathfrak{a}_1^{\nu_1} + \mathfrak{a}_2^{\nu_2} = A$.

Supongamos que el lema sea válido para $n - 1$, $n \geq 3$, ideales, que cumplan con la hipótesis del lema. Dados $\mathfrak{a}_1, \dots, \mathfrak{a}_n$, tales que $\mathfrak{a}_1 + \dots + \mathfrak{a}_n = A$, si $b := \mathfrak{a}_1 + \mathfrak{a}_2$, por hipótesis de inducción, el lema vale para los $n - 1$ ideales $b, \mathfrak{a}_3, \dots, \mathfrak{a}_n$, y dados μ, ν_3, \dots, ν_n , enteros positivos, $b^\mu + \mathfrak{a}_3^{\nu_3} + \dots + \mathfrak{a}_n^{\nu_n} = A$. Entonces existen $b \in b^\mu$, $c \in (\mathfrak{a}_3^{\nu_3} + \dots + \mathfrak{a}_n^{\nu_n})$, tales que

$$b + c = 1.$$

Como $b \in b^\mu = (\mathfrak{a}_1 + \mathfrak{a}_2)^\mu$, existen $a_1 \in \mathfrak{a}_1^\mu$ y $a_2 \in \mathfrak{a}_2$, tales que

$$b = a_1 + a_2.$$

Entonces

$$1 = a_2 + (a_1 + c) = a_2 + d, \quad a_2 \in \mathfrak{a}_2, \quad d := (a_1 + c) \in (\mathfrak{a}_1^\mu + \mathfrak{a}_3^{\nu_3} + \dots + \mathfrak{a}_n^{\nu_n}).$$

Entonces

$$1 = (a_2 + d)^{\nu_2} = a_2^{\nu_2} + \tilde{d}, \quad a_2^{\nu_2} \in \mathfrak{a}_2^{\nu_2}, \quad \tilde{d} \in (\mathfrak{a}_1^\mu + \mathfrak{a}_3^{\nu_3} + \dots + \mathfrak{a}_n^{\nu_n}).$$

Poniendo $\nu_1 := \mu$, se obtiene, entonces que $\mathfrak{a}_1^{\nu_1} + \dots + \mathfrak{a}_n^{\nu_n} = A$. \square

9.3.1. Ejercicios y Complementos.

1. Mostrar que $\mathbf{0}$ es un ideal primo Ssi A es un anillo de integridad.
2. Sea $(\mathbb{Z}, +, \cdot)$ el anillo de los números enteros. Mostrar que el ideal $\mathfrak{p} := (p)$, $p \in \mathbb{Z}$ es primo Ssi p es un número primo o $p = 0$. Mostrar, además que en \mathbb{Z} todo ideal primo es también maximal.
3. Mostrar que el ideal $\mathbf{0}$ es primo Ssi el anillo A es un dominio entero.
4. Sea $\varphi : A \rightarrow B$ un homomorfismo de anillos comutativos con unidad y B un dominio entero. Mostrar que $\ker \varphi$ es entonces un ideal primo de A . En particular, si $A = \mathbb{Z}$, entonces $\ker \varphi = (p)$, donde p es un número primo, llamado la *característica* del dominio entero B . Los dominios enteros de característica 0 poseen un subanillo isomorfo a \mathbb{Z} , mientras que los de característica $p \neq 0$ poseen un subanillo isomorfo a \mathbb{Z}_p .
5. Sea $\varphi : A \rightarrow B$ un homomorfismo de anillos comutativos con unidad. Mostrar que si $\mathfrak{q} \in \text{Spec } B$, entonces $\varphi^{-1}[\mathfrak{q}] \in \text{Spec}_{\ker \varphi} A$.
6. Dados un anillo A y un ideal \mathfrak{a} de A , mostrar, usando el segundo teorema de isomorfía, que los ideales primos (maximales) de A/\mathfrak{a} están en correspondencia biunívoca con los ideales primos (maximales) de A que contienen al ideal \mathfrak{a} y que éstos son de la forma $\mathfrak{p}/\mathfrak{a}$, donde \mathfrak{p} es un ideal primo (maximal) de A que contiene al ideal \mathfrak{a} .
7. Mostrar que todo ideal \mathfrak{a} de un anillo comutativo con unidad A está contenido en un ideal maximal. (Ayuda: aplicar teorema 9.14 al anillo A/\mathfrak{a}).
8. Sea $\varphi : A \rightarrow B$ un homomorfismo de anillos. Mostrar que si $\mathfrak{n} \in \Omega(B)$, entonces $\varphi^{-1}[\mathfrak{n}] \in \Omega_{\ker \varphi}(A)$.
9. Sea A un anillo comutativo con unidad. Decimos que $x \in A$ es un *elemento nilpotente*, si existe $n \in \mathbb{Z}^+$, tal que $x^n = 0$. Mostrar que el conjunto

$$\text{r}(A) := \{x \in A \mid x \text{ es nilpotente}\}$$

es un ideal de A , llamado el *nil radical* o *radical* de A . (Ayuda: para mostrar la cerradura respecto de la suma, si $x^n = 0 = y^m$, definir $N := n + m$ y aplicar binomio de Newton).

10. Mostrar que $\text{r}(A) \subseteq \bigcap_{\mathfrak{p} \in \text{Spec } A} \mathfrak{p}$. (En realidad, como veremos más adelante, subsiste la igualdad. Ver teorema 9.24).
11. Si \mathfrak{a} es un ideal del anillo comutativo con unidad A , mostrar que el conjunto

$$\text{r}(\mathfrak{a}) := \{x \in A \mid x^n \in \mathfrak{a} \text{ para algún } n \in \mathbb{Z}^+\}$$

es un ideal de A que contiene al ideal \mathfrak{a} , llamado el *radical* del ideal \mathfrak{a} . Mostrar también que $\text{r}(A/\mathfrak{a}) = \text{r}(\mathfrak{a})$ y que $\text{r}(A) = \text{r}(\mathbf{0})$.

12. Decimos que un ideal \mathfrak{a} de un anillo comutativo con unidad A es un *ideal radical*, si $\text{r}(\mathfrak{a}) = \mathfrak{a}$. Mostrar que todo ideal primo es un ideal radical. (La conversa no es, en general, válida).
13. Decimos que un ideal propio \mathfrak{q} de un anillo comutativo con unidad A es un *ideal primario*, si $x \cdot y \in \mathfrak{q}$ y $x \notin \mathfrak{q}$, entonces $y \in \text{r}(\mathfrak{q})$. Mostrar que si \mathfrak{p} es un ideal primo, entonces para cualquier $n \in \mathbb{Z}^+$, \mathfrak{p}^n es un ideal primario y que si \mathfrak{q} es un ideal primario, entonces $\text{r}(\mathfrak{q})$ es un ideal primo. En particular $\text{r}(\mathfrak{p}^n) = \mathfrak{p}$. (En la teoría de ideales los ideales primarios juegan un poco el papel de los números primos en los enteros, pues se demuestra que todo ideal de un anillo comutativo con unidad, es producto de ideales primarios). (Ver por ejemplo [2], [17] o [15]).

14. Sean \mathfrak{p} un ideal primo de un anillo comutativo con unidad A y S un subconjunto de A , tal que $S \subseteq \mathfrak{p}$. Mostrar que entonces \mathfrak{p} contiene al ideal (S) generado por el subconjunto S .
15. Sea p_1, \dots, p_n números primos distintos, y para cada $i = 1, \dots, n$, $q_i := p_i^{r_i}$, donde $r_i \in \mathbb{Z}^+$. Utilizar el resultado del ejercicio 4.2.4.12, para mostrar que si $m := \prod_{i=1}^n q_i$, entonces $m\mathbb{Z} = \bigcap_{i=1}^n q_i\mathbb{Z}$. Mostrar, además que se tiene un isomorfismo $\tilde{f} : \mathbb{Z}_m \rightarrow \prod_{i=1}^n \mathbb{Z}_{q_i}$.
16. Dados los números $p_1 := 3, p_2 = 5, p_3 = 7$ y $x_1 := 4, x_2 := 10, x_3 = 15$, encontrar un número $x \in \mathbb{Z}$, tal que $x \equiv x_i \pmod{p_i}, i = 1, 2, 3$.

9.3.2. Conjuntos Algebraicos y Topología de Zariski. De aquí en adelante, salvo indicación de lo contrario, todo anillo será comutativo con unidad. Por lo mostrado en el ejercicio 9.3.1,14, nos limitaremos a definir los conjuntos algebraicos sobre ideales.

Sean $X := \text{Spec } A$, donde A es un anillo, \mathfrak{a} un ideal de A . Al conjunto

$$\mathfrak{V}(\mathfrak{a}) := \{\mathfrak{p} \in X \mid \mathfrak{a} \subseteq \mathfrak{p}\}$$

lo llamamos el *conjunto algebraico abstracto*¹ o *variedad algebraica abstracta* generado por el ideal \mathfrak{a} . En general decimos que un subconjunto $V \subseteq X$ es un *conjunto algebraico abstracto*, si existe un ideal \mathfrak{a} del anillo A , tal que $V = V(\mathfrak{a})$.

Dado un subconjunto $V \subseteq X$, definimos

$$\mathfrak{J}(V) := \{x \in A \mid x \in \mathfrak{p}, \forall \mathfrak{p} \in V\}$$

$\mathfrak{J}(V) \neq \emptyset$, ya que $0 \in \mathfrak{J}(V), \forall V \subseteq X$ y es un ideal de A .

TEOREMA 9.18 (Propiedades de \mathfrak{V}). \mathfrak{V} es una aplicación

$$\mathfrak{V} : \mathfrak{J}(A) \rightarrow \mathcal{P}(X)$$

y tiene las siguientes propiedades:

- a) Si $\mathfrak{a} \subseteq \mathfrak{b}$, entonces $\mathfrak{V}(\mathfrak{b}) \subseteq \mathfrak{V}(\mathfrak{a})$, es decir \mathfrak{V} invierte inclusiones.
- b) $\mathfrak{V}(\emptyset) = X$ y $\mathfrak{V}(A) = \emptyset$, es decir X y \emptyset son conjuntos algebraicos.
- c) $\mathfrak{V}(\mathfrak{a} \cdot \mathfrak{b}) = \mathfrak{V}(\mathfrak{a} \cap \mathfrak{b}) = \mathfrak{V}(\mathfrak{a}) \cup \mathfrak{V}(\mathfrak{b})$. Es decir la unión de dos conjuntos algebraicos es un conjunto algebraico.
- d) Dada una familia de ideales $(\mathfrak{a}_i)_{i \in I}$, $\mathfrak{V}(\sum_{i \in I} \mathfrak{a}_i) = \bigcap_{i \in I} \mathfrak{V}(\mathfrak{a}_i)$, es decir la intersección sobre una familia cualquiera de conjuntos algebraicos es un conjunto algebraico.

DEMOSTRACIÓN.

- a) Supongamos que $\mathfrak{a} \subseteq \mathfrak{b}$, entonces si $\mathfrak{p} \in \mathfrak{V}(\mathfrak{b})$, $\mathfrak{b} \subseteq \mathfrak{p}$ y como $\mathfrak{a} \subseteq \mathfrak{b}$, resulta $\mathfrak{a} \subseteq \mathfrak{p}$. Por lo tanto $\mathfrak{p} \in \mathfrak{V}(\mathfrak{a})$.
- b) Queda al lector como ejercicio.
- c) Considerando que

$$\mathfrak{a} \cdot \mathfrak{b} \subseteq \mathfrak{a} \cap \mathfrak{b} \subseteq \mathfrak{a} \quad \text{y que} \quad \mathfrak{a} \cdot \mathfrak{b} \subseteq \mathfrak{a} \cap \mathfrak{b} \subseteq \mathfrak{b}$$

obtenemos, por inciso a),

$$(9.16) \quad \mathfrak{V}(\mathfrak{a}) \subseteq \mathfrak{V}(\mathfrak{a} \cap \mathfrak{b}) \subseteq \mathfrak{V}(\mathfrak{a} \cdot \mathfrak{b}) \quad \text{y} \quad \mathfrak{V}(\mathfrak{b}) \subseteq \mathfrak{V}(\mathfrak{a} \cap \mathfrak{b}) \subseteq \mathfrak{V}(\mathfrak{a} \cdot \mathfrak{b})$$

¹A diferencia de los conjuntos algebraicos obtenidos como raíces de conjuntos de polinomios en el espacio afín A^n, \mathbb{R}^n o \mathbb{C}^n . (Ver página 227)

Entonces, de (9.16), resulta

$$(9.17) \quad \mathfrak{B}(\mathfrak{a}) \cup \mathfrak{B}(\mathfrak{b}) \subseteq \mathfrak{B}(\mathfrak{a} \cap \mathfrak{b}) \subseteq \mathfrak{B}(\mathfrak{a} \cdot \mathfrak{b})$$

Vamos a mostrar que

$$(9.18) \quad \mathfrak{B}(\mathfrak{a} \cdot \mathfrak{b}) \subseteq \mathfrak{B}(\mathfrak{a}) \cup \mathfrak{B}(\mathfrak{b})$$

Sea $\mathfrak{p} \in \mathfrak{B}(\mathfrak{a} \cdot \mathfrak{b})$, entonces $\mathfrak{a} \cdot \mathfrak{b} \subseteq \mathfrak{p}$. Dados $x \in \mathfrak{a}, y \in \mathfrak{b}, xy \in \mathfrak{a} \cdot \mathfrak{b} \subseteq \mathfrak{p}$. Como \mathfrak{p} es un ideal primo, si $x \notin \mathfrak{p}$ debe valer que $\mathfrak{b} \subseteq \mathfrak{p}$ y si $y \notin \mathfrak{p}$ entonces $\mathfrak{a} \subseteq \mathfrak{p}$, por consiguiente $\mathfrak{p} \in \mathfrak{B}(\mathfrak{b}) \vee \mathfrak{p} \in \mathfrak{B}(\mathfrak{a})$ y (9.18) vale. De (9.17) y (9.18) se obtiene la igualdad deseada.

d) Queda al lector como ejercicio

□

Los lectores que ya han llevado un curso de topología observarán que los incisos a)-d) del teorema 9.18, son los axiomas de los conjuntos cerrados de una topología sobre X (ver, por ejemplo [8]), llamada la topología de Zariski. Este espacio es de suma importancia en la teoría de los esquemas² de la geometría algebraica moderna y es llamado el esquema afín. Un esquema es una generalización abstracta de lo que es una variedad algebraica y es localmente isomorfo a un esquema afín, para algún anillo adecuado. Para mayores referencias sobre la teoría de los esquemas ver, por ejemplo [18].

TEOREMA 9.19 (Propiedades de \mathfrak{J}). \mathfrak{J} es una aplicación

$$\mathfrak{J} : \mathcal{P}(X) \rightarrow \mathfrak{J}(A)$$

y tiene las siguientes propiedades:

- a) Si $V \subseteq W$, entonces $\mathfrak{J}(W) \subseteq \mathfrak{J}(V)$, es decir \mathfrak{J} invierte contenciones.
- b) $\mathfrak{J}(\bigcup_{i \in I} V_i) = \bigcap_{i \in I} \mathfrak{J}(V_i)$.
- c) Dada una familia $(V_i)_{i \in I}$ de subconjuntos de X , $\sum_{i \in I} \mathfrak{J}(V_i) \subseteq \mathfrak{J}(\bigcap_{i \in I} V_i)$.
- d) $V \subseteq \mathfrak{B}(\mathfrak{J}(V))$ y $\mathfrak{a} \subseteq \mathfrak{J}(\mathfrak{B}(\mathfrak{a}))$
- e) $\mathfrak{J}(X) = \bigcap_{\mathfrak{p} \in \text{Spec } A} \mathfrak{p} = r(A)$. (Ver teorema 9.24)
- f) $\mathfrak{J}(\emptyset) = A$

DEMOSTRACIÓN.

a) Queda al lector como ejercicio.

b) Por inciso a) vale

$$(9.19) \quad \mathfrak{J}\left(\bigcup_{i \in I} V_i\right) \subseteq \mathfrak{J}(V_i), \forall i \in I \Rightarrow \mathfrak{J}\left(\bigcup_{i \in I} V_i\right) \subseteq \bigcap_{i \in I} \mathfrak{J}(V_i)$$

Vamos a mostrar que también vale

$$(9.20) \quad \bigcap_{i \in I} \mathfrak{J}(V_i) \subseteq \mathfrak{J}\left(\bigcup_{i \in I} V_i\right)$$

En efecto, sea $x \in \bigcap_{i \in I} \mathfrak{J}(V_i)$, entonces $x \in \mathfrak{J}(V_i) \forall i \in I$, entonces $x \in \mathfrak{p}$,

$\forall \mathfrak{p} \in V_i, \forall i \in I$, lo que implica que $x \in \mathfrak{J}\left(\bigcup_{i \in I} V_i\right)$. Lo que muestra (9.20). De (9.19) y (9.20) se obtiene la igualdad deseada.

c) Queda al lector como ejercicio.

²Dicha teoría fue desarrollada por el matemático franco-alemán Alexander Grothendieck

- d) Queda al lector como ejercicio.
- e) Queda al lector como ejercicio.
- f) Queda al lector como ejercicio.

□

9.3.3. Anillo de Fracciones y Localización. Dado un anillo A , nuestra meta es construirnos, inspirados en la construcción de los números racionales \mathbb{Q} a partir de los números enteros \mathbb{Z} un anillo en el cual los elementos de un cierto subconjunto $S \subseteq A$ sean invertibles. Para entender la idea empezaremos construyendones el campo de fracciones de un dominio entero A .

Sea, entonces, A un dominio entero y $S := A \setminus \{0\}$, el conjunto S es entonces cerrado bajo el producto del anillo. Consideremos $\mathbb{Q}(A) := A \times S / \sim$, el conjunto de las clases de equivalencia respecto de la relación \sim , sobre $A \times S$, definida por $(a, s) \sim (b, t) \Leftrightarrow a \cdot t = b \cdot s$, o de forma equivalente $a \cdot t - b \cdot s = 0$. Si denotamos por $\frac{a}{s}$ la clase de equivalencia de (a, s) y definimos

$$(9.21) \quad \frac{a}{s} + \frac{b}{t} := \frac{a \cdot t + b \cdot s}{s \cdot t}$$

y

$$(9.22) \quad \frac{a}{s} \cdot \frac{b}{t} := \frac{a \cdot b}{s \cdot t}$$

, entonces, tal y como mostramos las propiedades de los números racionales \mathbb{Q} , el lector podrá comprobar que dichas operaciones están bien definidas y la validez del siguiente

TEOREMA 9.20. *Si A es un dominio entero, entonces $(\mathbb{Q}(A), +, \cdot)$ es un campo, llamado el campo de fracciones del dominio entero A . La aplicación*

$$i : A \rightarrow \mathbb{Q}(A)$$

definida por $i(a) := \frac{a}{1}$ es un homomorfismo inyectivo de anillos, por lo que $\mathbb{Q}(A)$ posee un subanillo isomorfo a A .

Siempre en un dominio entero, en lugar de considerar S como el conjunto de todos los elementos distintos de 0, podemos limitarnos a considerar un subconjunto S de A que tenga las siguientes propiedades: $1 \in S$ y S cerrado bajo el producto de A , es decir un submonoide de (A, \cdot) . Un conjunto S con estas propiedades se denomina un *conjunto multiplicativo*. Sobre $A \times S$ definimos la relación de equivalencia \sim del mismo modo que lo hicimos en el caso precedente y denotaremos por $S^{-1}A := A \times S / \sim$. Las operaciones binarias respectivas se definen exactamente igual que en (9.21) y (9.22) y se comprueba facilmente que éstas están bien definidas y que vale el siguiente

TEOREMA 9.21. *Sea A un dominio entero y S un subconjunto multiplicativo de A , tal que $0 \notin S$. Entonces $(S^{-1}A, +, \cdot)$ es un anillo, en el cual todos los elementos de S son invertibles. La aplicación*

$$i : A \rightarrow S^{-1}A$$

definida por $i(a) := \frac{a}{1}$ es un homomorfismo inyectivo de anillos, por lo que $S^{-1}A$ posee un subanillo isomorfo a A .

Nuestro siguiente paso es generalizar esta construcción al caso de un anillo commutativo con unidad cualquiera. Como A ya no es necesariamente un dominio entero, debemos considerar que pueden existir divisores de 0, por lo que es necesario modificar un poco

nuestra relación de equivalencia. En particular en un subconjunto multiplicativo S de A pueden existir divisores de cero y S contener al 0.

Consideremos entonces S un subconjunto multiplicativo del anillo A y definamos sobre $A \times S$ la siguiente relación

$$(a, s) \sim (b, t) : \Leftrightarrow \exists r \in S \text{ tal que } r \cdot (a \cdot t - b \cdot s) = 0$$

Entonces \sim es una relación de equivalencia sobre $A \times S$. Siendo la reflexividad y simetría obvias, mostremos la transitividad. En efecto, sean $(a, s), (b, t), (c, r) \in A \times S$, tales que

$$(a, s) \sim (b, t) \quad y \quad (b, t) \sim (c, r),$$

entonces existen $u, v \in S$, tales que

$$(9.23) \quad u \cdot (a \cdot t - b \cdot s) = 0 \quad y \quad v \cdot (b \cdot r - c \cdot t) = 0$$

Multiplicando en (9.23) las ecuaciones por $u \cdot v$ y $r \cdot s$ respectivamente y sumando se obtiene

$$(9.24) \quad u \cdot r \cdot t(a \cdot v - c \cdot s) = 0, \quad u \cdot r \cdot t \in S$$

lo que muestra que \sim es transitiva. Por lo tanto \sim es relación de equivalencia.

Por $S^{-1}A$ denotaremos al conjunto cociente de las clases de equivalencia respecto de la relación \sim . Si definimos en $S^{-1}A$ la suma y producto como en (9.21) y (9.22) respectivamente, entonces éstas están bien definidas. Mostraremos que la suma está bien definida, dejando al lector la sencilla demostración para el producto. Sean $(a, s), (\tilde{a}, \tilde{s})$ dos representantes de la fracción $\frac{a}{s}$ y $(b, t), (\tilde{b}, \tilde{t})$ dos representantes de la fracción $\frac{b}{t}$, entonces existen $u, v \in S$, tales que

$$(9.25) \quad u \cdot (a \cdot \tilde{s} - \tilde{a} \cdot s) = 0 \quad y \quad v \cdot (b \cdot \tilde{t} - \tilde{b} \cdot t) = 0,$$

debemos mostrar

$$\frac{a \cdot t + b \cdot s}{s \cdot t} = \frac{\tilde{a} \cdot \tilde{t} + \tilde{b} \cdot \tilde{s}}{\tilde{s} \cdot \tilde{t}}.$$

En efecto, considerando las ecuaciones (9.25)

$$u \cdot v((a \cdot t + b \cdot s) \cdot \tilde{s} \cdot \tilde{t} - (\tilde{a} \cdot \tilde{t} + \tilde{b} \cdot \tilde{s}) \cdot s \cdot t) = t \cdot \tilde{t} \cdot v(u \cdot (a \cdot \tilde{s} - \tilde{a} \cdot s)) + s \cdot \tilde{s} \cdot u \cdot (v \cdot (b \cdot \tilde{t} - \tilde{b} \cdot t)) = 0$$

donde $u \cdot v \in S$. Lo que muestra que la suma está bien definida.

Se tiene entonces el siguiente teorema, cuya sencilla demostración dejamos al lector como ejercicio.

TEOREMA 9.22. $(S^{-1}A, +, \cdot)$ es un anillo conmutativo con unidad, siendo $\frac{0}{1}$ el elemento neutro de la suma y $\frac{1}{1}$ el elemento neutro del producto. Se tiene, además que la aplicación

$$\varphi_S : A \rightarrow S^{-1}A$$

definida por $\varphi_S(a) := \frac{a}{1}$, $\forall a \in A$ es un homomorfismo de anillos y, en general, no es inyectiva. Se tiene, también, que todos los elementos de $\varphi_S[S]$ son invertibles en $S^{-1}A$, siendo $\frac{1}{s}$ el inverso de $\frac{s}{1}$.

El anillo $S^{-1}A$ recibe el nombre de *anillo de fracciones* de A respecto del subconjunto multiplicativo S .

Si $0 \in S$, entonces, como el lector comprobará con facilidad, $S^{-1}A = \left\{ \frac{0}{1} \right\}$

A continuación daremos algunos ejemplos de subconjuntos multiplicativos utilizados frecuentemente.

EJEMPLOS 9.4.

1. Si A^* es el subconjunto de elementos invertibles del anillo A , entonces $S := A^*$ es un subconjunto multiplicativo de A . En este caso $S^{-1}A = A$.
2. Si x es un elemento no nilpotente del anillo A , entonces

$$S := \{1, x, x^2, x^3, \dots\}$$

es un subconjunto multiplicativo de A que no contiene a 0. $S^{-1}A$ consta de las fracciones cuyo denominador son potencias de x .

3. Si \mathfrak{p} es un ideal primo de un anillo A , entonces $S := A \setminus \{\mathfrak{p}\}$ es un subconjunto multiplicativo de A .
4. $S := \bigcup_{\mathfrak{p} \in \text{Spec } A} \mathfrak{p}$ es un subconjunto multiplicativo del anillo A .

Surge la pregunta ¿Cómo son los ideales del anillo $S^{-1}A$? Si \mathfrak{a} es un ideal del anillo A y S un subconjunto multiplicativo, entonces

$$S^{-1}\mathfrak{a} := \left\{ \frac{a}{s} \mid a \in \mathfrak{a}, s \in S \right\}$$

es un ideal de $S^{-1}A$, en efecto, dados $\frac{a}{s}, \frac{b}{t} \in S^{-1}\mathfrak{a}$, entonces $\frac{a}{s} + \frac{b}{t} = \frac{a \cdot t + b \cdot s}{s \cdot t} \in S^{-1}\mathfrak{a}$, ya que $(a \cdot t + b \cdot s) \in \mathfrak{a}$ y $s \cdot t \in S$.

Dado $\frac{a}{s} \in S^{-1}\mathfrak{a}$ y $\frac{x}{u} \in S^{-1}A$, entonces $\frac{x}{u} \cdot \frac{a}{s} = \frac{x \cdot a}{u \cdot s} \in S^{-1}\mathfrak{a}$, ya que $x \cdot a \in \mathfrak{a}$ y $s \cdot t \in S$.

Si \mathfrak{a} es un ideal del anillo A y S un subconjunto multiplicativo, tal que $\mathfrak{a} \cap S \neq \emptyset$, entonces

$$S^{-1}\mathfrak{a} = S^{-1}A$$

ya que $\frac{s}{1}, s \in \mathfrak{a} \cap S$ es un elemento invertible en $S^{-1}\mathfrak{a}$. Entonces $S^{-1}\mathfrak{a}$ sólo puede ser un ideal propio si $\mathfrak{a} \cap S = \emptyset$.

Vamos a ver que todos los ideales de $S^{-1}A$ son de la forma $S^{-1}\mathfrak{a}$, donde \mathfrak{a} es un ideal de A . En efecto, sea $\tilde{\mathfrak{a}}$ un ideal de $S^{-1}A$, entonces

$$\mathfrak{a} := \varphi_S^{-1}[\tilde{\mathfrak{a}}] = \{x \in A \mid \frac{x}{1} \in \tilde{\mathfrak{a}}\}$$

es un ideal de A . Dado $\frac{x}{s} \in \tilde{\mathfrak{a}}$, entonces $\frac{x}{1} \in \tilde{\mathfrak{a}}$, ya que $\frac{x}{1} = \frac{s}{1} \cdot \frac{x}{s}$, por lo que $x \in \mathfrak{a}$ y $\frac{x}{s} \in S^{-1}\mathfrak{a}$. Por otra parte, si $\frac{x}{s} \in S^{-1}\mathfrak{a}$, entonces, por definición de \mathfrak{a} , $\frac{x}{1} \in \tilde{\mathfrak{a}}$ y $\frac{x}{s} = \frac{1}{s} \cdot \frac{x}{1} \in \tilde{\mathfrak{a}}$. Por lo tanto $\tilde{\mathfrak{a}} = S^{-1}\mathfrak{a}$.

Para los ideales primos se tiene el siguiente

TEOREMA 9.23. *Los ideales primos de $S^{-1}A$ están en correspondencia biunívoca con los ideales primos de A que no intersectan al subconjunto S . Si $\tilde{\mathfrak{p}}$ es un ideal de $S^{-1}A$, entonces existe un único ideal primo \mathfrak{p} de A , $\mathfrak{p} \cap S = \emptyset$, tal que $\tilde{\mathfrak{p}} = S^{-1}\mathfrak{p}$.*

DEMOSTRACIÓN. En efecto, como ya vimos, si $\mathfrak{p} := \varphi_S^{-1}[\tilde{\mathfrak{p}}]$, entonces $\tilde{\mathfrak{p}} = S^{-1}\mathfrak{p}$, y, como se demostró en el corolario 9.10, \mathfrak{p} es un ideal primo, por ser imagen inversa de un ideal primo y \mathfrak{p} no intersecta a S , pues de lo contrario $\tilde{\mathfrak{p}} = S^{-1}\mathfrak{p}$ no sería un ideal primo. Por otra parte, si \mathfrak{q} es otro ideal primo, tal que $\mathfrak{q} \cap S = \emptyset$ y $S^{-1}\mathfrak{q} = S^{-1}\mathfrak{p}$, vamos a mostrar que $\mathfrak{p} = \mathfrak{q}$. Sea $a \in \mathfrak{p}$, entonces $\frac{a}{1} \in S^{-1}\mathfrak{p} = S^{-1}\mathfrak{q}$, entonces existe $b \in \mathfrak{q}$, $s \in S$, tales que $\frac{b}{s} = \frac{a}{1}$, por lo que existe $u \in S$, tal que $u \cdot (a \cdot s - b) = 0$, es decir $u \cdot s \cdot a = b \in \mathfrak{q}$, como \mathfrak{q} ideal primo y $s \cdot u \notin \mathfrak{q}$, resulta $a \in \mathfrak{q}$, $\forall a \in \mathfrak{p}$, por lo que $\mathfrak{p} \subseteq \mathfrak{q}$, de forma análoga se muestra que $b \in \mathfrak{p}$, $\forall b \in \mathfrak{q}$, por lo tanto $\mathfrak{p} = \mathfrak{q}$. \square

Del ejercicio 9.3.1,10, sabemos que si A es un anillo conmutativo con unidad, entonces el nilradical de A , $r(A) \subseteq \bigcap_{\mathfrak{p} \in \text{Spec } A} \mathfrak{p}$, vamos ahora a mostrar, en el siguiente teorema, que la igualdad subsiste.

TEOREMA 9.24. *Sea A un anillo conmutativo con unidad. Entonces el nilradical*

$$r(A) = \bigcap_{\mathfrak{p} \in \text{Spec } A} \mathfrak{p}.$$

DEMOSTRACIÓN. Sólo nos falta mostrar que

$$(9.26) \quad \bigcap_{\mathfrak{p} \in \text{Spec } A} \mathfrak{p} \subseteq r(A).$$

En efecto, supongamos que $x \in \bigcap_{\mathfrak{p} \in \text{Spec } A} \mathfrak{p}$, y que x no sea nilpotente. Entonces $x^n \neq 0$, $\forall n \in \mathbb{Z}^+$ y el conjunto

$$S := \{1, x, x^2, \dots\}$$

es un conjunto multiplicativo, $0 \notin S$. Como $x \in \mathfrak{p}$, $\forall \mathfrak{p} \in \text{Spec } A$, tendríamos, entonces, que para cualquier ideal primo \mathfrak{p} , $\mathfrak{p} \cap S \neq \emptyset$, y $S^{-1}\mathfrak{p} = S^{-1}A$. Entonces, por teorema 9.23, $S^{-1}A$ no tendría ideales primos, en contradicción a que todo anillo conmutativo con unidad posee, al menos, un ideal maximal, el cual es primo. Por lo tanto vale (9.26). \square

Aplicando el teorema 9.24 al anillo A/\mathfrak{a} , donde \mathfrak{a} es un ideal de A , se obtiene el

COROLARIO 9.25. *Si \mathfrak{a} es un ideal del anillo conmutativo con unidad A , entonces su radical*

$$r(\mathfrak{a}) = \bigcap_{\mathfrak{p} \in \text{Spec}_{\mathfrak{a}} A} \mathfrak{p}$$

También como un corolario, se obtiene el famoso teorema de los ceros de Hilbert, versión abstracta.

COROLARIO 9.26 (Teorema de los Ceros de Hilbert). *Si \mathfrak{a} es un ideal del anillo conmutativo con unidad A , entonces $\mathfrak{J}(\mathfrak{B}(\mathfrak{a})) = r(\mathfrak{a})$.*

DEMOSTRACIÓN. $x \in \mathfrak{J}(\mathfrak{B}(\mathfrak{a}))$ Ssi $x \in \mathfrak{p}$, $\forall \mathfrak{p} \in \text{Spec}_{\mathfrak{a}} A$ Ssi $x \in \bigcap_{\mathfrak{p} \in \text{Spec}_{\mathfrak{a}} A} \mathfrak{p} = r(\mathfrak{a})$. \square

En sus orígenes la geometría algebraica estudiaba las propiedades de conjuntos de puntos en el espacio afín, \mathbb{R}^n o \mathbb{C}^n satisfacían sistemas de ecuaciones algebraicas (polinomios), como curvas y superficies, llamados conjuntos algebraicos. En su desarrollo posterior se pasa a considerar las llamadas variedades algebraicas, como variedades topológicas, con la propiedad de que cada punto posee una vecindad homeomorfa a algún conjunto algebraico, cuyas propiedades geométricas están intimamente ligadas al comportamiento de un cierto anillo asociado a dicho conjunto y en particular al espectro primo de dicho anillo, lo cual da origen al desarrollo de la teoría de esquemas, que constituye una generalización y abstracción de la teoría de variedades algebraicas, en la cual cada vecindad es homeomorfa a un esquema afín, dado por el espectro de un anillo, dotado de la topología de Zariski. En el estudio de las variedades algebraicas o de los esquemas se distingue entre las llamadas propiedades globales y las propiedades locales, siendo estas últimas las propiedades que son válidas en la vecindad de un cierto punto. En el estudio de las propiedades locales juega un papel muy importante el llamado anillo de las funciones racionales definidas en una vecindad adecuada de un punto, el cual tiene la propiedad de

poseer un único ideal maximal. Esto nos lleva a definir el concepto de anillo local y de localización.

Decimos que un anillo A comunitativo con unidad, es un *anillo local*, si A posee un único ideal maximal \mathfrak{m} . Un anillo local se suele representar por el par (A, \mathfrak{m}) .

Sea A un anillo comunitativo con unidad y $\mathfrak{p} \in \text{Spec } A$, entonces $S := A \setminus \mathfrak{p}$ es un subconjunto multiplicativo de A , que no contiene al 0. Entonces se tiene el siguiente

TEOREMA 9.27. *Si $S := A \setminus \mathfrak{p}$, donde $\mathfrak{p} \in \text{Spec } A$ y A es un anillo comunitativo con unidad, entonces el anillo $A_{\mathfrak{p}} := S^{-1}A$, es un anillo local, siendo $S^{-1}\mathfrak{p}$ su único ideal maximal.*

DEMOSTRACIÓN. En efecto, si $\tilde{\mathfrak{a}}$ es un ideal propio de $A_{\mathfrak{p}}$, entonces $\tilde{\mathfrak{a}} = S^{-1}\mathfrak{a}$, donde \mathfrak{a} es un ideal de A que no intersecta a S , es decir $\mathfrak{a} \subseteq \mathfrak{p}$. Por consiguiente todo ideal propio de $A_{\mathfrak{p}}$ está contenido en $S^{-1}\mathfrak{p}$. Lo que muestra que $S^{-1}\mathfrak{p}$ es el único ideal maximal de $A_{\mathfrak{p}}$. \square

Al anillo $A_{\mathfrak{p}}$ lo llamamos la *localización* del anillo A en el ideal primo \mathfrak{p} .

Desde el punto de vista geométrico estamos dándonos la localización del anillo A en el punto $\mathfrak{p} \in X$, donde $X := \text{Spec } A$ es el esquema afín.

9.3.4. Ejercicios y Complementos.

1. Completar la demostración de los teoremas 9.18 y 9.19.
2. Sea S un subconjunto multiplicativo de un anillo comunitativo con unidad A . Mostrar que las siguientes propiedades de las fracciones usuales de números racionales, también valen en $S^{-1}A$.
 - a) $\frac{x}{s} \cdot \frac{s}{1} = \frac{x}{1}, \forall x \in A, s \in S$
 - b) $\frac{x}{s} \cdot \frac{s}{t} = \frac{x}{t}, \forall x \in A, s, t \in S$
3. Completar la demostración de los teoremas 9.20 y 9.21.
4. Completar la demostración del teorema 9.22.
5. Dado un $\mathfrak{p} \in \text{Spec } A$, donde A es un anillo comunitativo con unidad, mostrar que los ideales primos de $A_{\mathfrak{p}}$, están en correspondencia biunívoca con los ideales primos de A contenidos en el ideal \mathfrak{p}
6. Mostrar que $A_{\mathfrak{p}} \neq \mathbf{0}, \forall \mathfrak{p} \in \text{Spec } A$, donde A es un anillo comunitativo con unidad, no trivial.
7. Si $\Omega(A)$ es el espectro maximal de un anillo comunitativo con unidad A , mostrar que $\mathfrak{J}(A) := \bigcap_{\mathfrak{m} \in \Omega(A)} \mathfrak{m}$ es un ideal de A , llamado el *radical de Jacobson* del anillo A . Mostrar también que $r(A) \subseteq \mathfrak{J}(A)$.
8. Si A es un anillo comunitativo con unidad que solo posee un número finito de ideales maximales $\mathfrak{m}_1, \dots, \mathfrak{m}_n$, mostrar que se tiene un isomorfismo $\tilde{f} : A/\mathfrak{J}(A) \rightarrow \prod_{i=1}^n A/\mathfrak{m}_i$. Un anillo que sólo posee un número finito de ideales maximales se llama un *anillo semilocal*.
9. Mostrar que en el anillo de los enteros \mathbb{Z} , $r(\mathbb{Z}) = \mathfrak{J}(\mathbb{Z}) = \mathbf{0}$.

9.4. Anillos Principales, Noetherianos, de Factorización Única y Euclídeanos

En esta sección introduciremos la noción de anillo principal, que son anillos cuyos ideales son generados por un único elemento. Daremos la definición de anillo noetheriano, que son anillos cuyos ideales son generados por un número finito de elementos. Introduciremos también la noción de anillo de factorización única, en el cual todo elemento posee

una única representación, salvo producto por un elemento invertible en el anillo, como producto de elementos irreducibles, que nos recordará la propiedad de todo número entero de descomponerse, en forma única, como producto de potencias de números primos. (Ver teorema 3.23). Terminaremos esta sección con la noción de anillo euclídeo, que son anillos sobre los cuales está definida una función similar a la función valor absoluto, definida sobre el anillo de los enteros \mathbb{Z} , que nos va a permitir dar una generalización del algoritmo euclídeo y demostraremos que todo anillo euclídeo es un anillo principal.

9.4.1. Anillos Principales. Decimos que un anillo comutativo con unidad, sin divisores de 0, A es un *anillo principal*, si todo ideal de A es un ideal principal.

TEOREMA 9.28. *El anillo $(\mathbb{Z}, +, \cdot)$ es un anillo principal y todos sus ideales son de la forma $n\mathbb{Z}$, $n \in \mathbb{Z}$.*

DEMOSTRACIÓN. En efecto, $(\mathbb{Z}, +, \cdot)$ es un anillo comutativo con unidad y por lema 4.19, todos los subgrupos de $(\mathbb{Z}, +)$ son de la forma $n\mathbb{Z}$, $n \in \mathbb{Z}$ y por consiguiente también los ideales de $(\mathbb{Z}, +, \cdot)$. \square

Como veremos más adelante no todo anillo es principal, pues hay anillos cuyos ideales no son todos principales, como será el caso de ciertos anillos de polinomios.

Decimos que un elemento $a \neq 0$ de un dominio entero A es *irreducible*, si a no es invertible y

$$(9.27) \quad a = bc \Rightarrow b \vee c \text{ invertibles.}$$

Un elemento distinto de 0 no invertible que no es irreducible diremos que es *reducible*.

Se dice que dos elementos a, b de un dominio entero A son *asociados entre sí*, si existe un elemento invertible $e \in A$, tal que $a = eb$.

El lector verificará, como un simple ejercicio, el siguiente

LEMA 9.29. *Sobre un dominio entero A , la relación $a \sim b$ Ssi a y b son asociados es una relación de equivalencia.*

LEMA 9.30. *Dos elementos a, b de un dominio entero A son asociados Ssi $(a) = (b)$.*

DEMOSTRACIÓN. Como a, b son asociados existe un elemento invertible $e \in A$, tal que $a = eb$, entonces $a \in (b)$ y $(a) \subseteq (b)$, por otra parte, como e es invertible $b = e^{-1}a$, de donde $(b) \subseteq (a)$. Por lo tanto $(a) = (b)$.

Por otra parte, si $(a) = (b)$, se tiene entonces que existen $c, d \in A$, tales que $a = cb$ y $b = da$, por lo que $a = c(da) = (cd)a$. Como A es dominio entero, se tiene que $cd = 1$ y c es invertible. Por consiguiente a, b son asociados. \square

LEMA 9.31. *Un elemento a de un dominio entero A es irreducible Ssi $\mathbf{0} \neq (a) \neq A$ y si todo ideal principal b , tal que $(a) \subseteq b$ es igual a (a) o igual a A . Es decir que (a) es un ideal maximal.*

DEMOSTRACIÓN. Si a es irreducible, entonces $a \neq 0$ y $(a) \neq \mathbf{0}$. Como a tampoco es invertible también vale $(a) \neq A$. Sea $b = (b)$ tal que $(a) \subseteq (b)$, entonces, en particular $a \in (b)$, por lo que existe $r \in A$, tal que $a = rb$. Como a irreducible se tiene que r invertible o bien b invertible, de donde resulta $(b) = (a)$ o $(b) = A$. \square

Del lema 9.31, se obtiene, de forma inmediata, para el caso de un anillo principal el siguiente

TEOREMA 9.32. *Un ideal propio \mathfrak{a} , no trivial, de un anillo principal A es maximal Ssi \mathfrak{a} es generado por un elemento irreducible $a \in A$.*

Sea A un dominio entero. Decimos que $a \in A$ divide a $b \in A$, expresado $a | b$, si $b \in (a)$. Entonces se dice que a es un divisor de b en el anillo A . Si $a | b$, entonces existe $r \in A$, tal que $b = ra$ y diremos que b es producto de los factores a y r .

Decimos que $c \in A$ es un divisor común de $a, b \in A$, si $c | a$ y $c | b$.

Decimos que $d \in A$ es un máximo común divisor de $a, b \in A$, si d es un divisor común de a, b y si c es otro divisor común de a, b , entonces $c | d$.

Si $d \in A$ es un máximo común divisor de a, b y $e \in A$ es un elemento invertible, entonces también $\bar{d} := ed$ es un máximo común divisor de a, b . Si d es máximo común divisor de a, b , entonces $a, b \in (d) = (ed) = (\bar{d})$, por lo que \bar{d} es divisor común de a, b . De $(d) = (ed) = (\bar{d})$ resulta que $d | \bar{d}$ y $\bar{d} | d$. Por consiguiente cualquier otro divisor común c divide a \bar{d} . Entonces en un dominio entero A existirán tantos máximo común divisores de $a, b \in A$, como elementos tenga el grupo de elementos invertibles A^* de A .

El siguiente teorema nos garantiza la existencia de un máximo común divisor, para dos elementos distintos de 0 en un anillo principal.

TEOREMA 9.33. *Sea A un anillo principal, $a, b \in A$, elementos distintos de 0 . Si $(a, b) = (c)$, entonces c es un máximo común divisor de a, b .*

DEMOSTRACIÓN. Si $(a, b) = (c)$, entonces $a \in (c)$ y $b \in (c)$, por lo que c es un divisor común de a, b . Si d es otro divisor común de a, b , entonces existen $a_1, b_1 \in A$, tales que $a = da_1, b = db_1$. Como $c \in (a, b)$, existen $s, r \in A$, tales que $c = ra + sb = rda + sdb$. Por lo tanto $d | c$ y c es un máximo común divisor de a, b . \square

Decimos que un elemento p de un dominio entero A es un *elemento primo*, si

- a) $p \neq 0$.
- b) (p) es un ideal primo.

Del inciso c) resulta que p no puede ser invertible y que $p | ab \Rightarrow p | a \vee p | b$.

LEMA 9.34. *Todo elemento primo en un dominio entero A es irreducible.*

DEMOSTRACIÓN. En efecto, sea $p \in A$ un elemento primo, y $a, b \in A$, tales que $p = ab$, entonces $ab \in (p)$ y, por definición de elemento primo $p | a \vee p | b$. Supongamos, sin limitación de la generalidad, que $p | a$, entonces existe $a_1 \in A$, tal que $a = a_1p$ y $p = (pa_1)b = p(a_1b)$, de donde resulta que $a_1b = 1$, por consiguiente b es invertible y p es irreducible. \square

LEMA 9.35. *Un elemento p de un dominio entero es primo Ssi el ideal (p) es un ideal primo distinto de 0 .*

DEMOSTRACIÓN. En efecto, por definición de elemento primo, (p) es un ideal primo. Por otra parte si (p) es un ideal primo, $(p) \neq A$ y p no es invertible y por hipótesis $p \neq 0$. Dados $a, b \in A$, tales que $ab \in (p)$, entonces, como (p) es un ideal primo $a \in (p)$ o $b \in (p)$. Por lo tanto p es un elemento primo de A . \square

TEOREMA 9.36. *En un anillo principal A es todo elemento irreducible un elemento primo.*

DEMOSTRACIÓN. En efecto, si a es un elemento irreducible de A , entonces, por definición de elemento irreducible, (a) es un ideal maximal y por consiguiente primo. Entonces, por lema 9.35, a es un elemento primo de A . \square

Como consecuencia del teorema 9.36 y del lema 9.35 se obtiene el siguiente

COROLARIO 9.37. *En un anillo principal A , en analogía al anillo de los enteros \mathbb{Z} , es todo ideal primo, distinto de $\mathbf{0}$ un ideal maximal.*

TEOREMA 9.38. *Si A es un anillo principal y $\varphi : A \rightarrow B$ un homomorfismo sobreyectivo de anillos, entonces B es un anillo principal.*

DEMOSTRACIÓN. Sea b un ideal cualquiera de B , entonces $\mathfrak{a} := \varphi^{-1}[b]$ es un ideal de A y, por la sobreyectividad de φ , $b = \varphi[\varphi^{-1}[b]]$. Como A es anillo principal, entonces existe $a_0 \in A$, tal que $\mathfrak{a} = (a_0)$. Dado $b \in b$, existe, nuevamente por la sobreyectividad de φ , $a \in A$, tal que $b = \varphi(a)$. Entonces $a \in \varphi^{-1}[b]$ y existe $r \in A$, tal que $a = ra_0$, entonces $b = \varphi(a) = \varphi(r)\varphi(a_0) \in (\varphi(a_0))$, por lo que $b \subseteq (\varphi(a_0))$. Por otra parte si $b \in (\varphi(a_0))$, entonces, existe $\bar{c} \in B$, tal que $b = \bar{c}\varphi(a_0)$. Como φ es sobreyectiva, existe $c \in A$, tal que $\bar{c} = \varphi(c)$ y $b = \varphi(c)\varphi(a_0) = \varphi(ca_0) \in \varphi[(a_0)] = b$. Entonces también $(\varphi(a_0)) \subseteq b$ y $b = (\varphi(a_0))$. Por consiguiente b es ideal principal. Como b es un ideal cualquiera, resulta que B es anillo principal. \square

Como una consecuencia inmediata del teorema 9.38, se obtiene el

COROLARIO 9.39. *La imagen homomorfa de un anillo principal es un anillo principal.*

9.4.2. Anillos Noetherianos. Decimos que un anillo A conmutativo con unidad es un *anillo noetheriano*, si todo ideal de A está finitamente generado.

Obviamente todo anillo principal es un anillo noetheriano.

Sea A un anillo conmutativo con unidad. Decimos que una cadena ascendente de ideales

$$(9.28) \quad \mathfrak{a}_0 \subseteq \mathfrak{a}_1 \subseteq \dots \subseteq \mathfrak{a}_k \subseteq \dots$$

es *estacionaria*, si existe $n \in \mathbb{N}$, tal que $\mathfrak{a}_m = \mathfrak{a}_n$, $\forall m \geq n$.

TEOREMA 9.40. *Un anillo conmutativo con unidad A es noetheriano Ssi toda cadena ascendente de ideales de A es estacionaria.*

DEMOSTRACIÓN. Si \mathfrak{a} es un ideal de A que no está finitamente generado, sea

$$S := \{a_0, a_1, \dots\}$$

un subconjunto infinito contable de generadores de \mathfrak{a} , tales que $a_n \notin (a_0, \dots, a_{n-1})$. Para $k \in \mathbb{N}$, sea $\mathfrak{a}_k := (a_0, \dots, a_k)$. Entonces la cadena ascendente de ideales

$$(9.29) \quad \mathfrak{a}_0 \subseteq \mathfrak{a}_1 \subseteq \dots \subseteq \mathfrak{a}_k \subseteq \dots$$

no es estacionaria. Por otra parte si A es un anillo noetheriano, consideremos la cadena ascendente de ideales

$$(9.30) \quad \mathfrak{a}_0 \subseteq \mathfrak{a}_1 \subseteq \dots \subseteq \mathfrak{a}_k \subseteq \dots,$$

entonces $\mathfrak{a} := \bigcup_{n \in \mathbb{N}} \mathfrak{a}_n$ es un ideal de A y, por hipótesis, está finitamente generado, digamos por los elementos a_1, \dots, a_m , entonces para cada m existe $n_m \in \mathbb{N}$, tal que $a_m \in \mathfrak{a}_{n_m}$. Como la cadena es ascendente, si N es el mayor de todos los n_m , entonces $a_1, \dots, a_m \in \mathfrak{a}_N$ y $\mathfrak{a} \subseteq \mathfrak{a}_N \subseteq \mathfrak{a}$. Por consiguiente $\mathfrak{a}_n = \mathfrak{a}_N$, $\forall n \geq N$. \square

TEOREMA 9.41. *Si A es un anillo noetheriano y $\varphi : A \rightarrow B$ un homomorfismo sobreyectivo de anillos, entonces B es un anillo noetheriano.*

DEMOSTRACIÓN. Dada una cadena ascendente de ideales de B

$$(9.31) \quad b_0 \subseteq b_1 \subseteq \dots \subseteq b_k \subseteq \dots$$

vamos a mostrar que ésta debe ser estacionaria. En efecto, la cadena (9.31) induce la cadena de ideales ascendentes en A

$$(9.32) \quad a_0 \subseteq a_1 \subseteq \dots \subseteq a_k \subseteq \dots,$$

donde $a_v := \varphi^{-1}[b_v]$, $v = 0, 1, \dots$, la cual, por hipótesis, es estacionaria, digamos a partir de un $n \in \mathbb{N}$. Entonces, por la sobreyectividad de φ , $b_m = \varphi[a_m] = \varphi[a_n] = b_n$, $\forall m \geq n$. Por lo tanto B es un anillo noetheriano. \square

Como una consecuencia inmediata del teorema 9.41, se obtiene el

COROLARIO 9.42. *La imagen homomorfa de un anillo noetheriano es un anillo noetheriano.*

Decimos que un dominio entero A posee la propiedad \mathbf{F}_0 , si todo elemento no invertible, distinto de 0 posee una representación como producto finito de factores irreducibles.

El siguiente teorema nos da una condición suficiente para la propiedad \mathbf{F}_0 .

TEOREMA 9.43. *Si en un dominio entero A toda cadena ascendente de ideales principales es estacionaria, entonces A posee la propiedad \mathbf{F}_0 .*

DEMOSTRACIÓN. Sea $a \in A$ un elemento no invertible distinto de 0 y supongamos que a no sea producto de factores irreducibles. Entonces a es reducible y existen $a, c \in A$ no invertibles, tales que $a = bc$. Entonces $a \in (b)$ y $a \in (c)$, si b y c fueran productos de factores irreducibles, también lo sería a , por lo que al menos uno de ellos no es producto de factores irreducibles. Supongamos, sin limitación de la generalidad, que b no sea producto de factores irreducibles y por consiguiente b reducible. Si $a_0 := (a)$ y $a_1 := (b)$, entonces $a_0 \subset a_1$ propiamente. Aplicando el razonamiento para b , obtenemos que b es producto de dos elementos no invertibles y uno de ellos no puede ser producto de factores irreducibles, por lo que se obtiene un ideal a_2 , tal que $a_0 \subset a_1 \subset a_2$. Continuando el proceso obtenemos entonces una cadena ascendente de ideales principales

$$(9.33) \quad a_0 \subset a_1 \subset \dots \subset a_k \subset \dots$$

que no podría ser estacionaria. En contradicción a la hipótesis. Por lo tanto a debe ser producto de factores irreducibles. \square

COROLARIO 9.44. *Todo anillo noetheriano posee la propiedad \mathbf{F}_0 .*

Entonces en un anillo noetheriano y en particular en un anillo principal, todo elemento no invertible, distinto de 0 es producto de factores irreducibles. En un anillo principal todo factor irreducible es también primo, por consiguiente todo elemento no invertible, distinto de 0 de un anillo principal, es producto de factores primos.

En general si un elemento de un dominio entero es producto de factores primos, no necesariamente dicha representación es única. Esto nos lleva a introducir una nueva clase de anillos, los *anillos factoriales* o de *factorización única*.

9.4.3. Anillos Factoriales o de Factorización Única. Decimos que un anillo A es un *anillo factorial* o de *factorización única*, si todo elemento no invertible, distinto de 0, posee una única representación, salvo producto con un elemento invertible y orden de los factores, como producto de factores irreducibles en A .

LEMA 9.45. *Sea A un dominio entero, con la propiedad \mathbf{F}_0 . Si $p \in A$ es un elemento primo, entonces vale*

$$\bigcap_{m=0}^{\infty} (p^m) = \mathbf{0}.$$

DEMOSTRACIÓN. Vamos a mostrar que ningún elemento distinto de 0 puede estar en la intersección de todos los ideales (p^m) , $m = 0, 1, \dots$. Si $a \in A$ es invertible, entonces $a \notin (p)$. Sea entonces $a \in A$ un elemento no invertible, distinto de 0. Como A posee la propiedad \mathbf{F}_0 , a es producto de elementos irreducibles, digamos $a = v_1 v_2 \cdots v_k$. Si alguno de los elementos v_κ es asociado con p , entonces $v_\kappa = e_\kappa p$, donde e_κ es un elemento invertible en A . Por consiguiente podemos escribir $a = e w_1 \cdots w_l p^m$, donde e es un elemento invertible, $m \geq 0$, w_λ irreducible $\forall \lambda = 1, \dots, l$ y ningún w_λ es asociado con p . Bajo estas condiciones $w_\lambda \notin (p)$, pues de lo contrario, por ser w_λ irreducible, resultaría w_λ asociado con p , lo cual, por construcción de los w_λ , no es cierto. Como (p) es un ideal primo, tampoco el producto de los w_λ está en (p) . Si $b := e w_1 \cdots w_l$, entonces $a = b p^m \in (p^m)$. Vamos a mostrar que $a \notin (p^{m+1})$. En efecto si $a \in (p^{m+1})$, entonces existe $c \in A$, tal que $a = c p^{m+1} = b p^m$ y $p^m(c p - b) = 0$, lo que implicaría que $b \in (p)$, lo cual no es posible. Por lo tanto $a \notin (p^{m+1})$. \square

El lema 9.45 nos dice que dado un elemento primo p de un dominio entero A , para cada elemento $a \in A$ distinto de 0, existe un número natural m , tal que $a \in (p^m)$, pero $a \notin (p^{m+1})$. Entonces podemos definir, para cada elemento primo $p \in A$, una aplicación

$$\mathbf{B}_p : A \setminus \{0\} \rightarrow \mathbb{N}$$

por medio de $\mathbf{B}_p(a) := m$, donde m es tal que $a \in (p^m)$, pero $a \notin (p^{m+1})$. Si a es invertible, $m = 0$, $\forall p \in A$ primo. $\mathbf{B}_p(a)$ nos indica, entonces, el número de veces que aparece p en una descomposición de a en factores irreducibles. De la demostración del lema 9.45, queda claro que $\mathbf{B}_p(a)$ nos da el número de factores asociados con p en cualquier descomposición del elemento a como producto de elementos irreducibles.

Bajo las mismas condiciones del lema 9.45 vale

LEMA 9.46. *Dados $a_1, \dots, a_n \in A \setminus \{0\}$ y $p \in A$ un elemento primo, entonces*

$$(9.34) \quad \mathbf{B}_p(a_1 \cdot a_2 \cdots a_n) = \sum_{v=1}^n \mathbf{B}_p(a_v).$$

DEMOSTRACIÓN. Para cada $v = 1, \dots, n$, sea $\mathbf{B}_p(a_v) = m_v$, entonces existen $b_v \in A$, $b_v \notin (p)$, tales que $a_v = b_v p^{m_v}$ y $a_1 \cdots a_n = b_1 \cdots b_m p^{m_1 + \cdots + m_n}$, donde $b_1 \cdots b_m \notin (p)$. De forma análoga a la demostración del lema 9.45, resulta que $a_1 \cdots a_m \notin (p^{m_1 + \cdots + m_n + 1})$. Por consiguiente vale (9.34). \square

Diremos que un dominio entero A posee la propiedad \mathbf{F}_1 , si todo elemento irreducible en A es un elemento primo en A .

TEOREMA 9.47. *En un dominio entero A las siguientes condiciones son equivalentes:*

- f1) *A es un anillo factorial.*
- f2) *Todo elemento no invertible, distinto de 0 de A posee una representación como producto de factores primos.*
- f3) *A posee las propiedades \mathbf{F}_0 y \mathbf{F}_1 .*

DEMOSTRACIÓN.

f2) \Rightarrow f3): Como todo elemento primo es irreducible, de f2) resulta que A posee la propiedad

F₀. Por otra parte si v es irreducible, por f2), v es producto de factores primos, digamos $v = p_1 \cdots p_n$ y por la irreducibilidad $n = 1$. Por lo tanto v es elemento primo.

f3⇒f2: Obvio.

f1⇒f3: Si A es factorial, entonces A posee la propiedad **F₀**. Falta mostrar que todo elemento irreducible es primo, si A es factorial. Sea v irreducible. Supongamos que el producto $ab \in (v)$, entonces existe $c \in A$, tal que $ab = cv$. Como A es factorial, a, b, c se descomponen, en forma única, salvo producto con un elemento invertible y orden de los factores, en producto de factores irreducibles. Entonces uno de los factores irreducibles de ab debe ser v que corresponde, ya sea a un factor irreducible de a , entonces $a \in (v)$ o a un factor irreducible de b y $b \in (p)$. Por lo tanto p es un elemento primo de A .

f3⇒f1): Dado un elemento no invertible, distinto de cero $a \in A$, entonces, por la propiedad **F₁**, a se descompone en un producto de factores primos. Supongamos que $a = p_1 \cdots p_r = q_1 \cdots q_n$ sean descomposiciones en factores primos de a y que exista un ν , $1 \leq \nu \leq n$, tal que $q := q_\nu \neq p_\rho$, $\forall \rho = 1, \dots, r$. Entonces $\mathbf{B}_q(a) = \mathbf{B}_q(p_1 \cdots p_r) = 0 \neq \mathbf{B}_q(q_1 \cdots q_n) = \mathbf{B}_q(a)$, lo cual es una contradicción. Por consiguiente, en las dos descomposiciones deben de comparecer los mismos elementos primos o ser asociados y el número de veces que comparece cada uno debe de ser el mismo. □

Del teorema 9.47, se obtiene, para el caso de un anillo principal, el siguiente

TEOREMA 9.48. *Todo anillo principal es factorial.*

DEMOSTRACIÓN. Por teorema 9.36 todo anillo principal posee la propiedad **F₁** y, por corolario 9.44, también la propiedad **F₀**. Entonces, por teorema 9.47, todo anillo principal es factorial. □

Como consecuencia del teorema 9.48, el anillo de los enteros \mathbb{Z} es un anillo factorial y todo campo es un anillo factorial.

Sea A un anillo factorial que no sea un campo. Entonces, dado un elemento $a \in A$ no invertible, distinto de 0, éste se descompone en un producto de factores primos, digamos $a = p_1^{m_1} \cdots p_n^{m_n}$, donde los p_ν son primos no asociados entre sí, $m_\nu \geq 0$ y $\mathbf{B}_{p_\nu}(a) = m_\nu$. Si $\bar{\mathcal{P}}$ es la clase de equivalencia de todos los elementos primos asociados al elemento primo p , de cada clase tomemos un único representante y formemos, con estos representantes, el conjunto \mathcal{P} de primos seleccionados. Entonces dados $p, q \in \mathcal{P}$, $p \neq q$, p, q no son asociados. Entonces, bajo estas condiciones, obtenemos, para anillos factoriales, el siguiente

TEOREMA 9.49 (Teorema de Factorización Única). *Sea A un anillo factorial. Entonces todo elemento $a \in A$, no invertible, se puede escribir como $a = ep_1^{m_1} \cdots p_n^{m_n}$, donde e es un elemento invertible de A y $p_1, \dots, p_n \in \mathcal{P}$. Esta representación es única, salvo orden de los factores. Por consiguiente, salvo producto por un elemento invertible, el elemento $a \in A$ está únicamente determinado por los números \mathbf{B}_p , $p \in \mathcal{P}$. Por otra parte si tenemos un conjunto de números naturales*

$$N := \{m_p \mid m_p = 0, \text{ salvo para un número finito de elementos } p \in \mathcal{P}\},$$

entonces existe un único elemento $a \in A$, salvo producto por un elemento invertible, tal que $\mathbf{B}_p(a) = m_p$, $\forall p \in \mathcal{P}$.

La relación de divisibilidad puede ser expresada con la ayuda de la función \mathbf{B}_p , como nos lo muestra el siguiente

TEOREMA 9.50. *Sean a, b elementos distintos de 0 de un anillo factorial A . Entonces b es un divisor de a , Ssi para cada elemento primo $p \in A$ vale*

$$(9.35) \quad \mathbf{B}_p(a) \geq \mathbf{B}_p(b).$$

DEMOSTRACIÓN. Si b es un divisor de a , entonces existe $r \in A$, tal que $a = rb$ y $a \in (p^m)$, si $b \in (p^m)$, por consiguiente vale (9.35). Supongamos ahora que (9.35) vale para cada elemento primo $p \in A$. Entonces, en particular, (9.35) vale para todo elemento primo $p \in \mathcal{P}$. Si $b = ep_1^{m_1} \cdots p_n^{m_n}$, $p_v \in \mathcal{P}$, entonces, por (9.35) cada $p_v^{m_v}$ es un factor de a y por consiguiente $b \mid a$. \square

En el caso de un anillo principal A , vimos en el teorema 9.33, que dados dos elementos $a, b \in A$, existe su máximo común divisor. Para el caso de los anillos factoriales, el siguiente teorema nos garantiza la existencia de un máximo común divisor, para cada subconjunto finito de elementos del anillo.

TEOREMA 9.51. *En un anillo factorial A , existe, para cada subconjunto finito de elementos distintos de 0 de A un máximo común divisor.*

DEMOSTRACIÓN. Sean $a_1, \dots, a_n \in A$, elementos distintos de 0 y \mathcal{P} el conjunto de los elementos primos definido arriba. Sea

$$\mu_p := \min_{1 \leq v \leq n} \mathbf{B}_p(a_v) \quad \text{para } p \in \mathcal{P}.$$

y $\mu_p \neq 0$ sólo para un número finito de elementos $p \in \mathcal{P}$, por consiguiente existe un $d \in A$, tal que $\mathbf{B}_p(d) = \mu_p$, $\forall p \in \mathcal{P}$. Como $\forall p \in \mathcal{P}$, $\mathbf{B}_p(d) \leq \mathbf{B}_p(a_v)$, $\forall v = 1, \dots, n$, resulta, por el teorema 9.50, que $d \mid a_v$, $\forall v = 1, \dots, n$. Por otra parte si $c \in A$ es un divisor común de a_1, \dots, a_n , entonces $\forall p \in \mathcal{P}$, $\mathbf{B}_p(c) \leq \mathbf{B}_p(a_v)$, $\forall v = 1, \dots, n$ y por consiguiente $\mathbf{B}_p(c) \leq \mathbf{B}_p(d)$, $\forall p \in \mathcal{P}$, lo que implica que $c \mid d$. Por lo tanto d es un máximo común divisor de a_1, \dots, a_n . \square

Decimos que los elementos a_1, \dots, a_n de un anillo factorial A son *primos relativos*, si son todos distintos de 0 y sus máximo común divisores son los elementos invertibles de A .

Si d es el máximo común divisor de los elementos a_1, \dots, a_n , entonces, para cada $v = 1, \dots, n$, existen elementos a'_1, \dots, a'_n , tales que $a_v = da'_v$ y los elementos a'_1, \dots, a'_n son primos relativos.

Referente a los ideales, si d es un máximo común divisor de a_1, \dots, a_n , $(a_v) \subseteq (d)$, $\forall v = 1, \dots, n$ y si $c \in A$ es tal que $(a_v) \subseteq (c)$, entonces $(d) \subseteq (c)$. Es decir que el ideal (d) es minimal entre todos los ideales principales que contengan a todos los a_v .

Dejamos al lector la tarea de constatar que el teorema 9.33 se puede generalizar de la siguiente forma:

TEOREMA 9.52. *Sean a_1, \dots, a_n elementos distintos de 0 de un anillo principal A . Entonces los generadores del ideal (a_1, \dots, a_n) son los máximo común divisores de a_1, \dots, a_n . Por otra parte a_1, \dots, a_n son primos relativos entre sí Ssi $(a_1, \dots, a_n) = A$, es decir que existen elementos $r_1, \dots, r_n \in A$, tales que $1 = r_1a_1 + \cdots + r_na_n$.*

9.4.4. Anillos Euclídeanos. Decimos que un anillo A es un *anillo euclídeo* si:

1. A es un anillo comutativo sin divisores de 0.
2. Existe una función $g : A \setminus \{0\} \rightarrow \mathbb{N}$, tal que
 - a) $g(a) \geq 0$, $\forall a \in A \setminus \{0\}$
 - b) $g(ab) \geq g(a)$, $\forall a, b \in A \setminus \{0\}$.
 - c) Dados $a, b \in A \setminus \{0\}$, $\exists t, r \in A$, tales que $a = tb + r$, donde $r = 0$ o $g(r) < g(b)$.

Como el lector notará, la función g , llamada la función *grado*, es una generalización de la función valor absoluto en \mathbb{Z} y c) es una generalización del algoritmo euclídeo. Entonces \mathbb{Z} es un anillo euclídeo.

TEOREMA 9.53. *El anillo de los enteros gaussianos $\mathbb{Z}[i]$, con la función $g(z) := |z|^2 = x^2 + y^2$, donde $z := x + iy$, es un anillo euclídeo.*

DEMOSTRACIÓN. g cumple, obviamente, con las propiedades a) y b) de una función grado. Falta mostrar que también cumple con la propiedad c). En efecto sean $\alpha := a + bi$, $\beta := c + di \in \mathbb{Z}[i] \setminus \{0\}$. $g(\alpha) = a^2 + b^2$, $g(\beta) = c^2 + d^2$. Consideremos

$$\frac{\alpha}{\beta} = \frac{a+bi}{c+di} = \frac{ac+bd}{c^2+d^2} + \frac{bc-ad}{c^2+d^2}i.$$

Entonces existen $m, n \in \mathbb{Z}$ y $v, w \in \mathbb{R}$, $|v| \leq \frac{1}{2}$, $|w| \leq \frac{1}{2}$ tales que

$$\frac{ac+bd}{c^2+d^2} = m + v, \quad \frac{bc-ad}{c^2+d^2} = n + w.$$

Haciendo $q := m + ni$ y $r := \beta(v + wi)$ se obtiene

$$\alpha = q\beta + r$$

donde $r \in \mathbb{Z}[i]$, ya que $r = \alpha - q\beta \in \mathbb{Z}[i]$. Además $g(r) = |\beta|^2(v^2+w^2) \leq g(\beta)(\frac{1}{4} + \frac{1}{4}) < g(\beta)$. Por lo tanto g cumple con la propiedad de una función grado sobre $\mathbb{Z}[i]$. \square

TEOREMA 9.54. *Si A es un anillo euclídeo, entonces A es un anillo con unidad y por consiguiente un dominio entero.*

DEMOSTRACIÓN. En particular A es un ideal de A , entonces, como, por teorema 9.55, A es anillo principal, existe $u \in A$, tal que $A = (u)$. Como, en particular $u \in (u)$, existe $c \in A$, tal que $u = cu$. Vamos a mostrar que c es el elemento unidad en A . En efecto, dado $a \in A$, entonces $a = bu$ y $ac = (bu)c = b(uc) = b(cu) = bu = a$. Por consiguiente $c = 1$. \square

TEOREMA 9.55. *Todo anillo euclídeo A es un anillo principal y por consiguiente un anillo factorial.*

DEMOSTRACIÓN. Si $\mathfrak{a} = \mathbf{0}$ la conclusión es obvia. Sea entonces $\mathfrak{a} \neq \mathbf{0}$. Entonces \mathfrak{a} posee elementos distintos de 0. Sea entonces $a_0 \in \mathfrak{a}$, $a_0 \neq 0$, tal que $g(a_0)$ sea minimal y sea $a \in \mathfrak{a}$, $a \neq 0$, entonces existen $t, r \in A$, tales que $a = ta_0 + r$, con $r = 0$ o $g(r) < g(a_0)$. Supongamos que $r \neq 0$, entonces, como $a, a_0 \in \mathfrak{a}$, resulta que $r \in \mathfrak{a}$ y $g(r) < g(a_0)$, en contradicción a la escogencia de a_0 . Por consiguiente, $r = 0$ y $a = ta_0$. Por lo tanto $\mathfrak{a} = (a_0)$. \square

9.4.5. Ejercicios y Complementos.

1. Mostrar el lema 9.29.
2. Sea \mathfrak{a} un ideal de un anillo principal A . Mostrar que A/\mathfrak{a} es también principal.
3. Sea S un subconjunto multiplicativo del anillo principal A . Mostrar que el anillo $S^{-1}A$ es también principal. En particular si $\mathfrak{p} \in \text{Spec } A$, entonces el anillo localizado $A_{\mathfrak{p}}$, de un anillo principales, es principal.
4. Sea \mathfrak{a} un ideal de un anillo noetheriano A . Mostrar que A/\mathfrak{a} es también noetheriano.
5. Sea S un subconjunto multiplicativo del anillo noetheriano A . Mostrar que el anillo $S^{-1}A$ es también noetheriano. En particular si $\mathfrak{p} \in \text{Spec } A$, entonces el anillo localizado $A_{\mathfrak{p}}$, de un anillo noetheriano, es noetheriano.
6. Sean p un elemento primo de un dominio entero A , $\mathbb{Q}(A)$ su campo de fracciones y

$$S := \{r \in \mathbb{Q}(A) \mid r = ap^m, a \in A, m \in \mathbb{Z}\}.$$

Mostrar que S es un subdominio entero de $\mathbb{Q}(A)$ y que el subgrupo de elementos invertibles S^* es el producto directo del subgrupo de elementos invertibles A^* con un grupo cíclico infinito.

7. Sea

$$\mathbb{Z}[i\sqrt{2}] := \{z \in \mathbb{C} \mid z = a + b\sqrt{2}i, a, b \in \mathbb{Z}\}.$$

Mostrar que $\mathbb{Z}[i\sqrt{2}]$ es un dominio entero, cuyos únicos elementos invertibles son 1 y -1 y que la función $g(z) := |z|^2$ es una función *grado* sobre $\mathbb{Z}[i\sqrt{2}]$, por lo que $\mathbb{Z}[i\sqrt{2}]$ es un anillo euclídeo y por consiguiente principal. (Ayuda: usar un procedimiento análogo al utilizado en la demostración del teorema 9.53, pero representar $\frac{1}{\sqrt{2}} \left(\frac{bc - ad}{c^2 + d^2} \right) = n + w$).

8. Sea

$$\mathbb{Z}[\sqrt{2}] := \{x \in \mathbb{R} \mid x = a + b\sqrt{2}, a, b \in \mathbb{Z}\}.$$

Mostrar que $\mathbb{Z}[\sqrt{2}]$ es un dominio entero, cuyos únicos elementos invertibles son 1 y -1 y que la función $g(x) := |a^2 - 2b^2|$ es una función *grado* sobre $\mathbb{Z}[\sqrt{2}]$, por lo que $\mathbb{Z}[\sqrt{2}]$ es un anillo euclídeo y por consiguiente principal.

9. a) Mostrar que

$$D := \{z \in \mathbb{C} \mid z = a + b\sqrt{5}i, a, b \in \mathbb{Z}\}$$

es un anillo, llamado el *anillo de Dedekind*.

- b) Mostrar que la función $g(z) := |z|^2$ no satisface, en general la propiedad c) de una función *grado* sobre D .
- c) Mostrar que si $z \mid w$ en D , entonces $g(z) \mid g(w)$ y $g(z) \leq g(w)$
- d) Mostrar que si z es invertible en D , entonces $g(z) = 1$, por lo que sólo 1 y -1 son invertibles en D .
- e) Si

$$(9.36) \quad (x_0) \subseteq (x_1) \subseteq \dots \subseteq (x_k) \subseteq \dots$$

Entonces se tiene

$$(9.37) \quad g(x_0) \geq g(x_1) \geq \dots \geq g(x_k) \geq \dots$$

- f) Como $g(x_k) \in \mathbb{N}$, mostrar que la cadena de desigualdades (9.37), debe ser estacionaria.
- g) Utilizar lo mostrado en f) para mostrar que la cadena de ideales (9.36) es estacionaria. Por lo que el anillo D posee la propiedad \mathbf{F}_0 .
- h) Mostrar que ningún elemento $z \in D$, satisface $g(z) = 2$ o $g(z) = 3$.
- i) Sea $\mathfrak{p} := (2, 1 + \sqrt{5})$. Mostrar que si existiera un $\alpha \in D$, tal que $\mathfrak{p} = (\alpha)$, entonces $g(\alpha)$ sería un divisor común de $g(2)$ y de $g(1 + \sqrt{5})$.
- j) Deducir de h) e i) que \mathfrak{p} no es un ideal principal. Entonces D no es un anillo principal y por consiguiente no es euclídeo.
- k) Usar h) para mostrar que los elementos $2, 3, 1 + \sqrt{5}i$ son irreducibles en D . Sin embargo $2 \mid (1 + \sqrt{5}i)(1 - \sqrt{5}i) = 6$, pero $2 \nmid (1 + \sqrt{5}i)$ y $2 \nmid (1 - \sqrt{5}i)$. Entonces 2 es un elemento irreducible en D , pero no es un elemento primo en D . Por consiguiente D no es un anillo factorial.

Más adelante veremos que, aunque D no es un anillo principal, sí es un anillo noetheriano.

CAPÍTULO 10

MÓDULOS Y ÁLGEBRAS

En este capítulo estudiaremos las propiedades principales de las estructuras algebraicas llamadas módulos y álgebras. Dado un conjunto S construiremos el llamado módulo libre sobre S y en el caso en que S posee la estructura de un monoide conmutativo, construiremos el álgebra libre sobre S .

Por razones pedagógicas y simplicidad limitaremos nuestro estudio a módulos y álgebras sobre un anillo conmutativo con unidad A , para evitarnos diferenciar entre módulos (álgebras) por la izquierda y módulos (álgebras) por la derecha. Igualmente, por abuso de notación y en aras de una mejor visualización, denotaremos, salvo casos particulares, las operaciones por $+ y \cdot$. También adoptaremos la expresión xy en lugar de $x \cdot y$.

10.1. Módulos

Sea $(A, +, \cdot)$ un anillo conmutativo con unidad. Recordamos al lector, tomando en consideración la notación adoptada, que un A -módulo es una estructura algebraica $(M, +, \cdot)$, donde $(M, +)$ es un grupo abeliano y

$$\cdot : A \times M \rightarrow M$$

una operación binaria que cumple con las siguientes propiedades:

1. $\lambda(x + y) = \lambda x + \lambda y, \forall x, y \in M, \forall \lambda \in A.$
2. $(\lambda + \alpha)x = \lambda x + \alpha x, \forall x \in M, \forall \lambda, \alpha \in A.$
3. $(\lambda\alpha)x = \lambda(\alpha x), \forall x \in M, \forall \lambda, \alpha \in A.$
4. Si 1 es la unidad en $(A, +, \cdot)$, entonces $1x = x, \forall x \in M.$

Dados dos A -módulos M, N , decimos que la aplicación

$$\varphi : M \rightarrow N$$

es un homomorfismo de A -módulos o una *aplicación A-lineal*, si

- a) $\varphi(x + y) = \varphi(x) + \varphi(y), \forall x, y \in M$
- b) $\varphi(\lambda x) = \lambda\varphi(x), \forall \lambda \in A, x \in M.$

El núcleo del homomorfismo φ de A -módulos es el conjunto:

$$\ker \varphi := \{x \in M \mid \varphi(x) = 0\}$$

EJEMPLOS 10.1.

1. $\mathbf{0} := \{0\}$ es un A -módulo, llamado el módulo trivial o módulo cero.
2. El anillo A es obviamente un A -módulo. En este caso coincide la operación binaria externa con el producto en A .
3. Si \mathfrak{a} es un ideal del anillo A , entonces \mathfrak{a} es un A -módulo.

$N \subseteq M$ es un *submódulo* del A -módulo M , si $(N, +)$ es un subgrupo de $(M, +)$ y $\lambda N \subseteq N, \forall \lambda \in A$.

Se comprueba facilmente que si

$$\varphi : M \rightarrow N$$

es un homomorfismo de A -módulos, entonces $\ker \varphi$ es un submódulo de M .

Dados un A -módulo M y un submódulo $N \subseteq M$, el lector comprobará facilmente que la relación

$$x \equiv y \quad (\text{mód } N) : \Leftrightarrow x - y \in N$$

es una relación de equivalencia sobre M y que el conjunto cociente de las clases de equivalencia M/N posee también la estructura de un A -módulo, por medio de las operaciones:

$$+ : M/N \times M/N \rightarrow M/N$$

definida por $\bar{x} + \bar{y} := \overline{x+y}$, $\forall \bar{x}, \bar{y} \in M/N$ y

$$\cdot : A \times M/N \rightarrow M/N$$

definida por $\lambda \cdot \bar{x} := \overline{\lambda x}$, $\forall \lambda \in A$, $\bar{x} \in M/N$. También comprobará facilmente que la proyección canónica

$$\pi : M \rightarrow M/N$$

es un homomorfismo de A -módulos y que se tiene el siguiente teorema de factorización:

TEOREMA 10.1 (Teorema de Factorización para Módulos). *Sea $\varphi : M \rightarrow N$ un homomorfismo de A -módulos de núcleo $\ker \varphi$, entonces existe un único homomorfismo de A -módulos*

$$(10.1) \quad \bar{\varphi} : M/\ker \varphi \rightarrow N$$

tal que el siguiente diagrama es comutativo

$$(10.2) \quad \begin{array}{ccc} M & \xrightarrow{\varphi} & N \\ \pi \downarrow & \nearrow \bar{\varphi} & \\ M/\ker \varphi & & \end{array}$$

Además $\bar{\varphi}$ es inyectiva y si φ es sobreyectiva, entonces $\bar{\varphi}$ es un isomorfismo.

10.1.1. Ejercicios y Complementos.

- Sean $\varphi : A \rightarrow B$ un homomorfismo de anillos comutativos con unidad y M un B -módulo. Si definimos

$$\cdot : A \times M \rightarrow M$$

por medio de $\lambda \cdot x := \varphi(\lambda)x$, $\forall \lambda \in A$, $x \in M$, mostrar que M es, entonces, un A -módulo. Es decir que el homomorfismo φ induce una estructura de A -módulo sobre el B -módulo M . En particular el anillo B es también un A -módulo.

- Mostrar que todo A -módulo es también un \mathbb{Z} -módulo.
- Mostrar que todo grupo abeliano es un \mathbb{Z} -módulo.
- Dados un A -módulo M y submódulos K, N , mostrar que se tiene un isomorfismo de A -módulos, entre $(N+K)/K$ y $N/(N \cap K)$ y entre $(N+K)/N$ y $K/(N \cap K)$.
- Dado un A -módulo M y submódulos K, N , tales que K es submódulo de N , mostrar que $(M/K)/(N/K)$ es isomorfo a M/N . (Ley de cancelación).
- Si $\varphi : M \rightarrow N$ es un homomorfismo de A -módulos, mostrar

- a) Si K es un submódulo de M , entonces $\varphi[K]$ es submódulo de N
 b) Si V es un submódulo de N , entonces $\varphi^{-1}[V]$ es un submódulo de M que contiene al $\ker \varphi$.
7. Sean M, N A -módulos y

$$\hom_A(M, N) := \{\varphi : M \rightarrow N \mid \varphi \text{ } A\text{-lineal}\}$$

Si, dados $\varphi, \psi \in \hom_A(M, N)$, definimos $(\varphi + \psi)(x) := \varphi(x) + \psi(x)$, $\forall x \in M$ y dados $\lambda \in A$, $\varphi \in \hom_A(M, N)$, definimos $(\lambda\varphi)(x) := \lambda\varphi(x)$, $\forall x \in M$, Mostrar que entonces $\hom_A(M, N)$ es un A -módulo. En particular $M^* := \hom_A(M, A)$ es un A -módulo, llamado el *módulo dual* de M .

8. Mostrar que todo homomorfismo de A -módulos $\varphi : M \rightarrow N$, induce un homomorfismo de A -módulos $\varphi^* : N^* \rightarrow M^*$, definido por $\varphi^*(f) := f \circ \varphi$, $\forall f \in N^*$.
 9. Sea K un A -módulo fijo. Mostrar que todo homomorfismo de A -módulos

$$\varphi : M \rightarrow N,$$

induce un homomorfismo de A -módulos

$$\varphi_* : \hom(K, M) \rightarrow \hom(K, N)$$

definido por $\varphi_*(\psi) := \varphi \circ \psi$, $\forall \psi \in \hom(K, M)$ y un homomorfismo de A -módulos

$$\varphi^* : \hom(N, K) \rightarrow \hom(M, K).$$

definido por $\varphi^*(\psi) := \psi \circ \varphi$, $\forall \psi \in \hom(N, K)$.

10. Mostrar que todo elemento $\varphi \in M^*$ está totalmente determinado por $\varphi(1)$.
 11. Dado un A -módulo M , definimos $M^{**} := (M^*)^*$. Mostrar que la aplicación

$$\varphi : M \rightarrow M^{**}$$

definida como la aplicación, tal que $\varphi(m)(f) := f(m)$, $\forall f \in M^*$, $m \in M$, es un homomorfismo inyectivo de A -módulos, llamado el homomorfismo canónico de $M \rightarrow M^{**}$. $\varphi_m := \varphi(m) : M^* \rightarrow A$ se llama el *homomorfismo de valuación* en m . Si φ es un isomorfismo, entonces se dice que M es un A -módulo *reflexivo*.

10.1.2. Módulo Libre. Formalmente la construcción del A -módulo libre es similar a la construcción del grupo libre abeliano. Sea S un conjunto no vacío, A un anillo conmutativo con unidad y

$$\varphi : S \rightarrow A$$

una aplicación, tal que $\varphi(s) = 0$, salvo un número finito de elementos de S . Entonces, si

$$\mathbf{s}_j : S \rightarrow A$$

es la aplicación, tal que $\mathbf{s}_j(s) = 0$, si $s \neq s_j$ y $\mathbf{s}_j(s_j) = 1$, entonces φ se puede escribir de la forma

$$\varphi = k_1 \mathbf{s}_1 + \cdots + k_n \mathbf{s}_n,$$

donde los $k_v \in A$, $\forall v = 1, \dots, n$.

De forma más general podemos escribir

$$\varphi = \sum_{s \in S} k_s \mathbf{s},$$

donde $k_s = 0$, salvo para un número finito de elementos $s \in S$, y

$$\mathbf{s} : S \rightarrow A$$

la aplicación tal que

$$s(x) = \begin{cases} 1 & \text{si } x = s, \\ 0 & \text{de lo contrario.} \end{cases}$$

φ admite una única representación de esta forma. En efecto, supongamos que

$$\varphi = \sum_{s \in S} k_s s = \sum_{s \in S} k'_s s$$

entonces

$$0 = \sum_{s \in S} (k_s - k'_s) s$$

y por consiguiente $k_s = k'_s, \forall s \in S$.

Sea

$$A\langle S \rangle := \{\varphi : S \rightarrow A \mid \varphi(s) = 0, \text{ salvo un número finito de elementos } s \in S\}$$

entonces $(A\langle S \rangle, +, \cdot)$, donde $+$ es la adición usual de aplicaciones sobre A , y

$$\cdot : A \times A\langle S \rangle \rightarrow A\langle S \rangle$$

la operación binaria definida por $(\lambda \cdot \varphi)(x) := \lambda \varphi(x), \forall \varphi \in A\langle S \rangle, x \in S$, es un A -módulo.

Por medio de la aplicación inyectiva

$$f : S \rightarrow A\langle S \rangle$$

definida por $f(s) := 's'$, podemos identificar a S como un subconjunto de $A\langle S \rangle$ y el módulo $A\langle S \rangle$ está generado por $f[S]$.

$(A\langle S \rangle, +, \cdot, f)$ se llama el *módulo libre* generado por el conjunto S ,

Usualmente se suele identificar S con $f[S]$ en $A\langle S \rangle$ y representar los elementos de $A\langle S \rangle$, como las “sumas formales”

$$\sum_{s \in S} k_s s.$$

El módulo libre $(A\langle S \rangle, +, f)$ posee la siguiente propiedad universal:

Dada una aplicación

$$g : S \rightarrow M,$$

donde M es un A -módulo, entonces existe un único homomorfismo de A -módulos

$$g_* : A\langle S \rangle \rightarrow M,$$

tal que el diagrama

(10.3)

$$\begin{array}{ccc} S & \xrightarrow{f} & A\langle S \rangle \\ g \downarrow & \nearrow g_* & \\ M & & \end{array}$$

es comunitativo.

En efecto

$$g_* : A\langle S \rangle \rightarrow M$$

definida por

$$g_* \left(\sum_{s \in S} k_s s \right) := \sum_{s \in S} k_s g(s)$$

es el único homomorfismo que hace conmutar al diagrama.

De la propiedad universal resulta, como el lector podrá comprobar, la unicidad, salvo isomorfismo, del módulo libre.

TEOREMA 10.2. Si $g : S \rightarrow S'$ es una aplicación entre dos conjuntos y $(A\langle S \rangle, +, f)$, $(A\langle S' \rangle, +, f')$ los respectivos módulos libres, entonces existe un único homomorfismo de A -módulos $g_* : A\langle S \rangle \rightarrow A\langle S' \rangle$, tal que el diagrama

$$(10.4) \quad \begin{array}{ccc} S & \xrightarrow{f} & A\langle S \rangle \\ g \downarrow & & \downarrow g_* \\ S' & \xrightarrow{f'} & A\langle S' \rangle \end{array}$$

es comutativo y si g es sobreyectiva también lo será g_* .

DEMOSTRACIÓN. En efecto, tenemos una aplicación

$$(f' \circ g) : S \rightarrow A\langle S' \rangle$$

y por la propiedad universal existe un único homomorfismo $g_* := (f' \circ g)_*$ que hace commutar al diagrama (10.3), con $M := A\langle S' \rangle$ y el cual hace commutar también al diagrama (10.4). \square

En el caso particular, en que S es un conjunto finito

$$S := \{s_1, \dots, s_n\}.$$

Entonces cada elemento de $\varphi \in A\langle S \rangle$, se escribe de forma única como

$$\varphi = \sum_{v=1}^n k_v s_v, \quad k_v \in A.$$

Entonces se dice que los elementos s_1, \dots, s_n forman una *base* de $A\langle S \rangle$.

10.1.3. Producto Directo de Módulos. También, de forma análoga a la teoría de grupos abelianos, es posible definir el producto directo y la suma directa sobre una familia $(M_i)_{i \in I}$ de A -módulos.

Si

$$M := \prod_{i \in I} M_i$$

es el producto cartesiano de la familia de conjuntos $(M_i)_{i \in I}$. Dados $(m_i)_{i \in I}, (n_i)_{i \in I} \in M$, por medio de $(m_i)_{i \in I} + (n_i)_{i \in I} := (m_i + n_i)_{i \in I}$, se define una suma $+ : M \times M \rightarrow M$, y por medio de $\lambda \cdot m := (\lambda m_i)_{i \in I}$ se define un producto $\cdot : A \times M \rightarrow M$, tales que $(M, +, \cdot)$ es un A -módulo y las proyecciones

$$p_i : M \rightarrow M_i$$

son homomorfismos de A -módulos, para todo $i \in I$. $(M, +, \cdot, p_i)_{i \in I}$ lo llamamos *el módulo producto directo* sobre la familia $(M_i)_{i \in I}$. El lector comprobará fácilmente que, en efecto, $(M, +, \cdot)$ cumple con los axiomas de A -módulo y que las proyecciones p_i son homomorfismos de A -módulos.

El módulo $(M, +, \cdot, p_i)_{i \in I}$ posee la siguiente *propiedad universal*: Dado un A -módulo cualquiera N y una familia de homomorfismos

$$(\psi_i : N \rightarrow M_i)_{i \in I},$$

existe un único homomorfismo

$$\psi : N \rightarrow M,$$

tal que para todo $i \in I$, el diagrama

$$(10.5) \quad \begin{array}{ccc} N & \xrightarrow{\psi} & M \\ & \searrow \psi_i & \downarrow p_i \\ & & M_i \end{array}$$

es comutativo.

En efecto $\psi : N \rightarrow M$, definido por $\psi(n) := (\psi_i(n))_{i \in I}$ es un homomorfismo de A -módulos y es el único que hace commutar al diagrama (10.5), como el lector comprobará facilmente.

De la propiedad universal que satisface el módulo producto $(M, +, \cdot, p_i)_{i \in I}$, se deduce que si $(\tilde{M}, +, \cdot, \tilde{p}_i)_{i \in I}$, es otro módulo que satisface dicha propiedad, entonces M es isomorfo a \tilde{M} .

En efecto, por la propiedad universal, existe un único homomorfismo $\psi : \tilde{M} \rightarrow M$ y un único homomorfismo $\tilde{\psi} : M \rightarrow \tilde{M}$, tales que los diagramas

$$(10.6) \quad \begin{array}{ccc} \tilde{M} & \xrightarrow{\psi} & M \\ & \searrow \tilde{p}_i & \downarrow p_i \\ & & M_i \end{array}$$

y

$$(10.7) \quad \begin{array}{ccc} M & \xrightarrow{\tilde{\psi}} & \tilde{M} \\ & \searrow p_i & \downarrow \tilde{p}_i \\ & & M_i \end{array}$$

son comutativos.

Entonces el homomorfismo $(\tilde{\psi} \circ \psi) : \tilde{M} \rightarrow \tilde{M}$ hace commutar al diagrama

$$(10.8) \quad \begin{array}{ccc} \tilde{M} & \xrightarrow{\tilde{\psi} \circ \psi} & \tilde{M} \\ & \searrow \tilde{p}_i & \downarrow \tilde{p}_i \\ & & M_i \end{array}$$

y por la propiedad universal $(\tilde{\psi} \circ \psi) = 1_{\tilde{M}}$. Un argumento análogo nos muestra que también $(\psi \circ \tilde{\psi}) = 1_M$. Por consiguiente ψ es un isomorfismo de A -módulos.

10.1.4. Suma Directas de Módulos. Sea $(M_i)_{i \in I}$ una familia de A -módulos.

Si

$$M = \prod_{i \in I} M_i$$

es el producto directo de la familia $(M_i)_{i \in I}$, consideremos el submódulo

$$\bigoplus_{i \in I} M_i$$

formado por los elementos $m = (m_i)_{i \in I} \in M$, tal que $m_i = 0$, salvo para un número finito de índices $i \in I$. Para cada índice $j \in I$, sea

$$\lambda_j : M_j \rightarrow \bigoplus_{i \in I} M_i$$

la aplicación tal que la j -componente de $\lambda_j(m) = m$ y el resto de las componentes es 0, entonces λ_j es un homomorfismo de A -módulos, $\forall j \in I$.

$$\left(\bigoplus_{i \in I} M_i, +, \cdot, \lambda_i \right)_i \in I$$

Se llama *la suma directa* de la familia de módulos $(M_i)_{i \in I}$.

En forma análoga al producto directo de módulos, la suma directa de módulos posee la siguiente propiedad universal:

Dada una familia de homomorfismos de A -módulos

$$(\psi_i : M_i \rightarrow N)_{i \in I},$$

existe un único homomorfismo

$$\psi : \bigoplus_{i \in I} M_i \rightarrow N,$$

tal que, $\forall i \in I$, el diagrama

$$(10.9) \quad \begin{array}{ccc} M_i & \xrightarrow{\lambda_i} & \bigoplus_{i \in I} M_i \\ \psi_i \downarrow & \nearrow \psi & \\ N & & \end{array}$$

es comutativo.

En efecto, el lector comprobará fácilmente que la aplicación

$$\psi : \bigoplus_{i \in I} M_i \rightarrow N$$

definida por

$$\psi(g) := \sum_{i \in I} \psi_i(g_i)$$

es un homomorfismo de A -módulos y que es el único que hace comutativo al diagrama (10.9).

Dada una familia de homomorfismos de A -módulos

$$(\varphi_i : M_i \rightarrow N)_{i \in I}$$

tal que

$$(N, +, \cdot, \varphi_i)_{i \in I}$$

posee la propiedad universal arriba indicada, entonces

$$(N, +, \cdot, \varphi_i)_{i \in I}$$

es isomorfo a

$$\left(\bigoplus_{i \in I} M_i, +, \lambda_i \right)_{i \in I}$$

Esto quiere decir que la suma directa es única, salvo isomorfismo. Dejamos al lector la demostración de esta propiedad, ya que es similar a la demostración de la unicidad del producto directo.

Si I es un conjunto finito de índices, entonces la suma directa y el producto directo coinciden, como el lector comprobará fácilmente.

Si S es un conjunto finito de n elementos, entonces se tiene el siguiente resultado, cuya demostración dejamos al lector:

$$(10.10) \quad A\langle S \rangle \approx \underbrace{A \oplus \cdots \oplus A}_n \approx \underbrace{A \times \cdots \times A}_n.$$

10.1.5. Ejercicios y Complementos.

1. Sean S un conjunto no necesariamente finito y A un anillo comutativo con unidad. Para cada $s \in S$, sea $A_s = A$. Mostrar que $A\langle S \rangle \approx \bigoplus_{s \in S} A_s$.
2. Sea M un A -módulo. Decimos que un elemento $x \in M$ es un *elemento de torsión* de M , si existe $\lambda \in A$, $\lambda \neq 0$, tal que $\lambda x = 0$. Mostrar que el conjunto

$$T(M) := \{x \in M \mid x \text{ es elemento de torsión}\}$$

es un submódulo de M , llamado el *submódulo de torsión*.

3. Sea M un A -módulo. Dado $x \in M$, definimos

$$\text{Ann}_A(x) := \{\lambda \in A \mid \lambda x = 0\}.$$

Mostrar que $\text{Ann}_A(x)$ es un ideal de A , llamado el *anulador* de x . Mostrar también que el conjunto

$$\text{Ann}_A M := \{\lambda \in A \mid \lambda M = 0\}$$

es un ideal de A , llamado el *anulador* del módulo M . y que

$$\text{Ann}_A M = \bigcap_{x \in M} \text{Ann}_A(x).$$

4. Sean S un conjunto y A un dominio entero. Si $M := A\langle S \rangle$, mostrar que $T(M) = \mathbf{0}$. Es decir un módulo libre sobre un dominio entero es libre de torsión.
5. Sean A un anillo comutativo con unidad y M un A -módulo. Dado $m \in M$, sea

$$\varphi : A \rightarrow M$$

el homomorfismo definido por $\varphi(1) := m$. Mostrar que M posee un submódulo isomorfo a $A/\text{Ann}_A(x)$.

6. Sean A un anillo comutativo con unidad, S un subconjunto multiplicativo de A y M un A -módulo.

a) Mostrar que la relación $(m, s) \sim (n, t) \Leftrightarrow \exists r \in S$, tal que $r(tm - sn) = 0$, es una relación de equivalencia sobre $M \times S$. Por $S^{-1}M$ denotaremos al conjunto cociente de las clases $\frac{m}{s}$

b) Mostrar que la suma definida por $\frac{m}{s} + \frac{n}{t} := \frac{tm + sn}{ts}$ está bien definida, así como el producto $\frac{\lambda}{t} \cdot \frac{m}{s} := \frac{\lambda m}{st}$.

c) Mostrar que $(S^{-1}M, +, \cdot)$ es un $S^{-1}A$ -módulo y un A -módulo, llamado el *módulo de fracciones* respecto del conjunto multiplicativo S .

d) Si $S := A \setminus \mathfrak{p}$, donde $\mathfrak{p} \in \text{Spec } A$, el módulo $M_{\mathfrak{p}}$ se llama el *localizado del módulo M en el ideal primo p*. Al conjunto

$$\text{Supp } M := \{\mathfrak{p} \in \text{Spec } A \mid M_{\mathfrak{p}} \neq \mathbf{0}\}$$

lo llamamos el *soporte* del módulo M . Mostrar que $\mathfrak{p} \in \text{Supp } M$ si $\text{Ann}_A M \subseteq \mathfrak{p}$ y que existe una correspondencia biunívoca entre $\text{Supp } M$ y $\text{Spec}(A/\text{Ann}_A M)$.

7. Sean A un dominio entero, S un conjunto y $M := A\langle S \rangle$ el módulo libre sobre S . Mostrar que $\text{Supp } M = \text{Spec } A$.

10.2. Álgebras

Recordamos al lector que un *A-álgebra*, donde A es un anillo conmutativo con unidad, es una estructura algebraica $((B, +, \cdot), \cdot)$, donde $(B, +, \cdot)$ es un A -módulo y

$$\cdot : B \rightarrow B \rightarrow B$$

una operación binaria que satisface las siguientes condiciones:

- a) $(x + y) \cdot z = x \cdot z + y \cdot z, \forall x, y, z \in B.$
- b) $x \cdot (y + z) = x \cdot y + x \cdot z, \forall x, y, z \in B.$
- c) $(\lambda x) \cdot y = x \cdot (\lambda y) = \lambda(x \cdot y), \forall x, y \in B, \lambda \in A.$

Siguiendo nuestro convenio de notación escribiremos también xy en lugar de $x \cdot y$, para $x, y \in B$.

Si \cdot es conmutativa (asociativa), entonces diremos que B es un álgebra conmutativa (asociativa). Si \cdot posee elemento unidad, entonces diremos que B es un álgebra con elemento unidad.

Una aplicación

$$\varphi : B \rightarrow C,$$

entre dos A -álgebras es un homomorfismo de A -álgebras, si φ es A -lineal y si, además, $\varphi(xy) = \varphi(x)\varphi(y), \forall x, y \in B$.

Si φ es un homomorfismo de A -álgebras, entonces definimos el núcleo de φ , como el conjunto

$$\ker \varphi := \{x \in B \mid \varphi(x) = 0\}.$$

Nosotros nos limitaremos a considerar A -álgebras conmutativas con unidad, sobre anillos conmutativos con unidad.

Un subconjunto $\alpha \subseteq B$, donde B es un A -álgebra conmutativa con unidad, es un *ideal* de A -álgebras, si α es un submódulo de B y para todo $x \in B$, $x\alpha \subseteq \alpha$.

El lector comprobará fácilmente que si

$$\varphi : B \rightarrow C$$

es un homomorfismo de A -álgebras, entonces $\ker \varphi$ es un ideal de A -álgebras.

Dados un A -álgebra B y un ideal de A -álgebras $\alpha \subseteq B$, el lector comprobará fácilmente que la relación

$$x \equiv y \pmod{\alpha} : \Leftrightarrow x - y \in \alpha$$

es una relación de equivalencia sobre B y que el conjunto cociente de las clases de equivalencia B/α posee también la estructura de un A -álgebra, por medio de las operaciones:

$$+ : B/\alpha \times B/\alpha \rightarrow B/\alpha$$

definida por $\bar{x} + \bar{y} := \overline{x + y}, \forall \bar{x}, \bar{y} \in B/\alpha$,

$$\cdot : A \times B/\alpha \rightarrow B/\alpha$$

definida por $\lambda \cdot \bar{x} := \overline{\lambda x}, \forall \lambda \in A, \bar{x} \in B/\alpha$ y

$$\cdot : B/\alpha \times B/\alpha \rightarrow B/\alpha$$

definida por $\bar{x} \cdot \bar{y} := \overline{x \cdot y}, \forall \bar{x}, \bar{y} \in B/\alpha$. También comprobará fácilmente que la proyección canónica

$$\pi : B \rightarrow B/\alpha$$

es un homomorfismo de A -álgebras y que se tiene el siguiente teorema de factorización:

TEOREMA 10.3 (Teorema de Factorización para álgebras). *Sea $\varphi : B \rightarrow C$ un homomorfismo de A -álgebras de núcleo $\ker \varphi$, entonces existe un único homomorfismo de A -álgebras*

$$(10.11) \quad \bar{\varphi} : B/\ker \varphi \rightarrow C$$

tal que el siguiente diagrama es comutativo

$$(10.12) \quad \begin{array}{ccc} B & \xrightarrow{\varphi} & C \\ \pi \downarrow & \nearrow \bar{\varphi} & \\ B/\ker \varphi & & \end{array}$$

Además $\bar{\varphi}$ es inyectiva y si φ es sobreyectiva, entonces $\bar{\varphi}$ es un isomorfismo.

10.2.1. Ejercicios y Complementos.

1. Si $\varphi : A \rightarrow B$ es un homomorfismo de anillos, mostrar que B es un A -álgebra.
2. Sean B un A -álgebra y a, b ideales de B . Mostrar que se tiene un isomorfismo de A -módulos entre $(a+b)/b$ y $a/(a \cap b)$ y entre $(a+b)/a$ y $b/(a \cap b)$.
3. Sean B un A -álgebra, y a, b ideales de B , tales que $b \subseteq a$. Mostrar que se tiene un isomorfismo de A -álgebras entre B/a y $(B/b)/(a/b)$. (Ley de cancelación).
4. Si B es un A -álgebra, en forma análoga a la definición de un A -módulo se puede definir la estructura de un B -módulo M , definiendo una operación binaria externa sobre $B \times M$. Dar dicha definición y mostrar que todo ideal del A -álgebra B es un B -módulo.

10.2.2. Álgebras Graduadas. Sean A un anillo comutativo con unidad, $(N, +)$ un monoide comutativo y $(M_i)_{i \in N}$ una familia de A -módulos, indizados por el monoide N . Para cada par de subíndices i, j y un subíndice fijo r exista una operación binaria externa

$$\cdot_{ij} : M_i \times M_j \rightarrow M_{i+j+r},$$

tal que

- a) $\cdot_{ij} = \cdot_{ji}, \forall i, j \in N$.
- b) $(m_i \cdot_{ij} m_j) \cdot_{(i+j+r)k} m_k = m_i \cdot_{i(j+k+r)} (m_j \cdot_{jk} m_k), \forall i, j, k \in N$.
- c) $(m_i + n_i) \cdot_{ij} m_j = m_i \cdot_{ij} m_j + n_i \cdot_{ij} m_j, \forall i, j \in N$.
- d) $(am_i) \cdot_{ij} (bm_j) = (ab)(m_i \cdot_{ij} m_j), \forall i, j \in N, a, b \in A$.

Entonces, la familia de operaciones binarias $(\cdot_{ij})_{i,j \in N}$, induce una operación binaria interna

$$\cdot : \sum_{i \in N} M_i \times \sum_{j \in N} M_j \rightarrow \sum_{i \in N} M_i,$$

definida por

$$(10.13) \quad \left(\sum_{i \in N} m_i \right) \cdot \left(\sum_{j \in N} m'_j \right) := \sum_{k \in N} n_{k+r}, \quad n_{k+r} := \sum_{i+j=k} m_i \cdot_{ij} m'_j,$$

obteniendo el siguiente diagrama comutativo:

$$(10.14) \quad \begin{array}{ccc} M_i \times M_j & \xrightarrow{\cdot_{ij}} & M_{i+j+r} \\ \lambda_i \times \lambda_j \downarrow & & \downarrow \lambda_{i+j+r} \\ \bigoplus_{i \in N} M_i \times \bigoplus_{j \in N} M_j & \xrightarrow{\cdot} & \bigoplus_{k \in N} M_k \end{array}$$

Entonces $\left(\left(\sum_{i \in N} M_i, +, \cdot\right), \cdot\right)$ es un A -álgebra, llamada el *A -álgebra graduada* de la familia de A -módulos $(M_i)_{i \in N}$, de *grado* r , sobre el monoide $(N, +)$. En particular r puede ser igual a 0 y se tiene, entonces, un A -álgebra graduada de grado 0. En muchos casos $N = \mathbb{N}$ o $N = \mathbb{Z}$ y r puede ser un número positivo o negativo.

10.2.3. Ejercicios y Complementos.

1. Mostrar que, en efecto, $\left(\left(\sum_{i \in N} M_i, +, \cdot\right), \cdot\right)$ es una A -álgebra y que el diagrama (10.14) es comutativo.
2. Sean A un anillo comunitativo con unidad, \mathfrak{a} un ideal propio de A , no trivial, entonces se tiene una familia de ideales $(\mathfrak{a}^\nu)_{\nu \in \mathbb{N}}$, donde $\mathfrak{a}^0 := A$ y el producto · del anillo induce, para cada par $\nu, \mu \in \mathbb{N}$, un producto

$$\cdot_{\nu\mu} : \mathfrak{a}^\nu \times \mathfrak{a}^\mu \rightarrow \mathfrak{a}^{\nu+\mu}.$$

Mostrar que $\left(\bigoplus_{\nu \in \mathbb{N}} \mathfrak{a}^\nu, +, \cdot\right), \cdot$ es un A -álgebra graduada de grado 0, con unidad, llamada el *álgebra de Rees* del ideal \mathfrak{a} .

3. Bajo las mismas condiciones del ejercicio precedente, se tiene una familia de ideales $(\mathfrak{a}^\nu / \mathfrak{a}^{\nu+1})_{\nu \in \mathbb{N}}$. Mostrar que el producto · sobre A induce un producto

$$\cdot_{\nu\mu} : \mathfrak{a}^\nu / \mathfrak{a}^{\nu+1} \times \mathfrak{a}^\mu / \mathfrak{a}^{\mu+1} \rightarrow \mathfrak{a}^{\nu+\mu} / \mathfrak{a}^{\nu+\mu+1}.$$

y que $\left(\bigoplus_{\nu \in \mathbb{N}} \mathfrak{a}^\nu / \mathfrak{a}^{\nu+1}, +, \cdot\right), \cdot$ es un A/\mathfrak{a} -álgebra graduada, de grado 0, con unidad, llamada el *álgebra graduada asociada* al ideal \mathfrak{a} . (En la geometría algebraica juega un papel muy importante el álgebra graduada asociada a un ideal primo y a un ideal maximal).

10.2.4. Álgebra Libre sobre un Monoide. Sean A un anillo comunitativo con unidad, (G, \cdot) un monoide comunitativo. Si $A\langle G \rangle$ es el A -módulo libre sobre el conjunto G , vamos a ver que, gracias a la operación binaria, definida, sobre G , podemos dotar a $A\langle G \rangle$ de una estructura de A -álgebra. En efecto, dados dos elementos de $A\langle G \rangle$, $x := \sum_{g \in G} a_g g$, $y := \sum_{g' \in G} b_{g'} g'$, definimos

$$(10.15) \quad x \cdot y := \sum_{h \in G} c_h h, \quad c_h := \sum_{g \cdot g' = h} a_g b_{g'}.$$

Entonces, como el lector comprobará fácilmente, $((A\langle G \rangle, +, \cdot, f), \cdot)$ es un A -álgebra, comunitativa, asociativa y con unidad, llamada el *A -álgebra libre sobre el monoide G* .

Si $((B, +, \cdot), \cdot)$ es un A -álgebra, comunitativa y asociativa con unidad, entonces, en particular, (B, \cdot) es un monoide comunitativo.

El A -álgebra libre sobre un monoide posee la siguiente propiedad universal: Dado un homomorfismo de monoídes

$$\varphi : G \rightarrow B,$$

donde B es un A -álgebra, entonces existe un único homomorfismo de A -álgebras

$$\varphi_* : A\langle G \rangle \rightarrow B,$$

tal que el diagrama

$$(10.16) \quad \begin{array}{ccc} G & \xrightarrow{f} & A\langle G \rangle \\ \varphi \downarrow & \swarrow \varphi_* & \\ B & & \end{array}$$

es comutativo.

En efecto

$$\varphi_* : A\langle G \rangle \rightarrow B$$

definida por

$$\varphi_* \left(\sum_{g \in G} k_g \mathbf{g} \right) := \sum_{g \in G} k_g \varphi(g)$$

es el único homomorfismo de A -álgebras que hace commutar al diagrama.

De la propiedad universal resulta, como el lector podrá comprobar, la unicidad, salvo isomorfismo, del módulo libre.

TEOREMA 10.4. *Si $\varphi : G \rightarrow G'$ es un homomorfismo de monoides y $((A\langle G \rangle, +, f), \cdot)$ ($((A\langle G' \rangle, +, f'), \cdot)$ las respectivas A -álgebras libres, entonces existe un único homomorfismo de A -álgebras $\varphi_* : A\langle G \rangle \rightarrow A\langle G' \rangle$, tal que el diagrama*

$$(10.17) \quad \begin{array}{ccc} G & \xrightarrow{f} & A\langle G \rangle \\ \varphi \downarrow & & \downarrow \varphi_* \\ G' & \xrightarrow{f'} & A\langle G' \rangle \end{array}$$

es comutativo y si φ es sobrejetivo también lo será φ_* .

DEMOSTRACIÓN. En efecto, tenemos un homomorfismo de monoides

$$(f' \circ \varphi) : G \rightarrow A\langle G' \rangle$$

y por la propiedad universal existe un único homomorfismo de A -álgebras

$\varphi_* := (f' \circ \varphi)_*$ que hace commutar al diagrama (10.16), con $B := A\langle G' \rangle$ y el cual hace commutar también al diagrama (10.17). \square

10.2.5. Ejercicios y Complementos.

1. Mostrar que, en efecto, $((A\langle G \rangle, +, \cdot, f), \cdot)$ es un A -álgebra comutativa, asociativa con unidad.
2. Verificar la propiedad universal del A -álgebra libre sobre un monoide y que φ_* es, en efecto, un homomorfismo de A -álgebras.

CAPÍTULO 11

ANILLO Y ÁLGEBRA DE POLINOMIOS

En este capítulo desarrollaremos las propiedades principales del anillo de polinomios, el cual resultará como un caso particular de un A -álgebra libre sobre el monoide libre abeliano $\mathbb{N}\langle S \rangle$, sobre un conjunto S . En particular estudiaremos las propiedades fundamentales del anillo de polinomios sobre un campo K y sobre un conjunto finito S .

11.1. Conceptos y Propiedades Generales

Sea, entonces, $(\mathbb{N}\langle S \rangle, \cdot)$ el monoide libre sobre un conjunto $S \neq \emptyset$, expresado en forma multiplicativa. (Ver ejercicio 8.2.6,8). Es decir que

$$s_1^{m_1} \cdots s_n^{m_n} := m_1 s_1 + \cdots + m_n s_n, \quad s_\nu \in S, \quad m_\nu \in \mathbb{N}, \quad \nu = 1, \dots, n.$$

En general, un elemento de $\mathbb{N}\langle S \rangle$, lo podemos escribir como la expresión

$$(11.1) \quad M(S) := \prod_{s \in S} s^{n_s} := \sum_{s \in S} n_s s,$$

la cual tiene sentido, por tratarse siempre de una suma finita. La expresión (11.1) se llama un *monomio simple* de elementos de S , de *grado* $\text{grad } M(S) := \sum_{s \in S} n_s$.

Dados dos monomios simples

$$M(S) := \prod_{s \in S} s^{m_s}, \quad N(S) := \prod_{s \in S} s^{n_s},$$

entonces, su producto es el monomio

$$(11.2) \quad M(S)N(S) = \prod_{s \in S} s^{m_s+n_s}$$

Obviamente de (11.2),

$$(11.3) \quad \text{grad}(M(S)N(S)) = \text{grad } M(S) + \text{grad } N(S).$$

Dado un anillo A commutativo con unidad, llamamos *anillo de polinomios con coeficientes en A* y S como *conjunto de indeterminadas*, al A -álgebra libre, $A\langle\mathbb{N}\langle S \rangle\rangle$, sobre el monoide $\mathbb{N}\langle S \rangle$. Los elementos de $A\langle\mathbb{N}\langle S \rangle\rangle$ los llamamos *polinomios* con coeficientes en el anillo A sobre el conjunto de indeterminadas S . Un polinomio $P \in A\langle\mathbb{N}\langle S \rangle\rangle$, es entonces una combinación lineal de monomios simples de $\mathbb{N}\langle S \rangle$. Dado un polinomio $P \in A\langle\mathbb{N}\langle S \rangle\rangle \setminus \{0\}$, entonces el *grado del polinomio P* , $\text{grad } P$ es el grado del monomio simple de mayor grado que comparece en P . Los polinomios de grado 0 son los elementos de $A \setminus \{0\}$. Al polinomio $P = 0$ no se le asigna ningún grado. Si Q es otro polinomio de grado $\text{grad } Q$, entonces por (11.3) se obtiene

$$(11.4) \quad \text{grad}(PQ) \leq \text{grad } P + \text{grad } Q.$$

La igualdad subsiste siempre si A no posee divisores de 0. (Ver ejercicios 11.1.1).

Decimos que un polinomio P es *homogéneo* de grado $\text{grad } P = m$, si todos sus monomios son de grado m .

Todo polinomio posee una representación única de la forma

$$P = \sum_{g \in \mathbb{N}\langle S \rangle} a_g g$$

Dos polinomios

$$P := \sum_{g \in \mathbb{N}\langle S \rangle} a_g g, \quad Q := \sum_{g \in \mathbb{N}\langle S \rangle} b_g g$$

son iguales Ssi $a_g = b_g, \forall g \in \mathbb{N}\langle S \rangle$.

En particular $P = 0$ Ssi $a_g = 0, \forall g \in \mathbb{N}\langle S \rangle$.

EJEMPLOS 11.1.

1. Sea $S := \{X\}$, en este caso denotaremos por $A[X]$ al anillo de polinomios correspondiente y lo llamaremos el *anillo de polinomios con coeficientes en A en la indeterminada X*. Un monomio simple de grado n es de la forma X^n . El monomio X^0 lo identificamos con el elemento unidad $1 \in A[X]$. Un elemento $P \in A[X]$ es de la forma general

$$(11.5) \quad P := \sum_{v \in \mathbb{N}} a_v X^v.$$

donde $a_v = 0$, salvo un número finito de subíndices $v \in \mathbb{N}$. Dado otro polinomio

$$(11.6) \quad Q := \sum_{v \in \mathbb{N}} b_v X^v.$$

aplicando las definiciones de suma y producto para el A -álgebra libre sobre un monoide, obtenemos

$$(11.7) \quad P + Q := \sum_{v \in \mathbb{N}} (a_v + b_v) X^v.$$

y

$$(11.8) \quad PQ := \sum_{\rho \in \mathbb{N}} c_\rho X^\rho, \quad c_\rho := \sum_{v+\mu=\rho} a_v b_\mu.$$

Más concretamente, sean

$$P := a_3 X^3 + a_2 X^2 + a_1 X + a_0, \quad Q := b_2 X^2 + b_1 X + b_0,$$

entonces

$$P + Q = a_3 X^3 + (a_2 + b_2) X^2 + (a_1 + b_1) X + (a_0 + b_0)$$

y

$$\begin{aligned} PQ &= (a_3 b_2) X^5 + (a_3 b_1 + a_2 b_2) X^4 + (a_3 b_0 + a_2 b_1 + a_1 b_2) X^3 + (a_2 b_0 + a_1 b_1 + a_0 b_2) X^2 \\ &\quad + (a_1 b_0 + a_0 b_1) X^1 + a_0 b_0. \end{aligned}$$

$$\text{grad } P = 3, \quad \text{grad } Q = 2, \quad \text{grad } PQ = 5 = \text{grad } P + \text{grad } Q, \text{ si } a_3 b_2 \neq 0.$$

2. Sea $S := \{X_1, X_2, \dots, X_n\}$, en este caso denotaremos por $A[X_1, \dots, X_n]$ al anillo de polinomios correspondiente y lo llamaremos el *anillo de polinomios con coeficientes en A, en las indeterminadas X_1, \dots, X_n* . Un monomio simple de grado m es de la forma $X_1^{m_1} \cdots X_n^{m_n}$, $m := \sum_{v=1}^n m_v$.

3. Sea $S := \{X, Y\}$ y consideremos el anillo de polinomios $A[X, Y]$. Para ilustrar la suma y producto de polinomios en $A[X, Y]$, consideremos los polinomios

$$P := a_{X^2Y^2}X^2Y^2 + a_{XY}XY + a_XX + a_YY + a_1, \quad Q := b_{X^2}X^2 + b_YY + b_1,$$

entonces

$$P + Q = a_{X^2Y^2}X^2Y^2 + a_{XY}XY + b_{X^2}X^2 + a_XX + (a_Y + b_Y)Y + (a_1 + b_1)$$

y

$$\begin{aligned} PQ &= a_{X^2Y^2}b_{X^2}X^4Y^2 + a_{X^2Y^2}b_YX^2Y^3 + a_{X^2}b_1X^2Y^2 + a_{XY}b_{X^2}X^3Y + a_{XY}b_YXY^2 \\ &\quad + (a_{XY}b_1 + a_Xb_Y)XY + a_Xb_{X^2}X^3 + a_Yb_{X^2}X^2Y + a_Yb_YY^2 + a_1b_{X^2}X^2 + (a_1b_Y + a_Yb_1)Y + a_1b_1. \end{aligned}$$

4. $P := X^3 + \frac{2}{3}X^2 + \frac{1}{2}$ es un polinomio en $\mathbb{Q}[X]$, de grado $\text{grad } P = 3$.
5. $P := X^4 + \pi X^3 + \sqrt{3}X + \sqrt{2}$ es un polinomio en $\mathbb{R}[X]$, de grado $\text{grad } P = 4$.
6. $P := (2 + \sqrt{2}i)X^5 + \pi iX^3 + iX^2 + (2 + i)$ es un polinomio en $\mathbb{C}[X]$, de grado $\text{grad } P = 5$.
7. Sea $D_{2 \times 2}$ el anillo de las matrices cuadradas, diagonales, con términos reales. Entonces

$$P := \begin{pmatrix} \pi & 0 \\ 0 & \sqrt{2} \end{pmatrix} X^3 + \begin{pmatrix} 3 & 0 \\ 0 & 4 \end{pmatrix} X^2 + \begin{pmatrix} e & 0 \\ 0 & \pi \end{pmatrix}$$

es un polinomio en $D_{2 \times 2}[X]$, de grado $\text{grad } P = 3$.

8. $P := X^5YZ + \sqrt{2}XY^2Z + (1 + \sqrt{3}i)XYZ^2$ es un polinomio en $\mathbb{C}[X, Y, Z]$ de grado $\text{grad } P = 7$.
9. $P := XYZ + X^2Y + Y^2Z + Z^3 + \sqrt{5}X^3$ es un polinomio homogéneo de grado $\text{grad } P = 3$, en $\mathbb{R}[X, Y, Z]$.

Siendo el anillo de polinomios un caso particular de un A -álgebra libre sobre un monoide, éste posee entonces las siguientes propiedades, inherentes a un A -álgebra libre sobre el monoide libre abeliano: El anillo de polinomios $A\langle\mathbb{N}\langle S\rangle\rangle$ posee la siguiente propiedad universal: Dado un homomorfismo de monoides

$$\varphi : \mathbb{N}\langle S \rangle \rightarrow B,$$

donde B es un A -álgebra comutativa, asociativa con unidad, entonces existe un único homomorfismo de A -álgebras

$$\varphi_* : A\langle\mathbb{N}\langle S\rangle\rangle \rightarrow B,$$

tal que el diagrama

$$(11.9) \quad \begin{array}{ccc} \mathbb{N}\langle S \rangle & \xrightarrow{f} & A\langle\mathbb{N}\langle S\rangle\rangle \\ \varphi \downarrow & \nearrow \varphi_* & \\ B & & \end{array}$$

es comunitativo.

De la propiedad universal resulta, como el lector podrá comprobar, la unicidad, salvo isomorfismo, del anillo de polinomios.

TEOREMA 11.1. Si $\varphi : \mathbb{N}\langle S \rangle \rightarrow \mathbb{N}\langle S' \rangle$ es un homomorfismo de monoides y $((A\langle \mathbb{N}\langle S \rangle \rangle, +, f), \cdot)$, los respectivos anillos de polinomios, entonces existe un único homomorfismo de A -álgebras $\varphi_* : A\langle \mathbb{N}\langle S \rangle \rangle \rightarrow A\langle \mathbb{N}\langle S' \rangle \rangle$, tal que el diagrama

$$(11.10) \quad \begin{array}{ccc} \mathbb{N}\langle S \rangle & \xrightarrow{f} & A\langle \mathbb{N}\langle S \rangle \rangle \\ \varphi \downarrow & & \downarrow \varphi_* \\ \mathbb{N}\langle S' \rangle & \xrightarrow{f'} & A\langle \mathbb{N}\langle S' \rangle \rangle \end{array}$$

es comutativo y si φ es sobreíectivo también lo será φ_* .

Si S y S' son dos conjuntos de la misma cardinalidad, se tiene entonces que

$$\varphi : \mathbb{N}\langle S \rangle \rightarrow \mathbb{N}\langle S' \rangle$$

es un isomorfismo de monoides y del teorema 11.1, resulta que los anillos de polinomios $A\langle \mathbb{N}\langle S \rangle \rangle$ y $A\langle \mathbb{N}\langle S' \rangle \rangle$ son isomorfos.

En particular los anillos de polinomios $A[X_1, \dots, X_n]$ y $A[Y_1, \dots, Y_n]$ son isomorfos.

El anillo de polinomios $A[X, Y]$ en dos indeterminadas, también puede ser obtenido como el anillo $(A[X])[Y]$, es decir como el $A[X]$ -álgebra libre sobre el monoide libre abeliano $\mathbb{N}\langle Y \rangle$. Un elemento $P \in (A[X])[Y]$, es de la forma

$$P = \sum_{v=0}^n a_v(X)Y^v, \quad a_v(X) \in A[X].$$

Se tiene una inyección canónica de monoides

$$\varphi : \mathbb{N}\langle X, Y \rangle \rightarrow (A[X])[Y]$$

definida por $\varphi(X) := X \in (A[X])[Y]$ y $\varphi(Y) := Y \in (A[X])[Y]$. En efecto, vamos a probar, que $((A[X])[Y], +, \cdot, \varphi)$ cumple con la propiedad universal de $A[X, Y]$. Dada una A -álgebra B y un homomorfismo de monoides

$$\psi : \mathbb{N}\langle X, Y \rangle \rightarrow B$$

se tiene, que

$$\psi_* : (A[X])[Y] \rightarrow B,$$

definida por

$$\psi_*(P) := \sum_{v=0}^n a_v(\psi(X))\psi(Y),$$

es un homomorfismo de A -álgebras y es el único que hace commutar al diagrama:

$$(11.11) \quad \begin{array}{ccc} \mathbb{N}\langle X, Y \rangle & \xrightarrow{\varphi} & (A[X])[Y] \\ \psi \downarrow & \nearrow \psi_* & \\ B & & \end{array}$$

Por consiguiente tenemos que el A -álgebra $(A[X])[Y]$ es isomorfa al A -álgebra $A[X, Y]$.

El lector podrá comprobar, que por medio de inducción, dado un conjunto finito

$$S := \{X_1, X_2, \dots, X_n\}$$

se puede mostrar que el A -álgebra de polinomios $A[X_1, \dots, X_n]$ es isomorfa al A -álgebra $(A[X_1, \dots, X_{n-1}])[X_n]$.

11.1.1. Ejercicios y Complementos.

1. Dar, en los incisos siguientes $P + Q$ y PQ e indicar los grados de cada polinomio.
 - a) $P := 3X^3 + 2X^2 + X + \sqrt{2}$, $Q := X^4 + 3X^2 + 1$, $P, Q \in \mathbb{R}[X]$.
 - b) $P := 2X^5 + 3X_2 + 2$, $Q := 2X^3 + 2X^2 + 2$, $P, Q \in \mathbb{Z}_4[X]$.
 - c) $P := 3XY^2 + 2X^2Y + XY + 3$, $Q := 2XY_2 + 3XY + 2$, $P, Q \in \mathbb{Z}_6[X]$.
 - d) Mostrar que en $\mathbb{Z}_4[X]$, el polinomio $P := 2X + 3$ es invertible con $P^2 = 1$.
 - e) Si A es un dominio entero, mostrar que los únicos elementos invertibles en $A[X]$, son los elementos invertibles de A . En particular si K es un campo, mostrar que los únicos elementos invertibles en $K[X_1, \dots, X_n]$ son los elementos de $K \setminus \{0\}$.
2. Mostrar que $\forall P, Q \in A[X_1, \dots, X_n]$, donde A es un anillo comutativo con unidad, $\text{grad}(P + Q) \leq \max(\text{grad } P, \text{grad } Q)$.
3. Dado un conjunto de indeterminadas S , mostrar que $ss' \neq 0$, $\forall s, s' \in S$. Deducir de este resultado que un monomio simple no puede ser 0. En particular si se tiene el anillo de polinomios $A[X_1, \dots, X_n]$, entonces $X_1^{m_1} \cdot X_2^{m_2} \cdots X_n^{m_n} \neq 0$, $\forall m_1, \dots, m_n \in \mathbb{N}$.
4. Mostrar que si A es un dominio entero, entonces el anillo de polinomios $A[X_1, \dots, X_n]$ es un dominio entero. En particular si A es un campo, $A[X_1, \dots, X_n]$ es un dominio entero.
5. Dados dos polinomios $P, Q \in A[X_1, \dots, X_n] \setminus \{0\}$, donde A es un dominio entero, mostrar que $\text{grad } P \leq \text{grad}(PQ)$ y que $\forall P \in A[X_1, \dots, X_n] \setminus \{0\}$, $\text{grad } P \geq 0$.
6. Mostrar que un homomorfismo de anillos $\varphi : A \rightarrow B$ induce un homomorfismo de anillos $\varphi_* : A[X] \rightarrow B[X]$. Si φ es inyectiva entonces también lo es φ_* y si φ es un isomorfismo, entonces φ_* es un isomorfismo.
7. Sean A un anillo comutativo con unidad, $A[X]$ el anillo de polinomios en la indeterminada X . Mostrar que el conjunto $A_n[X]$ de todos los polinomios homogéneos de grado n es un submódulo de $A[X]$.
8. Sean A un anillo comutativo con unidad, S el conjunto

$$S := \{X_1, X_2, \dots\}$$

un conjunto infinito contable y $A[X_1, X_2, \dots]$ el anillo de polinomios correspondiente. Mostrar que la cadena de ideales

$$\mathfrak{a}_0 \subseteq \mathfrak{a}_1 \subseteq \dots \subseteq \mathfrak{a}_k \subseteq \dots,$$

donde $\mathfrak{a}_0 = \mathbf{0}$, $\mathfrak{a}_1 := (X_1), \dots, \mathfrak{a}_k := (X_1, \dots, X_k), \dots$ no es estacionaria, por lo que $A[X_1, X_2, \dots]$ es un anillo no noetheriano y posee ideales que no son generados por un número finito de elementos.

9. Mostrar que si $\varphi : A[X_1, \dots, X_n] \rightarrow B$ es un homomorfismo de A -álgebras y $P(X_1, \dots, X_n) \in A[X_1, \dots, X_n]$, entonces $\varphi(P) = P(\varphi(X_1), \dots, \varphi(X_n))$.
10. Mostrar, por inducción que $A[X_1, \dots, X_n]$ es isomorfo a $(A[X_1, \dots, X_{n-1}])[X_n]$.
11. Si A es un anillo comutativo con unidad, sea $A_n[X]$ el submódulo de $A[X]$ de todos los polinomios homogéneos de grado n . Mostrar que $A[X]$ es el álgebra graduada de grado 0 de la familia de A -módulos $(A_n[X])_{n \in \mathbb{N}}$.
12. Sea A un anillo comutativo con unidad. Para cada $n \in \mathbb{N}$, sea $A_n = A$. Mostrar que el anillo de polinomios en una indeterminada $A[X]$ es isomorfo a $\bigoplus_{n=0}^{\infty} A_n$, en tanto que A -módulo.

13. Bajo las mismas condiciones del ejercicio precedente, mostrar que sobre $\bigoplus_{n=0}^{\infty} A_n$, se puede definir un producto

$$\cdot : \bigoplus_{n=0}^{\infty} A_n \times \bigoplus_{n=0}^{\infty} A_n \rightarrow \bigoplus_{n=0}^{\infty} A_n,$$

de la siguiente forma: Dados $\mathbf{a} := \sum_{n=0}^{\infty} a_n$, $\mathbf{b} := \sum_{m=0}^{\infty} b_m$, definimos

$$\mathbf{a} \cdot \mathbf{b} := \sum_{k=0}^{\infty} c_k, \text{ donde } c_k := \sum_{n+m=k}^{\infty} a_n b_m.$$

Mostrar, además, que con este producto $\bigoplus_{n=0}^{\infty} A_n$, adquiere la estructura de un A -álgebra graduada, de grado 0 con unidad, la cual es isomorfa a $A[X]$.

11.2. Anillo de Polinomios sobre un Campo

Particularmente interesantes resultan los anillos de polinomios sobre un campo K , ya que poseen propiedades especiales que no son válidas en el caso de un anillo comutativo con unidad, donde no todos sus elementos son invertibles. En particular demostraremos que si K es un campo, entonces el anillo $K[X]$ es un anillo euclídeo y por ende principal y factorial. Hecho que será de gran ayuda en el estudio de las *raíces* de polinomios en una indeterminada. Como veremos más adelante, algunas propiedades del anillo A se transmiten al anillo de polinomios $A[X_1, \dots, X_n]$, entonces si éstas valen para el anillo $K[X]$, como $K[X_1, \dots, X_n] = K[X_1, \dots, X_{n-1}]$, también valdrán para el anillo $K[X_1, \dots, X_n]$. Por esta razón en esta sección desarrollaremos las propiedades principales del anillo $K[X]$, donde K es un campo cualquiera.

Si P es un polinomio en $A[X]$, donde A es un anillo comutativo con unidad, sabemos que si $\text{grad } P = n$, entonces $P = a_n X^n + \dots + a_0$, donde $a_n \neq 0$. Al coeficiente a_n lo llamaremos el *coeficiente principal* del polinomio P de grado n .

11.2.1. El Anillo $K[X]$.

Sea K un campo entonces

TEOREMA 11.2. *El anillo $K[X]$ con la función*

$$g : K[X] \setminus \{0\} \rightarrow \mathbb{N},$$

definida por $g(P) := \text{grad } P$, $\forall P \in K[X] \setminus \{0\}$, es un anillo euclídeo.

DEMOSTRACIÓN. Por ejercicio 11.1.1.5, $g(P) := \text{grad } P$, cumple con las propiedades a) y b) de una función *grado* sobre $K[X]$. Falta sólo mostrar que cumple con la propiedad c).

En efecto, vamos a mostrar que dados $P, G \in K[X] \setminus \{0\}$, existen polinomios $Q, R \in K[X]$, tales que

$$(11.12) \quad P = QG + R, \quad \text{donde } R = 0 \quad \text{o} \quad \text{grad } R < \text{grad } G.$$

Si $\text{grad } P < \text{grad } G$, entonces no hay nada que mostrar ya que $Q := 0$ y $R := P$, satisfacen (11.12). Sea, entonces $\text{grad } P \geq \text{grad } G$ y

$$P := a_0 + a_1 X + \dots + a_m X^m, \quad G := b_0 + b_1 X + \dots + b_n X^n, \quad n \leq m, \quad a_m \neq 0 \neq b_n.$$

Como K es un campo, podemos formar el polinomio

$$P_1 := P - \frac{a_m}{b_n} X^{m-n} G.$$

Procedamos por inducción sobre el grado de P . Si $m = 0$, entonces $P, G \in K \setminus \{0\}$ y

$$P = \frac{P}{G}G + 0$$

y $Q := \frac{P}{G}$ y $R := 0$ satisfacen (11.12). Si $m = 1$, entonces $n = 0$ o $n = 1$. En el caso en que $n = 0$ se tiene que $G \in K \setminus \{0\}$ y de nuevo

$$P = \frac{P}{G}G + 0.$$

Si $n = 1$, entonces

$$P := aX + b, \quad G := cX + d, \quad a \neq 0 \neq c.$$

y

$$P = (cX + d)\frac{a}{c} + \left(b - \frac{ad}{c}\right)$$

y $Q := \frac{a}{c}, R := \left(b - \frac{ad}{c}\right)$, satisfacen (11.12). Supongamos, por hipótesis de inducción, que el teorema sea válido para todo polinomio de grado $\leq m - 1$ y mostremos que es válido para cualquier polinomio de grado m . Sea, pues, P un polinomio de grado $n \geq 2$, entonces el polinomio

$$P_1 := P - \frac{a_m}{b_n} X^{m-n} G.$$

está bien definido y $\text{grad } P_1 < \text{grad } P$ y

$$P = P_1 + \frac{a_m}{b_n} X^{m-n} G.$$

Si $\text{grad } P_1 < \text{grad } G$ o $P_1 = 0$, estamos listos. De lo contrario, por hipótesis de inducción, el teorema es válido para P_1 y G , por lo que existen polinomios Q_1, R , con $R = 0$ o $\text{grad } R < \text{grad } G$, tales que

$$P_1 = Q_1 G + R.$$

Entonces

$$P = G\left(Q_1 + \frac{a_m}{b_n} X^{m-n}\right) + R.$$

Con lo que queda demostrado el teorema. □

Del teorema 11.2, se obtiene, de forma inmediata, el siguiente

COROLARIO 11.3. *Si K es un campo, entonces el anillo de polinomios $K[X]$ es un anillo principal y por consiguiente factorial.*

Un resultado inverso al corolario 11.3 es el siguiente

TEOREMA 11.4. *Si el anillo de polinomios $A[X]$ es un anillo principal, entonces A es un campo.*

DEMOSTRACIÓN. Consideremos la aplicación

$$\hat{\varphi} : A[X] \rightarrow A,$$

inducida por $\hat{\varphi}(a) := a$ y $\hat{\varphi}(X) := 0$. Es decir si $P := a_n X^n + \dots + a_0$, entonces $\hat{\varphi}(P) = a_0$. Entonces $\hat{\varphi}$ es un homomorfismo sobreyectivo de anillos, cuyo núcleo es un ideal principal distinto de 0 , ya que $\ker \hat{\varphi} = (X)$. Como $A[X]$ es principal, es un dominio entero y por consiguiente también A es un dominio entero. Por el teorema de isomorfía resulta que $A[X]/\ker \hat{\varphi}$ es isomorfo a A , por lo que $\ker \hat{\varphi}$ es un ideal primo de $A[X]$ y, por corolario 9.37, $\ker \hat{\varphi}$ es un ideal maximal. Por consiguiente A es un campo. □

De la demostración del teorema 11.4, se infiere que el ideal (X) es un ideal primo y, por consiguiente, el elemento X es un elemento irreducible en $A[X]$. En general se tiene para el caso donde A es un dominio entero el siguiente

TEOREMA 11.5. *Si A es un dominio entero, entonces los elementos de la forma $X - a$, $a \in A$, son elementos primos en $A[X]$ y por consiguiente irreducibles. En particular si A es un campo, entonces los elementos de la forma $bX - a$, $b \in A \setminus \{0\}$, son primos y los ideales de la forma $(bX - a)$ maximales.*

DEMOSTRACIÓN. Dado $a \in A$, consideremos el homomorfismo de anillos

$$\varphi_a : A[X] \rightarrow A,$$

tal que $\varphi_a(b) := b$, $\forall b \in A$ y $\varphi_a(X) = a$. Entonces $\ker \varphi_a = (X - a)$ y, por el teorema de isomorfía, $A[X]/(X - a)$ es isomorfo a A que es un dominio entero. Por lo tanto $(X - a)$ es un ideal primo de $A[X]$ distinto de 0 y, por lema 9.35, $X - a$ es un elemento primo de $A[X]$.

Si A es un campo, entonces, como todo elemento $b \in A \setminus \{0\}$ es invertible, $bX - a = b(X - \frac{a}{b})$ y el ideal $(bX - a) = (X - \frac{a}{b})$. Haciendo $\tilde{a} := \frac{a}{b}$, entonces $(X - \tilde{a}) = \ker \varphi_{\tilde{a}}$, de donde resulta que $A[X]/(bX - a) = A[X]/(X - \tilde{a})$ es isomorfo al campo A . Por lo tanto $(bX - a)$ es un ideal maximal de $A[X]$ y por consiguiente ideal primo. Nuevamente, por lema 9.35, $(bX - a)$ es un elemento primo y por consiguiente irreducible en $A[X]$. \square

Del corolario 11.3 y del teorema 9.51 se obtiene el siguiente resultado, de gran importancia en la teoría de polinomios de una variable, con coeficientes en un campo:

TEOREMA 11.6. *Dado un conjunto finito de polinomios $\{P_1, \dots, P_n\} \subseteq K[X] \setminus \{0\}$, existe el máximo común divisor D de dichos polinomios y $(D) = (P_1, \dots, P_n)$. $D = 1$ Ssi los polinomios P_1, \dots, P_n son primos relativos y en tal caso $(P_1, \dots, P_n) = K[X]$.*

Como, por corolario 11.3, $K[X]$ es un anillo factorial, entonces todo polinomio $P \in K[X]$ se descompone de forma única, salvo producto con un elemento invertible y orden de los factores, en un producto de factores irreducibles (primos) $P = aP_1 \cdots P_m$, donde $a \in K \setminus \{0\}$. Incluso es posible escoger los polinomios P_μ de modo tal que dicho producto sea único.

Como los únicos elementos invertibles en $K[X]$ son los elementos de $K \setminus \{0\}$, dado un polinomio

$$P := a_n X^n + \cdots + a_0,$$

existe un único polinomio asociado a P , de la forma $P_1 := \frac{1}{a_n} P$. El coeficiente principal P_1 es 1. Un polinomio cuyo coeficiente principal es 1 se llama un *polinomio mónico*. Entonces todo polinomio $P \in K[X]$, posee un único asociado mónico. Formemos, entonces, nuestro conjunto de *primos seleccionados* \mathcal{P} , (ver página 174), como el conjunto

$$\mathcal{P} := \{P \in K[X] \mid P \text{ es un elemento primo mónico}\}.$$

Entonces para el caso particular del anillo de polinomios $K[X]$, que es, pues, un anillo factorial, podemos escribir el teorema de factorización única 9.49 de la siguiente forma:

TEOREMA 11.7 (Teorema de Factorización Única). *Todo polinomio $P \in K[X]$ posee una única representación, salvo orden de los factores, como producto de factores primos, monicos $P = aP_1^{m_1} \cdots P_n^{m_n}$, donde $a \in K$ es el coeficiente principal de P y $P_v \in \mathcal{P}$, $\forall v = 1, \dots, n$.*

EJEMPLOS 11.2.

1. Sea $P := 2X^2 - 8 \in \mathbb{Q}[X]$. Como producto de factores primos mónicos, P posee una única representación, salvo orden de sus factores, como

$P = 2(X + 2)(X - 2)$, donde $X + 2, X - 2$, por teorema 11.5, son factores primos. Si no nos limitamos a factores mónicos podemos representar a P de varias formas, donde lo único que varía es el producto por un elemento invertible en \mathbb{Q} . Así tenemos las siguientes representaciones:

$$P = (2X + 4)(X - 2) = (X + 2)(2X - 4) = \frac{1}{2}(2X + 4)(2X - 4) = \frac{1}{4}(4X + 8)(2X - 4)$$

2. Un elemento de un anillo de polinomios puede ser irreducible en un cierto campo y reducible en otro. Por ejemplo el polinomio $P := X^2 - 2$ es irreducible en $\mathbb{Q}[X]$ pero es reducible en $\mathbb{R}[X]$, ya que $P = (X - \sqrt{2})(X + \sqrt{2})$
3. Si $P = X^2 + 1$, P es irreducible en $\mathbb{R}[X]$ pero reducible en $\mathbb{C}[X]$, ya que $P = (X + i)(X - i)$.

Como lo muestran estos ejemplos, los factores irreducibles dependen del campo en el cual se esté estudiando el polinomio. Sin embargo, como nos lo muestra el siguiente teorema, el máximo común divisor de dos polinomios se mantiene invariante bajo una extensión del campo.

TEOREMA 11.8. *Sean κ un subcampo del campo K , $P, Q \in \kappa[X] \setminus \{0\}$. Entonces $D \in \kappa[X]$ es un máximo común divisor de P, Q en $\kappa[X]$ ssi D es un máximo común divisor de P, Q en $K[X]$.*

DEMOSTRACIÓN. Sean $\alpha, \tilde{\alpha}$ los ideales generados por P, Q en $\kappa[X]$ y en $K[X]$ respectivamente. Denotaremos por $(D)_\kappa$, respectivamente por $(D)_K$, los ideales generados por D en $\kappa[X]$, respectivamente en $K[X]$. Por el teorema 9.33, D es un máximo común divisor de P, Q en $\kappa[X]$, Ssi $(D)_\kappa = \alpha$. Vamos a mostrar que $(D)_K = \tilde{\alpha}$. Obviamente $D \in \tilde{\alpha}$, por lo que $(D)_K \subseteq \tilde{\alpha}$. Si $G \in \tilde{\alpha}$, entonces existen polinomios $R, S \in K[X]$, tales que $G = RP + SQ$. Como, por hipótesis, D es un máximo común divisor de P, Q en $\kappa[X]$, existen polinomios $P_1, Q_1 \in \kappa[X]$, tales que $P = DP_1$, $Q = DQ_1$. Entonces $G = RDP_1 + SDQ_1 = D\tilde{G} \in (D)_K$, donde $\tilde{G} := RP_1 + SQ_1 \in K[X]$. Por lo tanto $(D)_K = \tilde{\alpha}$ y D es un máximo común divisor de P, Q en $K[X]$.

Por otra parte, sea $D \in \kappa[X]$ un máximo común divisor de P, Q en $K[X]$. Si \tilde{D} es un máximo común divisor de P, Q en $\kappa[X]$, entonces, por la primera parte del teorema, \tilde{D} es un máximo común divisor de P, Q en $K[X]$ y existe un elemento invertible $e \in K$, tal que $D = e\tilde{D}$. Si $b, \tilde{b} \in \kappa$, son los coeficientes principales de D y \tilde{D} respectivamente, entonces $b = e\tilde{b}$, como $b, b \in \kappa \setminus \{0\}$, resulta entonces que $e = \frac{b}{\tilde{b}} \in \kappa$. Esto quiere decir que D y \tilde{D} son asociados en κ , por lo que con \tilde{D} también D es un máximo común divisor de P, Q en $\kappa[X]$. \square

Como consecuencia inmediata del teorema 11.8, resulta el

COROLARIO 11.9. *Si $D \in \kappa[X]$ es un máximo común divisor en $K[X]$ de $P, Q \in \kappa[X]$, entonces existe un elemento invertible $e \in K$, tal que eD es un máximo común divisor de P, Q en $\kappa[X]$. Por otra parte P, Q son primos relativos en $\kappa[X]$, Ssi son primos relativos en $K[X]$.*

A continuación daremos una serie de lemas que nos ayudarán a entender mejor los criterios de irreducibilidad en el anillo de polinomios $K[X]$.

LEMA 11.10. *Sea A un anillo, \mathfrak{a} un ideal de A y $\mathfrak{a}[X]$, el ideal generado por \mathfrak{a} en $A[X]$. Entonces vale:*

- a) $\mathfrak{a}[X] \cap A = \mathfrak{a}$.
- b) Existe un isomorfismo natural $A[X]/\mathfrak{a}[X] \cong (A/\mathfrak{a})[X]$.
- c) $\mathfrak{a}[X]$ es un ideal primo, Ssi \mathfrak{a} es un ideal primo.

DEMOSTRACIÓN.

- a) Por definición $\mathfrak{a}[X]$ consta de todos los polinomios cuyos coeficientes están en \mathfrak{a} , en particular $\mathfrak{a} \subseteq \mathfrak{a}[X]$, por consiguiente $\mathfrak{a}[X] \cap A = \mathfrak{a}$.
- b) La proyección canónica

$$\pi : A \rightarrow A/\mathfrak{a}$$

induce un homomorfismo sobreíectivo de anillos

$$\pi_* : A[X] \rightarrow (A/\mathfrak{a})[X]$$

definido por $\pi_*(a_n X^n + \cdots + a_0) := \bar{a}_n X^n + \cdots + \bar{a}_0$, donde $\bar{a}_v := \pi(a_v)$, $\forall v = 1, \dots, n$, cuyo núcleo es precisamente el ideal $\mathfrak{a}[X]$. Entonces, por el teorema de isomorfía, π_* induce un isomorfismo natural

$$\hat{\pi}_* : A[X]/\mathfrak{a}[X] \rightarrow (A/\mathfrak{a})[X].$$

- c) Por inciso b), $A[X]/\mathfrak{a}[X]$ es dominio entero Ssi $(A/\mathfrak{a})[X]$ es dominio entero. Por consiguiente $\mathfrak{a}[X]$ es ideal primo Ssi \mathfrak{a} es ideal primo.

□

Como aplicación del lema 11.10 obtenemos el

COROLARIO 11.11. *Un elemento $a \in A \setminus \{0\}$, donde A es un dominio entero, es un elemento primo en A , Ssi es un elemento primo en $A[X]$.*

LEMA 11.12. *Sea A un dominio entero, $a \in A$. $a = P_1 \cdots P_n$, $P_v \in A[X]$, es una descomposición en factores primos de $a \in A[X]$, Ssi es una descomposición en factores primos de a en A . En particular si $A[X]$ es factorial también lo es A .*

DEMOSTRACIÓN. De $0 = \text{grad } a = \text{grad } P_1 + \cdots + \text{grad } P_n$ resulta $\text{grad } P_v = 0$, $\forall v = 1, \dots, n$, por consiguiente $P_1, \dots, P_n \in A$ y, por corolario 11.11, P_1, \dots, P_n elementos primos en A . Por lo que $a = P_1 \cdots P_n$, es una descomposición en factores primos en A . Por otra parte si $a = P_1 \cdots P_n$, es una descomposición en factores primos en A , por corolario 11.11, es también una descomposición en factores primos en $A[X]$.

Por otra parte, si $A[X]$ es un anillo factorial, en particular todo elemento $a \in A$ no invertible, distinto de 0 posee una única descomposición en factores primos en $A[X]$, la cual es también una descomposición en factores primos en A . Si en A existiera otra descomposición en factores primos de a , ésta sería también otra descomposición en factores primos en $A[X]$, en contradicción a que $A[X]$ es factorial. Por lo tanto A debe ser también factorial. □

Más adelante, en el llamado teorema de Gauss, mostraremos que si A es un anillo factorial, entonces también el anillo de polinomios $A[X]$ es factorial. Gauss mostró dicha propiedad para el caso del anillo de los enteros \mathbb{Z} . Sin embargo la demostración se puede ampliar al caso más general de un anillo factorial cualquiera.

Decimos que un polinomio $P \in A[X]$, de grado $\text{grad } P \geq 1$, donde A es un anillo factorial, es un *polinomio primitivo*, si cualquier máximo común divisor de todos sus coeficientes distintos de 0, es un elemento invertible en A .

EJEMPLO 11.3. El polinomio $P := X^4 + 2X + 3$, es un polinomio primitivo en $\mathbb{Z}[X]$, mientras que el polinomio $Q := 2X^4 + 4X^3 + 6X + 12$ no es un polinomio primitivo en $\mathbb{Z}[X]$. En general todo polinomio mónico en $\mathbb{Z}[X]$ es primitivo. Si K es un campo sólo los polinomios cuyos coeficientes distintos de cero sean iguales a 1 son primitivos en $K[X]$.

Si P es un polinomio en $A[X]$, donde A es un anillo factorial, y $d \in A$ es un máximo común divisor de los coeficientes de P , entonces $P = dP_1$, donde P_1 es un polinomio primitivo en $A[X]$. Si d es un elemento invertible en A , entonces, por definición, P es ya un polinomio primitivo.

LEMA 11.13. *Todo polinomio primitivo de $A[X]$, donde A es un anillo factorial, se descompone, en $A[X]$, en producto finito de polinomios primitivos irreducibles.*

DEMOSTRACIÓN. En efecto, sea P es un polinomio primitivo en $A[X]$. Si P es irreducible, no hay nada que mostrar, al igual si $\text{grad } P = 1$, pues en este caso P es irreducible. Sea, entonces, P un polinomio reducible en $A[X]$ y por consiguiente $\text{grad } P \geq 2$. Entonces existen polinomios no invertibles $G, H \in A[X]$, tales que $P = GH$, con $\text{grad } G \neq 0 \neq \text{grad } H$, pues de lo contrario P no sería primitivo, ya que si suponemos, por ejemplo, $\text{grad } G = 0$, entonces $G = a \in A$ y a sería un divisor, no invertible, de todos los coeficientes de P . Por consiguiente G, H son polinomios de $\text{grad} \geq 1$, $\text{grad } G < \text{grad } P$, $\text{grad } H < \text{grad } P$ y deben ser primitivos, pues cualquier divisor común de todos los coeficientes de cualquiera de los factores de P sería divisor común de todos los coeficientes de P . Si suponemos, por hipótesis de inducción, que el lema valga para todo polinomio de grado menor que $\text{grad } P$, entonces como $P = GH$, con $\text{grad } G < \text{grad } P$ y $\text{grad } H < \text{grad } P$, G y H se descomponen, cada uno, en un producto finito de factores primitivos irreducibles, por lo tanto también P . \square

El lema que demostraremos a continuación es una generalización de un lema de Gauss, quien lo demostró para el caso en que $A = \mathbb{Z}$. Nosotros obtendremos el lema original de Gauss, como un corolario de este lema más general.

LEMA 11.14 (Gauss). *Sean A un anillo factorial y $\mathbb{Q}(A)$ su campo de fracciones. Entonces, para un polinomio primitivo $P \in A[X]$, son las siguientes condiciones equivalentes:*

- a) P es irreducible en $A[X]$.
- b) P es irreducible en $\mathbb{Q}(A)[X]$.
- c) P es un factor primo en $\mathbb{Q}(A)[X]$.
- d) P es un factor primo en $A[X]$.

DEMOSTRACIÓN.

- a) \Rightarrow b): Supongamos que P sea reducible en $\mathbb{Q}(A)[X]$, entonces existen polinomios $G, H \in \mathbb{Q}(A)[X]$, $\text{grad } G \geq 1$ y $\text{grad } H \geq 1$, tales que $P = GH$. Si a, b son los productos de todos los denominadores de los coeficientes de G y H respectivamente, entonces $G_1 := aG, H_1 := bH \in A[X]$. y $abP = G_1H_1$, si ab invertible en A , entonces $P = (ab)^{-1}(G_1)(H_1)$, donde $(ab)^{-1}(G_1), (H_1) \in A[X]$, en contradicción a la hipótesis. Si ab no es invertible en A , entonces cualquier factor primo p de ab divide a G_1H_1 , por lo que $p \mid G_1$ o $p \mid H_1$ en $A[X]$, como $A[X]$ es dominio entero, todos los factores primos de ab se cancelan con los de G_1 y H_1 , por lo que finalmente se obtiene $P = G_0H_0$, con $G_0, H_0 \in A[X]$, en contradicción a la hipótesis. Por lo tanto P irreducible en $A[X]$.
- b) \Rightarrow c): Inmediato del teorema 9.47, puesto que, por corolario 11.3, $\mathbb{Q}(A)[X]$ es un anillo factorial.
- c) \Rightarrow d): Supongamos que $P \mid GH$ en $A[X]$, entonces $P \mid GH$ en $\mathbb{Q}(A)[X]$, como P elemento primo en $\mathbb{Q}(A)[X]$, resulta que $P \mid G$ o $P \mid H$, en $\mathbb{Q}(A)[X]$. Supongamos, sin limitación de

la generalidad, que $P \mid G$ en $\mathbb{Q}(A)[X]$. Vamos a mostrar que entonces $P \mid G$ en $A[X]$. Como $P \mid G$ en $\mathbb{Q}(A)[X]$, existe un polinomio $G_1 \in \mathbb{Q}(A)[X]$, tal que $G = PG_1$. Para G_1 existe un elemento $a \in A \setminus \{0\}$, tal que $G_2 := aG_1 \in A[X]$. Entonces $aG = PG_2$. Si a invertible en A , estamos listos, pues entonces $P \mid G$ en $A[X]$. Si a no es invertible en A , entonces todo factor primo p de a en A , divide a PG_2 en $A[X]$, por lo que $p \mid P$ o $p \mid G_2$ en $A[X]$ y éstos se cancelan mutuamente. Como P es primitivo, ningún factor primo de a divide a P , por consiguiente, todo factor primo de a divide únicamente a G_2 , obteniendo, finalmente un polinomio $G_0 \in A[X]$, tal que $G = PG_0$, lo que nos muestra que $P \mid G$.

d) \Rightarrow a): Obvio, ya que todo factor primo de un anillo es irreducible en el anillo. \square

Como una consecuencia de los pasos utilizados en la demostración de la parte c) \Rightarrow d) se tiene el siguiente

COROLARIO 11.15. *Si el polinomio primitivo $P \in A[X]$ es un divisor de $G \in A[X]$ en $\mathbb{Q}(A)[X]$, entonces es también un divisor de G en $A[X]$.*

El lema de Gauss 11.14 nos permite reformular el lema 11.13 de la siguiente forma:

COROLARIO 11.16. *Todo polinomio primitivo de $A[X]$, donde A es un anillo factorial, se descompone, en $A[X]$, en producto finito de polinomios primos.*

Si P es un polinomio cualquiera, no invertible en $A[X]$, donde A es un anillo factorial, entonces, por lo anteriormente visto, si $d \in A$ es un máximo común divisor de todos los coeficientes de P , $P = dP_1$, donde P_1 es un polinomio primitivo, el cual, por corolario 11.16, se descompone, en $A[X]$, en un producto finito de factores primos primos y si d no es invertible en A , entonces también d se descompone en factores primos en A y por consiguiente el polinomio P se descompone, en $A[X]$, en un producto finito de factores primos. Esto nos lleva, en virtud del teorema 9.47, de los lemas 11.12 y 11.14 y del corolario 11.16, a enunciar el siguiente

TEOREMA 11.17 (Teorema de Gauss). *El anillo de polinomios $A[X]$ es un anillo factorial, Ssi el anillo A es factorial.*

En los dos siguientes corolarios enunciamos el lema y el teorema originales de Gauss:

COROLARIO 11.18 (Gauss, lema original). *Un polinomio mónico $P \in \mathbb{Z}[X]$ es irreducible en $\mathbb{Z}[X]$ Ssi es irreducible en $\mathbb{Q}[X]$.*

COROLARIO 11.19 (Teorema Original de Gauss). *El anillo de polinomios $\mathbb{Z}[X]$ es un anillo factorial.*

Aplicando, inductivamente, el teorema de Gauss al anillo de polinomios $A[X]$, donde A es un anillo factorial, se obtiene para el caso de un número contable de indeterminadas el siguiente

COROLARIO 11.20. *Si A es un anillo factorial, entonces el anillo de polinomios $A[X_1, X_2, \dots]$ es un anillo factorial. En particular, si K es un campo, entonces el anillo $K[X_1, X_2, \dots]$ es factorial.*

En general si A es un anillo principal, el anillo de polinomios $A[X]$ no necesariamente es principal, salvo que A sea un campo, como se demostró en el corolario 11.3. (Ver ejercicio 11.2.3.6). Sin embargo el teorema de la base de Hilbert nos dice que si A es un anillo noetheriano, entonces el anillo de polinomios $A[X_1, \dots, X_n]$ es también noetheriano. Este teorema es de suma importancia en la geometría algebraica.

TEOREMA 11.21 (Teorema de la Base de Hilbert). *Si A es un anillo noetheriano, entonces también lo es el anillo de polinomios $A[X]$.*

DEMOSTRACIÓN. Supongamos que $A[X]$ no sea un anillo noetheriano y sea \mathfrak{a} un ideal de $A[X]$ que no es finitamente generado. Sea $P_1 \in \mathfrak{a}$ un polinomio de menor grado. Escogido P_k , sea P_{k+1} un polinomio de menor grado en $\mathfrak{a} \setminus (P_1, \dots, P_k)$. n_k sea el grado de P_k y a_k su coeficiente principal. Entonces, por la forma en que se escogieron los P_k , se tiene

$$n_1 \leq n_2 \leq \dots \leq n_k \leq \dots .$$

Vamos a mostrar que entonces la cadena de ideales en A

$$(11.13) \quad \mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \dots \subseteq \mathfrak{a}_k \subseteq \dots ,$$

donde $\mathfrak{a}_\kappa := (a_1, \dots, a_\kappa)$, $\kappa = 1, 2, \dots$, no puede ser estacionaria. En contradicción a que A es un anillo noetheriano. En efecto, supongamos que $\mathfrak{a}_k = (a_1, \dots, a_k) = (a_1, \dots, a_{k+1}) = \mathfrak{a}_{k+1}$. Entonces tendríamos una ecuación

$$(11.14) \quad a_{k+1} = \sum_{\kappa=1}^k b_\kappa a_\kappa, \quad b_\kappa \in A.$$

y

$$G := P_{k+1} - \sum_{\kappa=1}^k b_\kappa X^{n_{k+1}-n_\kappa} P_\kappa \in \mathfrak{a} \setminus (P_1, \dots, P_k)$$

sería un polinomio de grado menor que el grado de f_{k+1} , en contradicción a la escogencia de P_{k+1} . \square

Esta corta demostración, sin duda la más corta que existe del teorema de la base de Hilbert, se la debemos a Heidrun Sarges, [21]. Ver también [14].

Como un corolario al teorema 11.21 obtenemos entonces

COROLARIO 11.22. *Si A es un anillo noetheriano, entonces el anillo de polinomios $A[X_1, \dots, X_n]$ es también noetheriano. En particular el anillo $K[X_1, \dots, X_n]$, donde K es un campo, es noetheriano.*

11.2.2. Criterios de Irreducibilidad. En general, determinar si un determinado polinomio es o no irreducible en $A[X]$, es una tarea bastante difícil. Sin embargo, existen algunos criterios que nos permitirán, en algunos casos, determinar la irreducibilidad o reducibilidad de un determinado polinomio en el anillo factorial $A[X]$.

Si P es un polinomio mónico reducible del anillo de polinomios factorial $A[X]$ y $P = GH$, $G, H \in A[X]$, entonces los coeficientes de G, H pueden ser escogidos de forma tal que G, H sean mónicos. En efecto, supongamos que a, b sean los coeficientes principales de G, H respectivamente. Entonces, como P es mónico, $ab = 1$, por lo que a, b invertibles en A y $P = (bG)(aH)$ es una descomposición de P en factores mónicos.

Si el grado de un polinomio es pequeño, en algunos casos, el método de comparación de coeficientes puede dar un buen resultado. Consideremos el polinomio $P := X^3 + 4X^2 + 5X + 1$ en $\mathbb{Z}[X]$. De ser reducible, tendría que existir un factor lineal de la forma $X + c$ y un factor de grado 2, de la forma $X^2 + aX + b$, ya que P es mónico. Entonces

$$(11.15) \quad X^3 + 4X^2 + 5X + 1 = (X^2 + aX + b)(X + c) = X^3 + (a + c)X^2 + (ac + b)X + bc$$

Comparando los coeficientes

$$(11.16) \quad a + c = 4$$

$$(11.17) \quad ac + b = 5$$

$$(11.18) \quad cb = 1$$

De la ecuación 11.18 se obtiene que $c = b = 1$ o $c = b = -1$. Resultado que, como el lector comprobará, no es compatible con las ecuaciones 11.16 y 11.17.

Supongamos que \mathfrak{m} sea un ideal maximal del anillo factorial A , tal que A/\mathfrak{m} sea finito. Entonces la proyección canónica

$$\pi : A \rightarrow A/\mathfrak{m}$$

induce un homomorfismo sobreyectivo

$$\pi_* : A[X] \rightarrow (A/\mathfrak{m})[X]$$

Si P es un polinomio reducible en $A[X]$, que no posee coeficientes en \mathfrak{m} , entonces existen $G, H \in A[X]$, tales que $P = GH$ y $\pi_*(P) = \pi_*(GH) = \pi_*(G)\pi_*(H)$. Es decir, $\bar{P} = \pi_*(P)$ es reducible en $(A/\mathfrak{m})[X]$. Por consiguiente si \bar{P} es un polinomio irreducible en $(A/\mathfrak{m})[X]$, entonces cualquier representante $P \in A[X]$ de \bar{P} es irreducible en $A[X]$.

Veamos un ejemplo concreto. Consideremos el polinomio $P := X^5 - X^2 + 1$ en $\mathbb{Z}[X]$ y $\mathfrak{m} := (2)$, entonces $\mathbb{Z}/\mathfrak{m} = \mathbb{Z}_2$ y $\bar{P} = X^5 + X^2 + 1$. En \mathbb{Z}_2 existen únicamente dos polinomios de grado 1, que son X y $X + 1$, el lector comprobará fácilmente que \bar{P} no es divisible por ninguno de los dos polinomios. Por consiguiente \bar{P} no es reducible en factores lineales. Analicemos ahora la posibilidad de que \bar{P} se descomponga en algún factor de grado 2. Los polinomios de grado 2 en $\mathbb{Z}_2[X]$, son $X^2, X^2 + X = X(X + 1), X^2 + 1 = (X + 1)^2$, que por ser múltiplos de X o de $X + 1$, no vienen al caso y el polinomio $X^2 + X + 1$, del cual se verifica fácilmente que no es un factor de \bar{P} . Por consiguiente \bar{P} es irreducible en $\mathbb{Z}_2[X]$ y, por lo tanto, irreducible en $\mathbb{Z}[X]$.

Otro criterio muy importante para determinar la irreducibilidad de un polinomio en un anillo factorial es el llamado criterio de Eisenstein:

TEOREMA 11.23 (Criterio de Eisenstein). *Sean A un anillo factorial,*

$$P := \sum_{v=0}^n a_v X^v$$

un polinomio en $A[X]$ y $p \in A$ un elemento primo, tales que se cumplan las siguientes condiciones:

- a) *Los coeficientes de P son, a excepción del coeficiente principal, divisibles por p*
- b) *a_0 no es divisible por p^2 .*

Entonces P es irreducible en $A[X]$.

DEMOSTRACIÓN. Supongamos que existan polinomios $G, H \in A[X]$, $\text{grad } G \geq 1$, $\text{grad } H \geq 1$, tales que $P = GH$, donde

$$G = b_r X^r + \cdots + b_0$$

$$H = c_s X^s + \cdots + c_0.$$

Por hipótesis, $a_0 = b_0 c_0$ es divisible por p , pero no por p^2 . Como p es un elemento primo, debe valer que $p \mid b_0$ o $p \mid c_0$, pero no ambos al mismo tiempo. Supongamos, sin limitación de la generalidad, que $p \mid b_0$ y sea b_m , $0 \leq m \leq r$ el primer coeficiente de G que no

pertenece al ideal (p) , el cual existe, ya que, por hipótesis, $a_n = b_r c_s \notin (p)$ y, al menos, $b_r \notin (p)$. Efectuando el producto se obtiene para el coeficiente a_m de P

$$a_m = \sum_{\mu=0}^m b_\mu c_{m-\mu} = b_m c_0 + \sum_{\mu=0}^{m-1} b_\mu c_{m-\mu}.$$

Por definición de m se tiene que

$$\sum_{\mu=0}^{m-1} b_\mu c_{m-\mu} \in (p).$$

Como, por a), también $a_m \in (p)$, ya que $m \leq r < n = r + s$, se obtiene, por substracción, que

$$b_m c_0 = a_m - \sum_{\mu=0}^{m-1} b_\mu c_{m-\mu} \in (p).$$

Como $p \notin (p)$ y p elemento primo, debe valer $c_0 \in (p)$, lo que implicaría $p^2 \mid a_0$, en contradicción a la condición b). Por lo tanto P es irreducible. \square

Para el caso en que $A = \mathbb{Z}$, el criterio de Eisenstein se puede reformular como el siguiente

COROLARIO 11.24 (Criterio de Eisenstein para Polinomios sobre \mathbb{Z}). *Sean*

$$P := \sum_{v=0}^n a_v X^v$$

un polinomio en $\mathbb{Z}[X]$ y $p \in \mathbb{Z}$ un número primo, tales que se cumplan las siguientes condiciones:

- a) *Los coeficientes de P son, a excepción del coeficiente principal, divisibles por p*
- b) *a_0 no es divisible por p^2 .*

Entonces P es irreducible en $\mathbb{Z}[X]$.

EJEMPLOS 11.4.

1. Los polinomios de la forma $X^n - p$, donde $p \in \mathbb{Z}$ es un número primo, son, por el criterio de Eisenstein, irreducibles en $\mathbb{Z}[X]$ y por consiguiente, por el lema de Gauss, irreducible en $\mathbb{Q}[X]$.
2. Consideremos el polinomio $P := X^4 + 5X + 10X + 15$. El número primo $p := 5$ divide a todos los coeficientes de P , salvo al principal, pero $p^2 = 25 \nmid 15$. Por consiguiente, por el criterio de Eisenstein, P es irreducible en $\mathbb{Z}[X]$ y, por el lema de Gauss, irreducible en $\mathbb{Q}[X]$.
3. Consideremos, en $\mathbb{Q}[X]$, el polinomio $P := \frac{5}{2}X^4 + \frac{7}{6}X^3 + \frac{14}{3}X^2 + \frac{21}{2}$, entonces $6P = P_1 := 15X^4 + 7X^3 + 28X^2 + 63$ es un polinomio en $\mathbb{Z}[X]$ y satisface las condiciones para aplicar el criterio de Eisenstein. Entonces P_1 es irreducible en $\mathbb{Z}[X]$ y por consiguiente también P .

En algunos casos, aunque el polinomio P no satisfaga las condiciones para aplicar el criterio de Eisenstein, es posible, por medio de un automorfismo sobre el anillo $A[X]$, transformar P en un polinomio que cumpla con las condiciones deseadas. El siguiente lema, cuya demostración dejamos al lector, nos da la justificación para hacerlo.

LEMA 11.25. *Sean A un anillo factorial y*

$$\varphi : A[X] \rightarrow A[X]$$

un automorfismo. Entonces el polinomio P es irreducible en $A[X]$ Ssi $\varphi(P)$ es irreducible en $A[X]$.

Es decir que la irreducibilidad de un polinomio es invariante bajo automorfismos. En particular es invariante bajo automorfismos de la forma $X \mapsto X - a$, $a \in A$. Como una aplicación de esta propiedad vamos a mostrar el siguiente resultado:

TEOREMA 11.26. *Sea $p \in \mathbb{N}$ un número primo, entonces el polinomio*

$$P := X^{p-1} + X^{p-2} + \cdots + X + 1$$

es irreducible en $\mathbb{Z}[X]$

DEMOSTRACIÓN. Consideremos el automorfismo

$$\varphi : \mathbb{Z}[X] \rightarrow \mathbb{Z}[X]$$

tal que $\varphi(X) := X + 1$, $\varphi(a) := a$, $\forall a \in A$ y aplíquemolo a la igualdad

$$X^p - 1 = (X - 1)P.$$

Esto nos da la igualdad

$$(X + 1)^p - 1 = ((X + 1) - 1)\varphi(P) = X\varphi(P).$$

Usando el binomio de Newton

$$X\varphi(P) = \sum_{v=0}^p \binom{p}{v} X^v - 1 = \sum_{v=1}^p \binom{p}{v} X^v,$$

de donde resulta

$$\varphi(P) = \sum_{v=1}^p \binom{p}{v} X^{v-1}.$$

Entonces el coeficiente principal de $\varphi(P)$ es 1. Para $v \neq p$ se tiene que $p \mid \binom{p}{v}$ y para $v = 1$, $\binom{p}{1} = p$, que no es divisible por p^2 . Entonces, por el criterio de Eisenstein, $\varphi(P)$ es irreducible en $\mathbb{Z}[X]$ y, por lema 11.25, P irreducible en $\mathbb{Z}[X]$. \square

Como resultado del teorema 11.26, podemos inferir que los siguientes polinomios son irreducibles en $\mathbb{Z}[X]$:

- a) $X^2 + X + 1$.
- b) $X^4 + X^3 + X^2 + X + 1$.
- c) $X^6 + X^5 + X^4 + X^3 + X^2 + X + 1$.

La siguiente reflexión nos da un método útil para saber, de manera sencilla, si un determinado polinomio mónico Q divide al polinomio P en el anillo $A[X]$, donde A es un anillo factorial. (Si A es un campo, no importará si Q es polinomio mónico o no). Supongamos que $Q \mid P$, entonces P está en el ideal $\mathfrak{a} := (Q)$ y la clase $\bar{P} = \bar{0}$ en $A[X]/\mathfrak{a}$. Viceversa, si la clase $\bar{P} = \bar{0}$ en $A[X]/\mathfrak{a}$, entonces $P \in \mathfrak{a}$ y $Q \mid P$. Como la aplicación canónica

$$\pi : A[X] \rightarrow A[X]/\mathfrak{a}$$

es un homomorfismo de anillos, si

$$P := a_n X^n + a_{n-1} X^{n-1} + \cdots + a_0,$$

entonces

$$\bar{P} = \bar{a}_n \xi^n + \bar{a}_{n-1} \xi^{n-1} + \cdots + \bar{a}_0,$$

donde ξ es la clase de X (mód α). Si

$$Q := X^m + b_{m-1} X^{m-1} + \cdots + b_0, \quad m < n,$$

entonces

$$\bar{Q} = \xi^m + \bar{b}_{m-1} \xi^{m-1} + \cdots + \bar{b}_0 = \bar{0}$$

Por lo que se obtiene

$$(11.19) \quad \xi^m = -(\bar{b}_{m-1} \xi^{m-1} + \cdots + \bar{b}_0).$$

Entonces para calcular \bar{P} , substituimos, en \bar{P} , ξ^m por (11.19). Si la expresión se anula, entonces $P \in \alpha$ y $Q \mid P$.

Veamos algunos ejemplos concretos:

EJEMPLOS 11.5.

1. Sean $P := X^3 + X^2 + 1$ y $Q := X - 1$ polinomios en $\mathbb{Z}[X]$. Entonces $\bar{Q} = \xi - \bar{1} = \bar{0}$, por lo que $\xi = \bar{1}$. Substituyendo, en \bar{P} , X por $\bar{1}$, se obtiene $\bar{P} = \bar{1} + \bar{1} + \bar{1} = \bar{3} \neq \bar{0}$, por consiguiente $Q \nmid P$.
2. Sean $P := X^2 + 2X + 1$, $Q := X + 1$ polinomios en $\mathbb{Z}[X]$. Entonces $\bar{Q} = \xi + \bar{1} = \bar{0}$, por lo que $\xi = -\bar{1}$. Haciendo la sustitución en \bar{P} , obtenemos $\bar{P} = \bar{1} - \bar{2} + \bar{1} = \bar{0}$. Por lo tanto $(X + 1) \mid P$.
3. Sea $A := \mathbb{Z}_2$ y consideremos los polinomios en $A[X]$, $P := X^4 + X^3 + X^2 + 1$ y $Q := X + 1$. Entonces, como $1 = -1$ en \mathbb{Z}_2 , obtenemos $\xi = 1$, substituyendo en \bar{P} , obtenemos $\bar{P} = \bar{1} + \bar{1} + \bar{1} + \bar{1} = \bar{0}$ en $\mathbb{Z}_2[X]$. Entonces $Q \mid P$ en $\mathbb{Z}_2[X]$. Si consideramos a P y a Q como polinomios en $\mathbb{Z}[X]$, entonces $\xi = -1$ y obtendríamos $\bar{P} = \bar{1} - \bar{1} + \bar{1} + \bar{1} = \bar{2} \neq \bar{0}$. Es decir que $Q \nmid P$ en $\mathbb{Z}[X]$.
4. Sean $P := X^4 + X^3 + X^2 + 1$ y $Q := X^2 - X - 1$ polinomios en $\mathbb{Z}[X]$. Entonces $\xi^2 - \xi - \bar{1} = \bar{0}$, por lo que $\xi^2 = \xi + \bar{1}$. Entonces

$$\bar{P} = (\xi + \bar{1})^2 + \xi(\xi + \bar{1}) + (\xi + \bar{1}) + \bar{1} = 2\xi^2 + 4\xi + \bar{3} \neq \bar{0}.$$

Por lo tanto $Q \nmid P$ en $\mathbb{Z}[X]$.

11.2.3. Ejercicios y Complementos.

1. Sea $A[X]$ el anillo de polinomios sobre el anillo comutativo con unidad A . Sean $F, G \in A[X]$, $G \neq 0$ y $b \in A$ el coeficiente principal de G . Mostrar que existen polinomios $Q, R \in A[X]$, tales que

$$(11.20) \quad b^s F = QG + R, \quad R = 0, \text{ o } \text{grad } R < \text{grad } G.$$

Además $s \in \mathbb{N}$, tal que $s = 0$ si $F = 0$ y si $F \neq 0$, entonces $s = \max\{0, \text{grad } F - \text{grad } G + 1\}$. Por otra parte, si b no es divisor de 0, entonces Q y R están únicamente determinados. (Ayuda: ver procedimiento de la demostración del teorema 11.2 y tener en cuenta que no podemos dividir por el coeficiente principal de G). Como el lector observará, si bien en un anillo comutativo cualquiera, con unidad, no vale el algoritmo euclídeo, vale la ecuación (11.20), que es una versión débil del algoritmo euclídeo.

2. Mostrar que en un anillo euclídeo A , $d \in A$ es un máximo común divisor de $a, b \in A$, Ssi existen $c, d \in A$, tales que $d = ca + db$. En general, d es el máximo común divisor de a_1, \dots, a_n , Ssi existen $c_1, \dots, c_n \in A$, tales que $d = c_1 a_1 + \cdots + c_n a_n$.

3. Sea $\mathbb{Q}(A)$ el campo de fracciones del anillo factorial A . Dados dos polinomios $P, G \in A[X]$, de grado ≥ 1 , mostrar que:
- Existen $a, b \in A$, tales que $P = aP_1$, $G = bG_1$, donde P_1, G_1 son polinomios primitivos en $A[X]$.
 - Si $D \in \mathbb{Q}(A)[X]$ es un máximo común divisor de P_1, G_1 , por una adecuada multiplicación de D con elementos de $\mathbb{Q}(A)$, se obtiene un polinomio primitivo, $\tilde{D} \in A[X]$ y \tilde{D} sigue siendo un máximo común divisor de P_1, G_1 en $\mathbb{Q}(A)[X]$.
 - Si D_1 es un máximo común divisor de P_1, G_1 en $A[X]$, entonces $D_1 \mid \tilde{D}$ en $\mathbb{Q}(A)[X]$ y D_1 es un polinomio primitivo.
 - $D_1 \mid \tilde{D}$ en $A[X]$. (Ver corolario 11.15).
 - $\tilde{D} \mid D_1$ en $A[X]$.
 - D_1, \tilde{D} son asociados en $A[X]$ y por consiguiente \tilde{D} es un máximo común divisor de P_1, G_1 en $\mathbb{Z}[X]$.
 - Multiplicando \tilde{D} por un máximo común divisor de a, b en A , se obtiene un máximo común divisor de P, G en $A[X]$.
4. Utilizar el algoritmo euclídeo, aplicable en $\mathbb{Q}[X]$ y usar un procedimiento similar al empleado en la página 40, para encontrar, en el anillo $\mathbb{Q}[X]$, un máximo común divisor de los polinomios

$$P := X^8 + 3X^7 + 3X^6 + 3X^5 + X^4 + 2X^3 + 2X^2 + 2X + 1$$

y

$$G := X^4 + X^3 + 2X^2 + X + 1.$$

Usar ejercicio precedente, si necesario, para obtener el máximo común divisor de dichos polinomios en $\mathbb{Z}[X]$. (Nótese que P, G son polinomios primos en $\mathbb{Z}[X]$).

- Mostrar que el polinomio $P := X^4 + 3X^3 + 3X^2 - 5$ es irreducible en $\mathbb{Z}[X]$. (Ayuda: Mostrar que \bar{P} es irreducible en $\mathbb{Z}_3[X]$ usando los procedimientos expuestos en las páginas 204 y 206).
- Sea \mathfrak{p} un ideal primo del anillo de polinomios $A[X]$, donde A es un anillo principal. Mostrar que:
 - $\mathfrak{p} \cap A$ es un ideal primo de A .
 - Si $\mathfrak{p} \cap A = (0)$, entonces \mathfrak{p} es un ideal principal generado por un polinomio irreducible $P \in A[X]$. (Ayuda: Considerar un polinomio P de grado minimal en \mathfrak{p} y aplicar ecuación (11.20)).
 - Si P, p son elementos primos de $A[X]$ y A respectivamente, tales que $p \nmid P$, entonces $\mathfrak{p} := (p, P)$ es un ideal primo de $A[X]$.
 - Si \mathfrak{p} es un ideal primo de $A[X]$, entonces \mathfrak{p} es un ideal principal o $\mathfrak{p} = (p, P)$, donde p, P son elementos primos de A y $A[X]$ respectivamente. (Ayuda: Si $\mathfrak{p} \cap A \neq (0)$, entonces $\mathfrak{p} \cap A$ es un ideal primo de A generado por un elemento primo $p \in A$, como A es principal (p) es también un ideal maximal y $A/(p)$ es un campo, por lo que el anillo $(A/(p))[X] \approx A[X]/(pA[X])$ es principal. Usar entonces los resultados del corolario 9.10 y lema 11.10).
- En los incisos siguientes, dar la imagen del polinomio $P \in A[X]$, en el anillo $A[X]/(\mathfrak{Q})$:
 - $P := X^3 + 2X^2 + 3X - 1$, $\mathfrak{Q} := X^2 - 2$, $A := \mathbb{Q}$. Mostrar que todo elemento de $\mathbb{Q}[X]/(\mathfrak{Q})$ es de la forma $a + b\xi$, donde ξ es la clase de X (mód (\mathfrak{Q})) y $a, b \in \mathbb{Q}$.

- b) $P := X^5 + X^4 + X^3 + X^2 + X + 1$, $Q := X^2 + 1$, $A := \mathbb{R}$. Mostrar que todo elemento de $\mathbb{R}[X]/(Q)$ es de la forma $a + b\xi$, donde ξ es la clase de X ($\text{mód } (Q)$) y $a, b \in \mathbb{R}$.
- c) $P := X^5 + X^4 + X^3 + X^2 + X + 1$, $Q := X^3 - 3$, $A := \mathbb{Q}$. Mostrar que todo elemento de $\mathbb{Q}[X]/(Q)$ es de la forma $a + b\xi + c\xi^2$, donde ξ es la clase de X ($\text{mód } (Q)$) y $a, b, c \in \mathbb{Q}$.

11.3. Raíces de Polinomios

Las raíces de polinomios en una o en varias indeterminadas han jugado un papel importantísimo tanto en el álgebra como en la geometría. Muchos problemas de la vida real nos llevan a considerar ecuaciones polinómicas o sistemas de ecuaciones polinómicas. El problema de encontrar las raíces de un polinomio o las raíces comunes de un conjunto de polinomios en un anillo A , está íntimamente relacionado con la reducibilidad o irreducibilidad de dichos polinomios en el anillo $A[X]$. Si consideramos el anillo de polinomios $\mathbb{R}[X, Y]$, de la geometría analítica clásica sabemos que el conjunto de raíces del polinomio $X^2 + Y^2 - 1$ es una curva en el plano afín \mathbb{R}^2 llamada una *circunferencia*, con centro en el origen $(0, 0)$ y radio $r = 1$, ver figura 11.1. Si el mismo polinomio lo consideramos como un polinomio en $\mathbb{R}[X, Y, Z]$, entonces el conjunto de sus raíces forman una superficie en \mathbb{R}^3 , llamada *cilindro circular*, ver figura 11.2. En esta sección nos limitaremos a

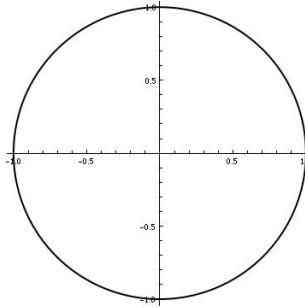


FIGURA 11.1. Circunferencia

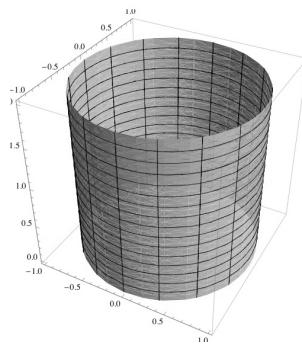


FIGURA 11.2. Cilindro Circular

considerar anillos de polinomios en un número finito de indeterminadas

$$S := \{X_1, \dots, X_n\}.$$

En particular dedicaremos nuestra atención al anillo $K[X]$, donde K es un campo.

11.3.1. Funciones Polinómicas o Polinomiales. Consideremos el anillo de polinomios $A[X_1, \dots, X_n]$, donde A es un anillo conmutativo con unidad. Todo monomio simple $M(X_1, \dots, X_n) \in \mathbb{N}(S)$

$$M(X_1, \dots, X_n) := X_1^{m_1} X_2^{m_2} \cdots X_n^{m_n},$$

induce una *función monomial*

$$\Phi_M : A^n \rightarrow A$$

definida por

$$\Phi_M(a_1, \dots, a_n) := a_1^{m_1} a_2^{m_2} \cdots a_n^{m_n}.$$

Si

$$P := \sum_{M \in \mathbb{N}(S)} \alpha_M M,$$

entonces

$$\Phi_P := \sum_{M \in \mathbb{N}(S)} \alpha_M \Phi_M$$

es una función

$$\Phi_P : A^n \rightarrow A,$$

la *función polinomial* o *polinómica* inducida por el polinomio P . Una función polinomial también se suele llamar una *función algebraica*.

EJEMPLOS 11.6.

1. Si

$$P := a_0 + a_1 X + \cdots + a_n X^n \in A[X],$$

entonces para $\lambda \in A$,

$$\Phi_P(\lambda) = a_0 + a_1 \lambda + \cdots + a_n \lambda^n.$$

2. Si

$$P := X^2 Y^3 Z + 3X^3 Y + 5Y \in \mathbb{Q}[X],$$

entonces para $\lambda := (\lambda_1, \lambda_2, \lambda_3) \in \mathbb{Q}^3$

$$\Phi_P(\lambda) = \lambda_1^2 \lambda_2^3 \lambda_3 + 3\lambda_1^3 \lambda_2 + 5\lambda_2.$$

Decimos que $\mathbf{a} := (a_1, \dots, a_n) \in A^n$ es una *raíz* del polinomio $P \in A[X_1, \dots, X_n]$, si

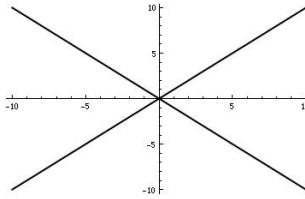
$$\Phi_P(\mathbf{a}) = 0 \in A.$$

Un polinomio $P \in A[X_1, \dots, X_n]$, no necesariamente posee alguna raíz en A^n . Así por ejemplo, el polinomio $X^2 + 1$ no posee ninguna raíz en el campo \mathbb{R} , como tampoco el polinomio $X^2 + Y^2 + 1$ posee raíces en \mathbb{R}^2 . En cambio el polinomio $X^2 - 1$ posee dos raíces en \mathbb{Z} , que son $r_1 := 1$ y $r_2 := -1$ y el polinomio $X^2 - Y^2 = (X + Y)(X - Y)$ posee en \mathbb{R}^2 el siguiente conjunto de raíces :

$$V := \{\lambda \in \mathbb{R}^2 \mid \lambda = (\lambda, -\lambda)\} \cup \{\lambda \in \mathbb{R}^2 \mid \lambda = (\lambda, \lambda)\}. \quad (\text{Ver figura 11.3}).$$

Por comodidad en la escritura, escribiremos $P(\lambda)$ en lugar de $\Phi_P(\lambda)$, para $\lambda \in A^n$.

Analicemos, como ejemplos sui generis, algunos polinomios sobre un anillo con divisores de 0, como, por ejemplo, el anillo de polinomios sobre \mathbb{Z}_4 . Sea $P := 2X^5 + 2X^4 +$

FIGURA 11.3. $V \subseteq \mathbb{R}^2$

$2X^3 + 2X$ en $\mathbb{Z}_4[X]$ y determinemos sus raíces en \mathbb{Z}_4 . Obviamente $0 \in \mathbb{Z}_4$ es una raíz de P . Como 2 es un divisor de 0 en \mathbb{Z}_4 , se tiene

$$P(2) = 2(2^5) + 2(2^4) + 2(2^3) + 2^2 = 0,$$

por consiguiente $2 \in \mathbb{Z}_4$ es una raíz de P . El lector comprobará fácilmente, que también $1, 3 \in \mathbb{Z}_4$ son raíces de P . En particular obsérvese que $2X$ posee dos raíces en \mathbb{Z}_4 , que son 0 y 2 y que $2X = 2(X + 2)$. P es también un divisor de 0 en $\mathbb{Z}_4[X]$, ya que $2P = 0$. El polinomio $Q := 2X^4 + 2X^3 + X$ posee una única raíz en \mathbb{Z}_4 , que es el $0 \in \mathbb{Z}_4$, mientras que el polinomio $2Q = 2X$ posee dos raíces en \mathbb{Z}_4 , 0 y 2 y $\text{grad } 2Q < \text{grad } Q$.

Estos ejemplos nos enseñan que en un anillo con divisores de 0, el anillo de polinomios correspondiente, se comporta de una manera extraña en cuanto a sus raíces, en el caso que existan.

11.3.2. Raíces en el anillo $A[X]$. En esta subsección nos limitaremos al estudio de las raíces de polinomios en una indeterminada. En particular veremos que la existencia de una raíz, en el anillo A , de un polinomio $P \in A[X]$ está íntimamente relacionada con la reducibilidad de P en $A[X]$.

TEOREMA 11.27. *Sea A un anillo commutativo con unidad. Un elemento $a \in A$ es raíz de un polinomio $P \in A[X]$, Ssi el polinomio $X - a$ divide a P en $A[X]$.*

DEMOSTRACIÓN. Si $P = (X - a)G$, $G \in A[X]$, entonces $P(a) = (a - a)G(a) = 0G(a) = 0$ y a es una raíz de P . Por otra parte, supongamos que $a \in A$ es una raíz de P . Como $X - a$ es un polinomio monólico, se obtiene, para P , aplicando la ecuación (11.20), una representación de la forma

$$P = (X - a)Q + R, \quad Q, R \in A[X], \quad \text{grad } R < \text{grad } G = 1.$$

Entonces $R \in A$ y de $0 = P(a) = R(a) = R$, resulta que $R = 0$. Por lo tanto $P = (X - a)G$. \square

Si $P := bX + c$ y $a \in A$ es una raíz de P , entonces $bX + c = (X - a)G$. Como $(X - a)$ es monólico, $\text{grad } G = 0$, es decir un elemento de A , digamos $d := G$. Entonces $bX + c = dX - ad$, de donde $d = b$, el coeficiente principal de P y $c = ad = ab$, es decir $b \mid c$ o b invertible en A . Viceversa, si $b \mid c$ en A o b invertible en A , entonces P posee una raíz en A . Si P es un polinomio de grado 2, digamos $P := b_0 + b_1X + b_2X^2$ y a_1 una raíz de P en A , entonces tenemos que $P = (X - a_1)G$, $\text{grad } G = 1$, ya que $(X - a_1)$ es monólico. Si $G = bX + c$, $b, c \in A$, entonces obtenemos que $P = (X - a)(bX + c)$. G puede o no poseer una raíz en A . Si a_2 , es una raíz de G , entonces $P = (X - a_1)(X - a_2)d$, donde $d = b_2$ el coeficiente principal de P . En el caso en que $a_1 = a_2 = a$, se obtiene $(X - a)^2d$. El lector notará, por lo anteriormente expuesto, que G posee una raíz en A , Ssi $b \mid c$ en A o b invertible en A . En general, para cualquier polinomio $P \in A[X]$, que posea, al menos una raíz en A , se tiene el siguiente

TEOREMA 11.28. *Sea A un anillo y el polinomio $P \in A[X] \setminus \{0\}$ posea, en A , al menos una raíz. Entonces existen un polinomio $G \in A[X]$, que no posee raíces en A , elementos distintos $a_1, \dots, a_m \in A$ y números $n_1, \dots, n_m \in \mathbb{N}$, tales que*

$$(11.21) \quad P = (X - a_1)^{n_1} \cdots (X - a_m)^{n_m} G, \quad y \quad \sum_{\mu=1}^m n_\mu \leq \text{grad } P.$$

Si A es un dominio entero, entonces $\{a_1, \dots, a_m\}$ es el conjunto de todas las raíces de P en A , n_μ es el número más grande, tal que $(X - a_\mu)^{n_\mu} \mid P$ en $A[X]$ y la representación (11.21), de P , es única.

DEMOSTRACIÓN. Procedamos por inducción sobre $\text{grad } P$. Ya vimos que para $\text{grad } P = 1(2)$ vale (11.21). Supongamos, por hipótesis de inducción, que (11.21) valga para todo polinomio G con $2 \leq \text{grad } G < \text{grad } P$ y mostremos que (11.21) vale para P . En efecto, como, por hipótesis del teorema, P posee al menos una raíz $a_1 \in A$, entonces, por teorema 11.27, existe un polinomio $G \in A[X]$, $\text{grad } G < \text{grad } P$, tal que

$$P = (X - a_1)G.$$

Si G no posee raíces en A , estamos listos. De lo contrario, G satisface la hipótesis del teorema y, por hipótesis de inducción, G satisface (11.21) y se tiene

$$G = (X - a_1)^{n_1} \cdots (X - a_m)^{n_m} H, \quad \sum_{\mu=1}^m n_\mu \leq \text{grad } G.$$

y H es un polinomio de $A[X]$, que no posee raíces en A . Entonces

$$P = (X - a_1)G = (X - a_1)(X - a_1)^{n_1} \cdots (X - a_m)^{n_m} H, \quad \sum_{\mu=1}^m n_\mu + 1 \leq \text{grad } P.$$

Si A es un dominio entero, sea $\mathbb{Q}(A)$ su campo de fracciones. Denotemos por \mathcal{M} al conjunto de todas las raíces de P en A . Entonces $\{a_1, \dots, a_m\} \subseteq \mathcal{M}$. Si $a \in \mathcal{M}$, entonces

$$P(a) = (a - a_1)^{n_1} \cdots (a - a_m)^{n_m} G(a) = 0.$$

Como $G(a) \neq 0$ y A es dominio entero, entonces uno de los factores $(a - a_\mu)$ debe de ser igual a 0. Por lo tanto $\mathcal{M} = \{a_1, \dots, a_m\}$. Por otra parte, como G no posee ninguna raíz en A , ninguno de los factores $(X - a_\mu)$ divide a G en $\mathbb{Q}(A)[X]$, y por la factorialidad de $\mathbb{Q}(A)[X]$, n_μ es el mayor número, tal que $(X - a_\mu)^{n_\mu}$ divide a P en $\mathbb{Q}(A)[X]$ y por consiguiente en $A[X]$. En cuanto a la unicidad de la representación, supongamos que se tiene otra representación de P como

$$P = (X - a_1)^{n_1} \cdots (X - a_m)^{n_m} G_1, \quad \sum_{\mu=1}^m n_\mu \leq \text{grad } P.$$

Entonces

$$0 = (X - a_1)^{n_1} \cdots (X - a_m)^{n_m} (G - G_1),$$

y por la integridad de $A[X]$ resulta que $G = G_1$. \square

Si A es un dominio entero, entonces a los números n_μ en (11.21) los llamamos la *multiplicidad u orden* de la raíz a_μ en A . Si $n_\mu = 1$, entonces a_μ es una *raíz simple* del polinomio P . Si $n_\mu > 1$, entonces se dice que a_μ es una *raíz múltiple* de multiplicidad u orden n_μ .

Entonces, si A es un dominio entero, por teorema 11.21 se tiene

$$(11.22) \quad \text{grad } P = \sum_{\mu=1}^m n_\mu + \text{grad } G.$$

Decimos que un polinomio $P \in A[X]$, donde A es un anillo conmutativo con unidad, se descompone en *factores lineales*, si, en (11.21), $G = d \in A$. En tal caso P tiene todas sus raíces posibles en A y d es el coeficiente principal de P .

La igualdad (11.22) nos dice que el número máximo de raíces del polinomio P , incluyendo sus multiplicidades n_μ , en A , en el caso en que A es un dominio entero, no puede superar al grado del polinomio P y que la igualdad se da, únicamente en el caso en que P se descompone en factores lineales en A .

EJEMPLOS 11.7.

1. Sea $P := 2X^3 + 3X^2 - 2X - 3$ un polinomio en $\mathbb{Z}[X]$. Entonces en $\mathbb{Z}[X]$ podemos escribir P como

$$P = X^2(2X + 3) - (2X + 3) = (X^2 - 1)(2X + 3) = (X + 1)(X - 1)(2X + 3),$$

donde $G := 2X + 3$ no posee raíces en \mathbb{Z} . Sin embargo en $\mathbb{Q}[X]$, $(2X + 3) = 2(X + \frac{3}{2})$ y

$$P = (X^2 - 1)(2X + 3) = (X + 1)(X - 1)(X + \frac{3}{2})2,$$

donde $G := 2$ no posee ninguna raíz en $\mathbb{Q}[X]$.

2. Sea $P := X^3 - X^2 - 2X + 2$ en $\mathbb{Q}[X]$, entonces

$$P = X(X^2 - 2) - (X^2 - 2) = (X - 1)(X^2 - 2).$$

Vamos a mostrar que $G := X^2 - 2$ no posee ninguna raíz en $\mathbb{Q}[X]$. En efecto, supongamos que $\frac{p}{q} \in \mathbb{Q}$ sea una raíz de G , donde $p, q \in \mathbb{Z}$ no poseen ningún

divisor común fuera de 1. Entonces se tiene que $2 = \frac{p^2}{q^2}$ y $2q^2 = p^2$. Es decir que el cuadrado de p es un número par, lo que implica que p es también par. Entonces $p = 2p_1$ y $2q^2 = 4p_1^2$. Por consiguiente $q^2 = 2p_1^2$, lo que implicaría que tanto p como q son números pares, en contradicción a que no poseen ningún divisor común, salvo 1. Sin embargo sabemos que existe un número real $\sqrt{2}$, que es raíz de $X^2 - 2$ en $\mathbb{R}[X]$

$$P = (X - 1)(X - \sqrt{2})(X + \sqrt{2})1,$$

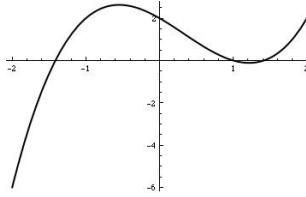
donde $G := 1$ no posee ninguna raíz en $\mathbb{R}[X]$.

Si trazamos la gráfica de la función $\Phi_P : \mathbb{R} \rightarrow \mathbb{R}$, obtenemos las raíces de P en los puntos donde la curva intersecta al eje x . (Ver figura 11.4).

TEOREMA 11.29. *Sea A un dominio entero y $P, G \in A[X] \setminus \{0\}$. Si $G \mid P$ en $A[X]$ y $G \notin A$ y P posee una descomposición en factores lineales en $A[X]$, entonces también G posee una descomposición en factores lineales en $A[X]$.*

DEMOSTRACIÓN. Por hipótesis, P posee, en $A[X]$, una descomposición en factores lineales

$$(11.23) \quad P = (X - a_1)^{n_1} \cdots (X - a_m)^{n_m}d, \quad d \in A, \quad \sum_{\mu=1}^m n_\mu = \text{grad } P.$$

FIGURA 11.4. Φ_P

Si $\mathbb{Q}(A)$ es el campo de fracciones de A , entonces (11.23), es también una descomposición en factores lineales de P en $\mathbb{Q}(A)[X]$ y por la factorialidad de $\mathbb{Q}(A)[X]$ ésta es única. Como $G \mid P$, G no puede tener raíces en $\mathbb{Q}(A)$ que no estén ya en A . Si G no tuviera ninguna raíz en A , entonces, por teorema 11.28,

$$P = (X - b_1)^{r_1} \cdots (X - b_s)^{r_s} G,$$

y por la unicidad de dicha representación, ya que A es un dominio entero, ésta representación debe ser igual a (11.23) y $G = d \in A$, en contradicción a que $G \notin A$. Entonces G satisface las condiciones del teorema 11.28 y posee una descomposición

$$(11.24) \quad G = (X - c_1)^{k_1} \cdots (X - c_l)^{k_l} G_1, \quad c_i \in A, \quad G_1 \in A[X],$$

y G_1 no posee raíces en $\mathbb{Q}(A)$, entonces

$$(11.25) \quad P = P_1(X - c_1)^{k_1} \cdots (X - c_l)^{k_l} G_1, \quad P_1 \in A[X].$$

Si P_1 no tiene raíces en A , entonces, por la unicidad de la representación tenemos que (11.23) debe ser igual a (11.25), por consiguiente $P_1 G_1 \in A$ y (11.25) es una descomposición de G en factores lineales. Si P_1 posee raíces en A , entonces P_1 posee una representación

$$(11.26) \quad P_1 = P_2(X - d_1)^{t_1} \cdots (X - t_j)^{t_j}, \quad P_2 \in A[X],$$

y P_2 no posee raíces en A . Entonces se obtiene que

$$P = P_1 G = (X - d_1)^{t_1} \cdots (X - t_j)^{t_j} (X - c_1)^{k_1} \cdots (X - c_l)^{k_l} P_2 G_1,$$

donde $P_2 G_1$ no posee raíces en A . Entonces, de la unicidad de la representación, resulta que $d = P_2 G_1 \in A$, lo que implica que $G_1 \in A$ y por lo tanto (11.24) es una descomposición en factores lineales de G . \square

El hecho de que un polinomio P , sobre un dominio entero, posea, a lo sumo, $\text{grad } P$ raíces nos lleva al siguiente

TEOREMA 11.30. *Un polinomio de grado $\leq m$ sobre un dominio entero A , con un número infinito de elementos, está únicamente determinado por sus valores sobre $m + 1$ elementos distintos de A . En particular, dos polinomios distintos $P, Q \in A[X]$ inducen funciones Φ_P, Φ_Q distintas sobre A .*

DEMOSTRACIÓN. Supongamos que los valores de los polinomios de grado m , $P, Q \in A[X] \setminus \{0\}$ coincidan en $m + 1$ elementos distintos de A . Entonces el polinomio $H := P - Q$, $\text{grad } H \leq m$, poseería más de $\text{grad } H$ raíces en A , lo cual sólo es posible si $H = 0$. \square

Como una consecuencia del teorema 11.21, se obtiene, para la estructura del grupo de elementos invertibles A^* de un dominio entero A , el siguiente resultado:

TEOREMA 11.31. *Todo subgrupo finito H , del grupo de elementos invertibles A^* de un dominio entero A , es cíclico. En particular, los subgrupos multiplicativos de campos finitos son cílicos.*

DEMOSTRACIÓN. En efecto, para cada entero positivo m , el polinomio $X^m - 1$ posee en A , a lo sumo, m raíces en A , lo que trae, como consecuencia, que existan, a lo sumo, m elementos en H , tales que $a^m = 1$. Es decir que H contendrá, a lo sumo, un único subgrupo de orden m . Entonces, por teorema 6.6, H es cíclico. \square

Recordamos al lector que, dado un dominio entero A , el núcleo del homomorfismo

$$\varphi : \mathbb{Z} \rightarrow A,$$

definido por $\varphi(n) := m \cdot 1_A := \underbrace{1 + \cdots + 1}_n$ es un ideal primo de \mathbb{Z} , $\ker \varphi = (p)$, donde $p = 0$, o p es un número primo, llamado la *característica* del dominio entero A . (Ver ejercicio 9.3.1.4). Si $\ker \varphi = (0)$, la característica de A es 0, entonces A posee un subanillo isomorfo a \mathbb{Z} y si la característica de A es un número primo p , entonces A posee un subanillo isomorfo a \mathbb{Z}_p . En el caso particular en que A es un campo, entonces tendremos campos de característica 0 o bien de característica $p \neq 0$.

Si K es un campo, denotaremos por $\text{car } K$ la característica de K . Obviamente todo campo de característica $\text{car } K = 0$ es infinito, por lo que si K es un campo finito, entonces $\text{car } K = p \neq 0$.

Los campos finitos son también llamados campos de Galois y juegan un papel muy importante en la teoría algebraica de números, en la teoría de códigos y criptografía.

Si K es un campo finito, entonces el grupo aditivo $(K, +)$, es cíclico y $px = 0, \forall x \in K$, entonces tenemos que $\circ(x) \mid p$. Como p es un número primo $\circ(x) = p, \forall x \in K$. Esto implica que $p \mid \circ(K)$. Si q fuera otro primo, distinto de p , tal que $q \mid \circ(K)$, entonces, por teorema 6.6, K tendría un subgrupo H de orden $\circ(H) = q$ y para $x \in H, 0 = px$ implicaría $p \mid \circ(H) = q$, lo cual no es posible. Esto quiere decir, que $\circ(K) = p^m, m \in \mathbb{N}, m \geq 1$. Con esto hemos mostrado el siguiente resultado:

TEOREMA 11.32. *Si K es un campo finito, de característica $p \neq 0$, entonces $\circ(K) = p^m$, donde m es un número entero mayor o igual a 1. Es decir que el número de elementos del campo K es una potencia de la característica p .*

Para los subcampos de un campo finito P , el teorema 11.21 nos lleva al siguiente resultado:

TEOREMA 11.33. *Sea K un campo de característica $p \neq 0$ y p^m elementos. Entonces todo subcampo κ de K posee p^n elementos, donde $n \mid m$. Por otra parte, si n es un divisor de m , entonces K contiene un subcampo κ de p^n elementos. Los elementos de κ son exactamente las raíces, en K , del polinomio $X^{p^n} - X$.*

DEMOSTRACIÓN. Sea κ un subcampo de K que posee p^n elementos y κ^*, K^* los subgrupos multiplicativos correspondientes de elementos invertible. Entonces $p^n - 1 = \circ(\kappa) \mid \circ(K) = p^m - 1$ y vale la siguiente relación de congruencia:

$$(11.27) \quad p^n - 1 \equiv 0, \pmod{(p^n - 1)}.$$

Por el algoritmo euclídeo podemos escribir $m = qn + r, q, r \in \mathbb{Z}, r < n$, o $r = 0$. Considerando que $p^n \equiv 1, \pmod{(p^n - 1)}$ se tiene

$$(11.28) \quad 0 \equiv p^m - 1 = p^{qn} p^r - 1 = p^r - 1, \pmod{(p^n - 1)}.$$

Como $0 \leq p^r - 1 < p^n - 1$, debe valer, por fuerza, $p^r = 1$ y por consiguiente $r = 0$. Por lo tanto $n \mid m$.

Vamos a mostrar, ahora, que K contiene, a lo sumo, un único subcampo κ con p^n elementos. En efecto, como $\circ(\kappa^*) = p^n - 1$, todo elemento $x \in \kappa^*$ satisface la ecuación $x^{p^n} - x = 0$, es decir que x es raíz en K del polinomio $X^{p^n} - X$, el cual posee en K , a lo sumo, p^n raíces, incluyendo al 0.

Finalmente, sea $n \in \mathbb{Z}, n \geq 0$, tal que $n \mid m$, vamos a mostrar que el polinomio $P := X^{p^n} - X$ posee todas sus raíces en K y que el conjunto de éstas forman un subcampo κ de K . Obviamente 0, 1 son raíces de P en K . Dadas $x, y \in K$ raíces de P , $(xy)^{p^n} = x^{p^n}y^{p^n} = xy$, por lo que xy es también una raíz de P . Como $\text{car } K = p$, tenemos que

$$(11.29) \quad (x+y)^{p^n} = \sum_{v=0}^{p^n} \binom{p^n}{v} x^{p^n-v} y^v = x^{p^n} + y^{p^n} \quad (\text{Ver ejercicio 11.3.3,2}).$$

Entonces por (11.29) resulta que con x, y también $x+y$ es raíz de P . Es decir que el conjunto de las raíces de P son cerradas bajo la suma y el producto de K y que 0, 1 son raíces de P . Nos falta sólo mostrar que todas las raíces de P están en K . A tal efecto basta mostrar que K^* posee un subgrupo de orden $p^n - 1$. Como, por teorema 11.31, K^* es cíclico, basta entonces mostrar que $(p^n - 1) \mid (p^m - 1)$ y, por teorema 6.6, K^* posee un subgrupo de orden $p^n - 1$. En efecto, $p^m - 1 = (p^n - 1)q$, donde $q := (p^{m-n} + p^{m-2n} + \dots + p^n + 1)$. \square

En particular, del teorema 11.33, resulta, para $n = 1$, que todo campo K de característica $p \neq 0$ posee un único subcampo κ_p , con, exactamente, p elementos, llamado el *campo primo* de K , cuyos elementos son las raíces, en K , del polinomio $X^p - X$. El campo primo κ_p es entonces isomorfo al campo \mathbb{Z}_p .

TEOREMA 11.34. *Sea K un grupo finito de característica $p \neq 0$ y p^m elementos, entonces el grupo de automorfismos $(\text{Aut}(K), \circ)$ es un grupo cíclico de orden m , generado por el automorfismo*

$$\varphi : K \rightarrow K,$$

definido por $\varphi(x) := x^p, \forall x \in K$.

DEMOSTRACIÓN. Vamos a mostrar que, en efecto, φ es un automorfismo de campos. Como $\text{car } K = p$, se tiene

$$\varphi(x+y) = (x+y)^p = x^p + y^p = \varphi(x) + \varphi(y), \text{ y } \varphi(xy) = (xy)^p = x^p y^p = \varphi(x)\varphi(y), \forall x, y \in K.$$

Lo que muestra que φ es un homomorfismo de campos. Como K finito y todo homomorfismo de campos es inyectivo, (ver ejercicio 9.2.6,7), resulta que φ es un automorfismo de campos. Si $a \in K$ es un generador del grupo K^* , consideremos al conjunto

$$M := \{a^{p^0}, a^p, \dots, a^{p^{m-1}}\}.$$

Como los automorfismos de K están totalmente definidos por sus valores sobre a , resulta, entonces, que $\varphi^n(a) = a^{p^n}$, por lo que $\circ(\varphi) = m$. Vamos a mostrar ahora que todo automorfismo $\psi \in \text{Aut}(K)$ es de la forma φ^n , para algún $n \in \mathbb{N}$. Supongamos que $\psi(a) \in M$, por ejemplo $\psi(a) = a^{p^\mu}$, entonces $\psi = \varphi^\mu$. Vamos a mostrar que, en efecto, para cualquier automorfismo $\psi \in \text{Aut}(K)$, $\psi(a) \in M$.

Consideremos el polinomio

$$P := \prod_{\mu=0}^{m-1} (X - a^{p^\mu}),$$

cuyas raíces son exactamente los elementos de M . Si mostramos que $\psi(a)$ es una raíz de P , estamos listos. Desarrollando el producto, obtenemos para P la representación

$$P = \sum_{\mu=0}^m a_\mu X^\mu,$$

donde $a_\mu \in K$. Vamos a mostrar que incluso $a_\mu \in \kappa_p$, el campo primo de K . A tal efecto, consideremos el homomorfismo

$$\varphi_* : K[X] \rightarrow K[X],$$

inducido por φ . entonces

$$(11.30) \quad \varphi_*(P) = \prod_{\mu=0}^{m-1} \varphi(X - a^{p^\mu}) = \prod_{\mu=0}^{m-1} (X - a^{p^{\mu+1}}) = P,$$

ya que $a^{p^m} = a = a^{p^0}$. Por otra parte tenemos también

$$(11.31) \quad \varphi(P) = \sum_{\mu=0}^m \varphi(a_\mu) X^\mu.$$

Entonces de (11.30) y de (11.31), se obtiene que $a_\mu^p = a_\mu$, por lo que los coeficientes a_μ son raíces del polinomio $X^p - X$ y, por consiguiente, están en el campo primo κ_p . Entonces, tomando en cuenta que los elementos del campo primo permanecen invariantes bajo cualquier automorfismo, (ver ejercicio 11.3.3, 5), obtenemos

$$P(\psi(a)) = \sum_{\mu=0}^m a_\mu \psi(a)^\mu = \psi\left(\sum_{\mu=0}^m a_\mu a^\mu\right) = \psi(P(a)) = 0,$$

ya que $P(a) = 0$. Lo que muestra el teorema. \square

Si $P \in A[X]$, donde A es un dominio entero, es un polinomio irreducible en $A[X]$, de grado mayor o igual a 1, surge la pregunta si existe un campo K que contiene al anillo A , tal que P posea una raíz en K . La respuesta nos la da el siguiente

TEOREMA 11.35. *Sea A un dominio entero y $P \in A[X]$ un polinomio irreducible . Entonces existe un campo K , que contiene al anillo A , tal que P posee una raíz en K .*

DEMOSTRACIÓN. Sea $\mathbb{Q}(A)$ el campo de fracciones de A y consideremos a P como un polinomio en $\mathbb{Q}(A)[X]$. Si P posee una raíz en $\mathbb{Q}(A)$ estamos listos. Si P no posee raíces en $\mathbb{Q}(A)$, podemos suponer que P es irreducible en $\mathbb{Q}(A)[X]$, (caso contrario tomamos un factor irreducible de P en $\mathbb{Q}(A)[X]$). Como $\mathbb{Q}(A)$ es un campo, el anillo $\mathbb{Q}(A)[X]$ es principal y (P) es un ideal maximal, por lo que $K := \mathbb{Q}(A)[X]/(P)$ es un campo que contiene a $\mathbb{Q}(A)$ y por consiguiente a A . Si ξ es la clase de equivalencia de X en K , y

$$\pi : \mathbb{Q}(A)[X] \rightarrow K$$

la proyección canónica, entonces $0 = \pi(P) = P(\xi) \in K$. Por lo tanto $\xi \in K$ es una raíz de P . \square

El teorema 11.35 constituye la base para la teoría de extensión de campos y nos asegura que siempre podremos encontrar un campo K en el cual un polinomio dado posea, al menos, una raíz. La filosofía es, dado un polinomio cualquiera, encontrar un campo L en el cual P se descomponga en factores lineales. Como veremos en el teorema 11.36, dicho campo existe.

Los siguientes ejemplos nos aclaran la idea.

EJEMPLOS 11.8.

1. Sea $\kappa := \mathbb{Q}$ y consideremos el polinomio $P := X^2 - 2 \in \mathbb{Q}[X]$. P es irreducible en $\mathbb{Q}[X]$. En efecto si P fuera reducible en $\mathbb{Q}[X]$, existirían $a_1, a_2 \in \mathbb{Q}$, tales que

$$P = (X - a_1)(X - a_2), \quad a_1^2 = a_2^2 = 2.$$

Supongamos que $a_1 \in \mathbb{Q}$, entonces existirían números enteros p, q , primos entre sí, tales que $a_1 = \frac{p}{q}$ y de $2 = \frac{p^2}{q^2}$ resultaría $p^2 = 2q^2$, es decir p^2 y por consiguiente p serían números pares. Sea $p := 2p_1$, entonces $p^2 = 4p_1^2 = 2q^2$, lo que implicaría $q^2 = 2p_1^2$ y q sería igualmente un número par, en contradicción a que p, q no poseen divisores en común. Por teorema 11.35, P posee entonces una raíz ξ en el campo $\mathbb{Q}[X]/(P)$, donde $\xi^2 = 2$. La raíz ξ la denotaremos por $\sqrt{2}$. Con ξ también $-\xi \in \mathbb{Q}[X]/(P)$ es una raíz de P . Es decir que P se descompone en $\mathbb{Q}[X]/(P)$ en factores lineales.

2. Sea $P := aX^2 + bX + c$, $a, b, c \in \mathbb{Q}$, $a \neq 0$. Si ξ es una raíz de P en algún campo K que contiene a \mathbb{Q} , también será raíz del polinomio $P_1 := X^2 + b_1X + c_1$, donde $b_1 := \frac{b}{a}$ y $c_1 := \frac{c}{a}$, por lo que podemos fijar nuestra atención al polinomio mónico P_1 . Vamos a analizar, entonces, la reducibilidad del polinomio mónico $P := X^2 + bX + c$. Si ξ es una raíz de P en un campo K , entonces

$$\xi^2 + b\xi + c = 0 \quad \text{en } K.$$

y podemos escribir

$$(\xi^2 + b\xi + \frac{b^2}{4}) = \frac{b^2}{4} - c,$$

de donde

$$(11.32) \quad (\xi + \frac{b}{2})^2 = \frac{b^2 - 4c}{4} = \frac{\Delta}{4}, \quad \text{donde } \Delta := b^2 - 4c.$$

Δ se llama el *discriminante* del polinomio P . Si $\eta := \xi + \frac{b}{2}$, entonces de (11.32) obtenemos

$$(11.33) \quad \eta^2 = \frac{\Delta}{4}$$

Si $\Delta = 0$, entonces $-\frac{b}{2} \in \mathbb{Q}$ es una raíz de orden 2 de P y P es reducible en $\mathbb{Q}[X]$.

Si $\Delta > 0$ y $\Delta = \Delta_1^2$, $\Delta_1 \in \mathbb{Q}$, entonces P es reducible en $\mathbb{Q}[X]$. Si no existe un racional Δ_1 , tal que $\Delta = \Delta_1^2$, entonces P posee sus raíces en $K := \mathbb{Q}[X]/(P) \neq \mathbb{Q}$, donde $K \subseteq \mathbb{R}$. De (11.33) obtenemos para η

$$\eta = \frac{\sqrt{\Delta}}{2}$$

y con η , también $-\eta$ satisface (11.33). Entonces, en K , P posee las raíces

$$\xi_1 := -\frac{b}{2} + \frac{\sqrt{\Delta}}{2}, \quad \xi_2 := -\frac{b}{2} - \frac{\sqrt{\Delta}}{2}$$

y P se descompone en K en los factores

$$P = (X - \xi_1)(X - \xi_2) = \left(X + \frac{b}{2} - \frac{\sqrt{\Delta}}{2}\right)\left(X + \frac{b}{2} + \frac{\sqrt{\Delta}}{2}\right).$$

Si $\Delta < 0$, entonces $\eta^2 = \Delta = -\Delta_1$, donde $\Delta_1 > 0$, entonces P es irreducible en \mathbb{R}

3. Sea $P := X^3 - 3$. P es irreducible en $\mathbb{Q}[X]$. Si P tuviera una raíz en \mathbb{Q} , entonces existirían enteros p, q primos relativos, tales que $3 = \frac{p^3}{q^3}$, de donde $p^3 = 3q^3$. Como p, q son primos relativos, existen enteros a, b , tales que

$$1 = ap + bq, \quad \text{de donde } p^2 = ap^3 + bp^2q = 3aq^3 + bp^2q.$$

Entonces tendríamos que $q | p^2$ y $p^2 = qp_1, p_1 \in \mathbb{Z}$, por lo que

$$p = ap^2 + bqp = aqp_1 + bqp$$

lo que implicaría que $q | p$, en contradicción a que p, q son primos relativos.

Entonces P posee una raíz ξ en $K := \mathbb{Q}[X]/(P) \subseteq \mathbb{R}$, donde ξ es la clase de X ($\text{mód } (P)$), $\xi^3 = 3$. Denotaremos $\sqrt[3]{3} := \xi$. Entonces, en K , P se descompone en

$$P = (X - \sqrt[3]{3})(X^2 + \sqrt[3]{3}X + (\sqrt[3]{3})^2),$$

donde el polinomio

$$G := X^2 + \sqrt[3]{3}X + (\sqrt[3]{3})^2$$

es irreducible en \mathbb{R} , ya que $\Delta = (\sqrt[3]{3})^2 - 4(\sqrt[3]{3})^2 = -3(\sqrt[3]{3})^2 < 0$.

Por aplicaciones sucesivas del teorema 11.35 se obtiene el siguiente

TEOREMA 11.36. *Sea $P \in A[X]$, donde A es un dominio entero, un polinomio irreducible en $A[X]$, entonces existe un campo K que contiene al anillo A , tal que el polinomio P se descompone en $K[X]$ en factores lineales. (Ver teorema 12.14)*

El campo más pequeño K_P , tal que P se descompone en factores lineales, se llama el *campo de descomposición* del polinomio P .

11.3.3. Ejercicios y Complementos.

1. Mostrar que los polinomios

$$P := X^2 + 6X + 9, \quad Q := X^3 + X^2 - 9X - 9,$$

poseen una descomposición en factores lineales en $\mathbb{Z}[X]$, mientras que el polinomio

$$H := 2X^2 - 3X^2 - 2X + 3,$$

no posee una descomposición en factores lineales en $\mathbb{Z}[X]$, sin embargo sí se descompone en factores lineales en $\mathbb{Q}[X]$. Dar dicha descomposición

2. Si p es un número primo, mostrar que los coeficientes binomiales

$$\binom{p}{v}, \quad 0 \leq v \leq p, \quad \binom{p^m}{v}, \quad 0 \leq v \leq p^m, m \in \mathbb{Z}^+,$$

son múltiplos de p , salvo para $v = 0$ y $v = p$. Deducir de ésto que en un campo de característica p

$$(x + y)^{p^m} = x^{p^m} + y^{p^m}, \quad \forall m \in \mathbb{Z}^+.$$

3. Mostrar que si p es un número primo, entonces el único endomorfismo de campos

$$\varphi : \mathbb{Z}_p \rightarrow \mathbb{Z}_p$$

es la identidad.

4. Mostrar que si

$$\varphi : K \rightarrow K'$$

es un homomorfismo de campos de característica $p \neq 0$, entonces φ mapea al campo primo κ_p sobre el campo primo κ'_p y que la restricción

$$\varphi|_{\kappa_p} : \kappa_p \rightarrow \kappa'_p$$

es un isomorfismo de campos.

5. Sea K un campo de característica $p \neq 0$. Mostrar que la restricción de todo endomorfismo

$$\varphi : K \rightarrow K$$

sobre el campo primo κ_p es la identidad. Es decir que los elementos de κ_p permanecen invariantes bajo cualquier endomorfismo del campo K . (Ayuda: utilizar el hecho que κ_p es isomorfo a \mathbb{Z}_p y aplicar ejercicio 3).

6. Dar detalles de la demostración del teorema 11.36.

7. Dar el campo de descomposición del polinomio $P := X^3 - 3$

8. Dar el campo de descomposición del polinomio $P := X^2 + 1 \in \mathbb{Q}[X]$. Si ξ es la clase de X (mód (P)), en $K := \mathbb{Q}[X]/(P)$, mostrar que $\xi^2 = -1$ y que ξ genera un subgrupo multiplicativo, cíclico de K , de orden 4. Si

$$\mathbb{Q}[i] := \{z \in \mathbb{C} \mid z = a + bi, a, b \in \mathbb{Q}\},$$

mostrar que K es isomorfo a $\mathbb{Q}[i]$

9. Si $K := \mathbb{R}[X]/(X^2 + 1)$, mostrar que todo elemento de K es de la forma $a + b\xi$, $a, b \in \mathbb{R}$ y que el homomorfismo

$$\psi : \mathbb{R}[X] \rightarrow \mathbb{C},$$

definido por $\psi(P) := P(i)$, induce un isomorfismo entre K y \mathbb{C} .

11.3.4. Multiplicidad, Derivación y Polinomio Derivada. En esta subsección definiremos el llamado *polinomio derivada*, en analogía a la derivada de una función polinómica sobre el campo de los números reales. Sin embargo, advertimos al lector, que la definición de polinomio derivada introducida aquí, no tiene nada que ver con un proceso de límite ni con la continuidad de funciones, y que es compatible para polinomios sobre cualquier campo K .

Empezaremos mostrando que la multiplicidad de una raíz u orden de un polinomio dado $P \in A[X]$, donde A es un anillo comutativo con unidad, es independiente del anillo en el cual se encuentre dicha raíz.

TEOREMA 11.37. *Sea A un anillo y $a \in A$ una raíz, de multiplicidad n , del polinomio $P \in A[X] \setminus \{0\}$. Si \tilde{A} es un anillo que contiene a A y posee el mismo elemento unidad, entonces a , como elemento de \tilde{A} es también raíz de multiplicidad n , del polinomio $P \in \tilde{A}[X]$.*

DEMOSTRACIÓN. Por hipótesis

$$P = (X - a)^n G, \quad \text{donde} \quad G \in A[X],$$

y a no es raíz de G . Supongamos que en $\tilde{A}[X]$ existe un polinomio \tilde{G} , tal que

$$P = (X - a)^{n+1} \tilde{G},$$

entonces substrayendo ambas representaciones obtenemos

$$0 = (X - a)^n (G - (X - a)\tilde{G}),$$

donde el polinomio mónico $(X - a)^n$ no es un divisor de 0, por lo que $G = (X - a)\tilde{G}$, en contradicción a que a no es raíz de G . \square

Sea M una A -álgebra, decimos que una aplicación

$$D : M \rightarrow M$$

es una *derivada* o *derivación* sobre M , si

- a) D es una aplicación lineal.
- b) $\forall x, y \in M, D(xy) = D(x)y + xD(y)$.

En el caso particular en que $M := A$, D es una derivación sobre el anillo A .

TEOREMA 11.38. *Sea A un anillo conmutativo con unidad, $A[X]$ el anillo de polinomios correspondiente. Dado un polinomio $P \in A[X]$*

$$P := \sum_{v=0}^n a_v X^v,$$

y D la aplicación

$$D : A[X] \rightarrow A[X],$$

definida por medio de $D(P) := P'$, donde

$$P' := \sum_{v=1}^n a_v v X^{v-1}.$$

Entonces D posee las siguientes propiedades:

1. $D : A[X] \rightarrow A[X]$ es una aplicación lineal de A -módulos.
2. $D(PG) = D(P)G + PD(G) = P'G + PG'$.
3. $D(P^n) = nP^{n-1}D(P) = nP^{n-1}P'$.

Es decir D es una derivación sobre $A[X]$.

DEMOSTRACIÓN.

1. Debemos mostrar que $D(P + G) = D(P) + D(G)$ y que $D(aP) = aD(P)$, $\forall P, G \in A[X], a \in A$. Si n es el mayor grado entre los polinomios P y G , entonces, haciendo 0 los coeficientes que no aparecen en alguno de los dos polinomios, podemos escribir:

$$P := \sum_{v=0}^n a_v X^v, \quad G := \sum_{v=0}^n b_v X^v, \quad P + G = \sum_{v=0}^n (a_v + b_v) X^v.$$

Entonces

$$D(P + G) = \sum_{v=1}^n v(a_v + b_v) X^{v-1} = \sum_{v=1}^n v a_v X^v + \sum_{v=1}^n v b_v X^v = D(P) + D(G).$$

Y

$$D(aP) = D\left(a \sum_{v=0}^n a_v X^v\right) = D\left(\sum_{v=0}^n a a_v X^v\right) = \sum_{v=1}^n v a a_v X^{v-1} = a \sum_{v=1}^n v a_v X^{v-1} = a D(P).$$

2. Mostremos primero que la propiedad vale para

$$P := X^m, \quad G := G := \sum_{v=0}^n b_v X^v.$$

Entonces

$$\begin{aligned} D(PG) &= D\left(X^m \sum_{v=0}^n b_v X^v\right) = D\left(\sum_{v=0}^n b_v X^{v+m}\right) = \sum_{v=0}^n (v+m)b_v X^{v+m-1} \\ &= mX^{m-1} \sum_{v=0}^n b_v X^v + X^m \sum_{v=0}^n v b_v X^{v-1} = D(P)G + PD(G). \end{aligned}$$

Procedamos ahora por inducción sobre el grado de P . Para $\text{grad } P = 0$, la propiedad resulta de la linealidad de D . Supongamos que la propiedad se cumple para todo polinomio de grado menor a $m = \text{grad } P$. Entonces podemos escribir

$$P = a_m X^m + P_1, \quad \text{grad } P_1 < m.$$

Entonces

$$PG = a_m X^m G + P_1 G$$

y

$$D(PG) = D(a_m X^m G) + D(P_1 G) = a_m D(X^{m-1})G + a_m X^m D(G) + D(P_1 G).$$

Por hipótesis de inducción se tiene que

$$D(P_1 G) = D(P_1)G + P_1 D(G),$$

entonces

$$\begin{aligned} D(PG) &= a_m D(X^{m-1})G + a_m X^m D(G) + D(P_1)G + P_1 D(G) \\ &= D(a_m X^{m-1})G + a_m X^m D(G) + D(P_1)G + P_1 D(G) \\ &= (a_m X^{m-1} + D(P_1))G + (a_m X^m + P_1)D(G) \\ &= D(P)G + PD(G). \end{aligned}$$

3. Resulta, por inducción sobre n , de aplicar 2 a P y $G := P^{n-1}$.

□

El polinomio derivada nos da una herramienta muy útil para determinar la multiplicidad de una raíz de un polinomio, como se muestra en el siguiente

TEOREMA 11.39. *Sea A un anillo y $P \in A[X] \setminus \{0\}$. Si $a \in A$ es una raíz de P de orden $n \geq 2$, entonces $P' = 0$ o a es una raíz de P' de orden $j \geq n-1$; si $n \cdot 1 \in A$ no es un divisor de 0 en A , entonces, con toda certeza $j = n-1$. Un elemento $a \in A$ es una raíz simple del polinomio P , Ssi $P(a) = 0$ y $P'(a) \neq 0$.*

DEMOSTRACIÓN. Si a es una raíz de orden $n \geq 2$ de P , entonces podemos escribir

$$P = (X - a)^n G, \quad G \in A[X], \quad G(a) \neq 0, \quad \text{y} \quad P' = n(X - a)^{n-1} G + (X - a)^n G',$$

de donde

$$P' = (X - a)^{n-1} (nG + (X - a)G') = (X - a)^{n-1} \tilde{G}, \quad \tilde{G} := nG + (X - a)G'.$$

Entonces, $P' = 0$, o a es una raíz de P' , de orden $j \geq n-1$. $j = n-1$ Ssi $\tilde{G}(a) \neq 0$. $\tilde{G}(a) \neq 0$ Ssi $(n \cdot 1)G(a) \neq 0$, lo cual sucede con toda certeza si $n \cdot 1$ no es divisor de 0 en A .

Por otra parte, si a es una raíz simple de P , entonces

$$P = (X - a)G, \quad G \in A[X], \quad G(a) \neq 0, \quad P' = G + (X - a)G',$$

de modo que $P'(a) = G(a) \neq 0$. Por otra parte si $P(a) = 0$ y $P'(a) \neq 0$, entonces, por la primera parte del teorema, a no puede ser una raíz de orden ≥ 2 de P , por lo que a debe ser una raíz simple de P . \square

Si K es un campo de característica $p \neq 0$ y κ_p el campo primo correspondiente y $P = X^{p^m} - X \in \kappa_p[X]$, entonces

$$P' = p^m X^{p^m-1} - 1 = -1.$$

Entonces $P'(x) = 1 \neq 0, \forall x \in K$. Con esto hemos demostrado el siguiente resultado

TEOREMA 11.40. *Sea K un campo de característica $p \neq 0$, κ_p el campo primo correspondiente. Entonces todas las raíces en K , del polinomio $P := X^{p^m} - X$ son simples.*

Como consecuencia inmediata del teorema 11.40 se obtiene el siguiente resultado de gran importancia en la teoría de los campos finitos:

TEOREMA 11.41. *Para cada número primo p y para cada entero positivo m , existe un campo κ con, exactamente, p^m elementos,*

Otra consecuencia del teorema 11.39 es el siguiente

TEOREMA 11.42. *Si P es un polinomio irreducible en $\kappa[X]$, donde κ es un campo cualquiera, si $P' \neq 0$, entonces en cualquier otro campo K , que contenga al campo κ , P sólamente podrá tener raíces simples.*

DEMOSTRACIÓN. Supongamos que K sea un campo que contiene al campo κ , tal que $a \in K$ es una raíz múltiple de P . Como $P' \neq 0$, entonces existe el máximo común divisor $D \in \kappa[X]$ de p, P' . Como $\kappa[X]$ es un anillo principal, entonces existen polinomios $G, H \in \kappa[X]$, tales que $D = GP + HP'$. Siendo a una raíz múltiple de P , entonces, por teorema 11.39, a es también raíz de P' y por consiguiente raíz de $D = GP + HP'$. Como $D \neq 0$, se debe tener $\text{grad } D > 0$. Por otra parte se tiene

$$0 < \text{grad } D \leq \text{grad } P' < \text{grad } P,$$

ya que $D \mid P'$. Pero si $0 < \text{grad } D < \text{grad } P$, entonces D sería un divisor propio de P en $\kappa[X]$, en contradicción a que P es irreducible en $\kappa[X]$. Por lo tanto $a \in K$, debe ser una raíz simple de P . \square

Ilustremos estos resultados con el siguiente ejemplo concreto:

EJEMPLO 11.9. Sea $p := 2, m := 2$, entonces el campo finito de característica $p = 2$, que contiene a $\kappa_p := \mathbb{Z}_2$, y posee $2^2 = 4$ elementos consta de las raíces del polinomio $P := X^4 - X \in \kappa_p[X]$, que son todas simples, ya que $P' = -1 = 1$.

$$P = X(X^3 - 1) = X(X - 1)(X^2 + X + 1)$$

Las raíces 0, 1 están en \mathbb{Z}_2 , sin embargo, el polinomio $G := X_2 + X + 1$, no posee raíces en \mathbb{Z}_2 , por lo que G es irreducible en $\mathbb{Z}[X]$, pero sí en el campo $K := \mathbb{Z}_2[X]/(G)$. Si ξ es la clase de X en K , entonces, teniendo en cuenta que en κ_p , $1 = -1$, tenemos que ξ es un elemento que debe satisfacer:

$$(11.34) \quad \xi^2 = \xi + 1$$

y por teorema 11.31, ξ genera el subgrupo multiplicativo K^* de K y debe ser un elemento de orden 3, entonces, el campo buscado es, en este caso $K := \{0, 1, \xi, \xi + 1\}$.

En un campo κ de característica 0, como $\text{grad } P' = \text{grad } P - 1$, entonces $P' = 0$. Si $P \in \kappa$. Entonces un polinomio P , con $\text{grad } P \geq 1$, irreducible en $\kappa[X]$, sólo puede poseer raíces simples en cualquier campo K que contenga a κ .

Para campos de característica $p \neq 0$, la situación es diferente, como lo muestra el siguiente

TEOREMA 11.43. *En un campo κ de característica $p \neq 0$, $P' = 0$, Ssi P es un polinomio en X^p , es decir P posee una representación de la forma*

$$(11.35) \quad P = \sum_{\mu=0}^m a_{p^\mu} X^{p^\mu}, \quad a_{p^\mu} \in \kappa.$$

DEMOSTRACIÓN. Si P es de la forma (11.35), entonces todos los coeficientes de P' son múltiplos de p y por consiguiente iguales a 0 en κ , por lo que $P' = 0$. Supongamos ahora que $P' = 0$. Si

$$P := \sum_{\lambda=0}^l b_\lambda X^\lambda \quad \text{y} \quad P' = \sum_{\lambda=0}^l \lambda b_\lambda X^{\lambda-1} = 0,$$

entonces $\lambda b_\lambda = 0$, $\forall \lambda \geq 0$, lo que implica que, para $p \nmid \lambda$, $b_\lambda = 0$. Por consiguiente P debe ser un polinomio en X^p . \square

Ahora surge la pregunta ¿Qué pasa con las raíces de un polinomio P , en un campo de característica $p \neq 0$, cuando $P' = 0$? La respuesta nos la da el siguiente

TEOREMA 11.44. *Sea P un polinomio irreducible en $\kappa[X]$, donde κ es un campo de característica $p \neq 0$. Sea $P' = 0$ y $r \in \mathbb{Z}^+$, tal que P es un polinomio en X^{p^r} , pero no en $X^{p^{r+1}}$. Entonces toda raíz de P , en cualquier campo K que contenga a κ , es de multiplicidad p^r .*

DEMOSTRACIÓN. Como P es un polinomio irreducible, $\text{grad } P > 0$. Entonces, como $P' = 0$, por teorema 11.43, P es un polinomio en X^p . Sea $r \in \mathbb{Z}^+$, tal que P es polinomio en X^{p^r} , pero no en $X^{p^{r+1}}$, entonces existe un polinomio $G \in \kappa[Y]$, tal que $P = G(X^{p^r})$, en donde la aplicación

$$\Phi_{X^{p^r}} : \kappa[Y] \rightarrow \kappa[X],$$

definida por $\Phi_{X^{p^r}}(G) := G(X^{p^r})$, es un homomorfismo de anillos. Entonces G es también irreducible en $\kappa[Y]$. G no es un polinomio en Y^p , pues de lo contrario P sería un polinomio en $X^{p^{r+1}}$.

Supongamos ahora que $a \in K$, donde K es un campo que contiene a κ , es una raíz de P . Por teorema 11.36, existe un campo L_1 que contiene al campo K , tal que el polinomio $G \in \kappa[Y]$, se descompone en factores lineales

$$G = b(Y - b_1)(Y - b_2) \cdots (Y - b_m), \quad b, b_1, \dots, b_m \in L_1.$$

Como G no es un polinomio en Y^p , $G' \neq 0$ y por teorema 11.40, todas las raíces de G son simples. Substituyendo Y por X^{p^r} , obtenemos

$$P = b(X^{p^r} - b_1) \cdots (X^{p^r} - b_m)$$

en L_1 . Nuevamente, por teorema 11.40, podemos encontrar un campo L que contiene al campo L_1 , en el cual cada uno de los polinomios $X^{p^r} - b_\mu$ posee una raíz a_μ , $\mu = 1, \dots, m$. Como

$$a_\mu^{p^r} = b_\mu$$

se obtiene

$$X^{p^r} - b_\mu = X^{p^r} - a_\mu^{p^r} = (X - a_\mu)^{p^r}$$

y por consiguiente

$$P = b(X - a_1)^{p^r} \cdots (X - a_m)^{p^r}$$

en $L[X]$. Como los b_μ son todos diferentes, también los a_μ son todos diferentes, por lo que cada a_μ es una raíz de orden p^r . Como $a \in K \subseteq L$, a debe coincidir con una de las raíces a_μ y por consiguiente es de orden p^r . \square

Al grado m del polinomio $G \in \kappa[Y]$, tal que $P = G(X^{p^r})$, se le llama el *grado reducido* de P .

EJEMPLOS 11.10.

1. Sea p un número primo, κ un campo de característica p y $r := 2$, $P := a_0 + a_1X^{p^2} + a_2X^{2p^2} + a_3X^{3p^2}$, $a_\nu \in \kappa$, entonces $G = a_0 + a_1Y + a_2Y^2 + a_3Y^3$ es el polinomio en $\kappa[Y]$, tal que $P = G(X^{p^2})$. $m = 3$ es el grado reducido de P
2. Sea $p := 3$, $\kappa := \mathbb{Z}_3$ y $P := 1 + X^3 + X^6 + 2X^9 + X^{12}$, entonces P es un polinomio en X^3 , $G := 1 + Y + Y^2 + 2Y^3 + Y^4$, es el polinomio en $\kappa[Y]$, tal que $G(X^3) = P$. $m = 4$ es el grado reducido de P .
3. Sea $p := 2$, $\kappa := \mathbb{Z}_2$ y $P := 1 + X^4 + X^8 + X^{12} + X^{16}$. Entonces P es un polinomio en $X^4 = X^{2^2}$, con $r := 2$ y $G := 1 + Y + Y^2 + Y^3 + Y^4$. $m := 4$ es el grado reducido de P .

Sea κ un campo. Decimos que un polinomio irreducible $P \in \kappa[X]$ es *separable sobre* κ , si $P' \neq 0$. Decimos que un polinomio cualquiera $G \in \kappa[X]$ es separable sobre κ , si $G \neq 0$, $\text{grad } G > 0$ y cada factor irreducible de G es separable. Un polinomio que no es separable se dice que es *inseparable*.

En particular en un campo κ de característica 0 todo polinomio en $\kappa[X]$ es separable.

El concepto de separabilidad está inspirado en el hecho de que todas las raíces de un polinomio irreducible, cuyo polinomio derivada no es el polinomio cero, son simples, tal como se vió en el teorema 11.42.

Decimos que un campo κ es *perfecto*, si todo polinomio de grado positivo es separable sobre κ .

Por lo anteriormente demostrado, todo campo de característica 0 es perfecto.

Sin embargo, también los campos de característica $p \neq 0$ pueden ser perfectos. Un criterio necesario y suficiente para la perfección de un campo de característica $p \neq 0$, nos lo da el siguiente

TEOREMA 11.45. *Un campo κ de característica $p \neq 0$ es perfecto, Ssi el homomorfismo*

$$\varphi : \kappa \rightarrow \kappa,$$

donde $\varphi(x) := x^p$ es un automorfismo.

DEMOSTRACIÓN. Supongamos que φ es un automorfismo y sea

$$P := \sum_{\nu=0}^n a_{p\nu} X^{p\nu}, \quad a_{p\nu} \in \kappa,$$

un polinomio en X^p , de grado positivo. Por hipótesis, para cada ν , $0 \leq \nu \leq n$, existe $b_\nu \in \kappa$, tal que $b_\nu^p = a_{p\nu}$, por lo que podemos escribir

$$P = \sum_{\nu=0}^n b_\nu^p X^{p\nu} = \left(\sum_{\nu=0}^n b_\nu X^\nu \right)^p.$$

Esto quiere decir, que los polinomios en X^p sobre κ no son irreducibles y la derivada de cada factor de la forma

$$\sum_{v=0}^n b_v X^v$$

es distinta de 0. Por consiguiente P es separable y κ es un campo perfecto.

Supongamos ahora que κ sea un campo perfecto. Vamos a mostrar que φ debe ser un automorfismo. Como φ es un homomorfismo de campos φ es siempre inyectivo. Si φ no fuera un automorfismo, entonces φ no sería sobreyectiva y existiría $a \in \kappa$, tal que el polinomio

$$P := X^p - a$$

no posee raíces en κ . Sea K un campo que contiene a κ , tal que P posee una raíz $b \in K$, entonces

$$P = X^p - b^p = (X - b)^p.$$

Sea G un factor irreducible y mónico de P en $\kappa[X]$. Como G es también factor de P en $K[X]$, G posee una representación en $K[X]$ como

$$G = (X - b)^m, \quad m \geq 2,$$

pues, si $m = 1$, implicaría $b \in \kappa$, lo cual no podría ser. Entonces b sería una raíz múltiple, de orden m , del polinomio G , irreducible en $\kappa[X]$, en contradicción a que κ es perfecto. Por consiguiente φ debe ser sobreyectiva y por consiguiente un automorfismo. \square

De los teoremas 11.34 y 11.45, se obtiene de forma inmediata el siguiente resultado:

COROLARIO 11.46. *Todo campo finito es perfecto. En particular el campo primo κ_p de un campo K de característica p es perfecto.*

11.3.5. Ejercicios y Complementos.

1. En los siguientes incisos determinar si el polinomio dado es un polinomio en X^{p^r} , para algún primo p . Dado el caso determinar r , el polinomio $G \in \kappa[Y]$, tal que $P = G(X^{p^r})$ y el grado reducido de P .
 - a) $P := 1 + X^4 + X^8 + X^{12} + X^{16}$.
 - b) $P := 2 + X^3 + 2X^6 + 2X^9 + X^{12} + 2X^{15}$.
 - c) $P := 1 + X^9 + 2X^{18} + X^{27}$.
2. Sea $P := X^4 - 7X^3 + 18X^2 - 20X + 8$.
 - a) Mostrar que 1, 2 son raíces de P en $\mathbb{Z}[X]$.
 - b) Usando el criterio del polinomio derivada, determinar los ordenes de las raíces 1, 2.
 - c) Dar la descomposición de P en factores lineales. ¿Existen otras raíces de P en algún campo que contenga a \mathbb{Z} ?
3. Sea A un dominio entero, $a \in A$ y $P \in A[X]$. Mostrar que el ideal $\alpha := (P, a)$ es igual a $A[X]$. Si $P(a)$ es un elemento invertible en A .
4. Sean κ un campo y $P, G \in \kappa[X]$, donde P es un polinomio irreducible en $\kappa[X]$. Si existe un campo K contenido en κ , tal que P, G poseen en K , una raíz en común, entonces $P \mid G$ en $\kappa[X]$.
5. Encontrar el campo K de característica $p := 3$, con $p^2 = 9$ elementos, que consta de todas las raíces del polinomio $P := X^9 - X \in \kappa_3[X]$. (Ayuda: Descomponer P en factores irreducibles, teniendo en cuenta que en $\kappa_3 = \mathbb{Z}_3$, $-1 = 2$ y usar el hecho que el grupo K^* de todos los elementos invertibles de K es cíclico de orden 8, mostrando que $\xi := \sqrt[4]{2}$ genera todas las raíces, salvo 0, de P).

6. Sean κ un campo de característica $p \neq 0$ y $a \in \kappa$ un elemento que no puede ser representado en κ como p -potencia de algún elemento. Mostrar que $P := X^p - a$ es irreducible en $\kappa[X]$. (Ayuda: si el exponente $m \geq 2$ de la demostración de la segunda parte del teorema 11.45, fuese menor que p , entonces el coeficiente b utilizado, se representaría como producto de ciertas potencias de b^m y b^p y $b \in \kappa$, lo que sería una contradicción).
7. Sea κ el campo de fracciones del dominio entero $A := \mathbb{Z}_p[Y]$, donde p es un número primo. Mostrar que $P := X^p - Y$ es irreducible en $\kappa[X]$. κ es un ejemplo de un campo que no es perfecto.

11.4. Conjuntos Algebraicos y Topología de Zariski

Dado un polinomio cualquiera $P \in A[X_1, \dots, X_n]$, definimos

$$\mathfrak{V}_A(P) := \{\lambda \in A^n \mid P(\lambda) = 0\}.$$

Es decir que $\mathfrak{V}_A(P)$ es el conjunto de todas las raíces de P en A^n . Como vimos en los ejemplos anteriores $\mathfrak{V}_A(P)$ puede ser vacío. Al conjunto $\mathfrak{V}(P)$ lo llamamos el *conjunto algebraico* definido por el polinomio P .

Si $a \in A \setminus \{0\}$, entonces $\mathfrak{V}(a) = \emptyset$, ya que $\Phi_a(x) = a$, $\forall x \in A$. Si $P \in A[X_1, \dots, X_n]$ es el polinomio 0, entonces $\mathfrak{V}_A(0) = A^n$.

Si P es un polinomio reducible, $P = GH$, entonces $P(\lambda) = 0$, Ssi $G(\lambda) = 0$ o $H(\lambda) = 0$. Entonces si P no es irreducible y $P = GH$ se obtiene

$$\mathfrak{V}_A(P) = V(G) \cup V(H).$$

En general, si $A[X]$ es un anillo factorial y $P = P_1 \cdots P_m$ es una descomposición de P en factores irreducibles, entonces

$$\mathfrak{V}_A(P) = \bigcup_{v=1}^n \mathfrak{V}_A(P_v).$$

Si \mathfrak{a} es un ideal del anillo de polinomios $A[X_1, \dots, X_n]$, entonces definimos

$$\mathfrak{V}_A(\mathfrak{a}) := \{\lambda \in A^n \mid P(\lambda) = 0, \forall P \in \mathfrak{a}\}.$$

En particular, si $\mathfrak{a} := (P)$, entonces, como el lector comprobará, $\mathfrak{V}_A(P) = \mathfrak{V}_A(\mathfrak{a})$. También se comprueba fácilmente, que si $\mathfrak{a} := (P_1, \dots, P_m)$, entonces

$$(11.36) \quad \mathfrak{V}_A(\mathfrak{a}) = \bigcap_{\mu=1}^m \mathfrak{V}_A(P_\mu).$$

De hecho, por el teorema de la base de Hilbert 11.21 y el corolario 11.22, todo ideal de $A[X_1, \dots, X_n]$ es de esta forma, si A es un anillo noetheriano y en particular si A es un campo.

En la geometría algebraica a todo conjunto algebraico correspondiente a un ideal principal, se le llama una *hipersuperficie* de A^n . Entonces (11.36) nos dice que un conjunto algebraico correspondiente a un ideal cualquiera de $A[X_1, \dots, X_n]$ es intersección de, a lo sumo, un número finito de hipersuperficies de A^n .

\mathfrak{V}_A es una aplicación

$$\mathfrak{V}_A : \mathfrak{I}(A[X_1, \dots, X_n]) \rightarrow \mathcal{P}(A^n),$$

donde $\mathfrak{I}(A[X_1, \dots, X_n])$ es el conjunto de todos los ideales de $A[X_1, \dots, X_n]$.

De forma análoga se define una aplicación

$$\mathfrak{I} : \mathcal{P}(A^n) \rightarrow \mathfrak{I}(A[X_1, \dots, X_n]),$$

por

$$\mathfrak{J}(V) := \{P \in A[X_1, \dots, X_n] \mid P(\mathbf{x}) = 0 \ \forall \mathbf{x} \in V\}$$

$\mathfrak{J}(V)$ se llama el *ideal de anulación* del subconjunto $V \subseteq A^n$.

Para las aplicaciones $\mathfrak{J}, \mathfrak{B}_A$ se tienen las siguientes propiedades, que resumimos en el siguiente teorema cuando A es un campo K :

TEOREMA 11.47. *Sea K un campo, entonces las aplicaciones $\mathfrak{J}, \mathfrak{B}_K$ poseen las siguientes propiedades:*

1. $\mathfrak{J}(K^n) = (0)$, si K es de característica 0, y $\mathfrak{J}(\emptyset) = (1) = K[X_1, \dots, X_n]$.
2. $\mathfrak{a} \subseteq \mathfrak{b} \Rightarrow \mathfrak{B}_K(\mathfrak{b}) \subseteq \mathfrak{B}_K(\mathfrak{a})$.
3. *Dados dos subconjuntos $V, U \in K^n$, $V \subseteq U \Rightarrow \mathfrak{J}(U) \subseteq \mathfrak{J}(V)$.*
4. *Para todo $V \subseteq K^n$, $\mathfrak{J}(V) = r(\mathfrak{J}(V))$. Es decir $\mathfrak{J}(V)$ es un ideal radical.*
5. *Dado un conjunto algebraico $V := \mathfrak{B}_K(\mathfrak{a})$, $\mathfrak{B}_K(\mathfrak{J}(V)) = V$.*
6. *Dados dos conjuntos algebraicos U, V , se tiene $\mathfrak{J}(U \cup V) = \mathfrak{J}(U) \cap \mathfrak{J}(V)$ y $U \cup V = \mathfrak{B}_K(\mathfrak{J}(U) \cdot \mathfrak{J}(V))$*
7. *Dada una familia de conjuntos algebraicos $(V_i)_{i \in I}$*

$$\bigcap_{i \in I} V_i = \mathfrak{B}_K \left(\sum_{i \in I} \mathfrak{J}(V_i) \right).$$

DEMOSTRACIÓN.

1. Si K es finito de orden p^m , donde p es un número primo y $m \in \mathbb{Z}^+$, entonces $\mathfrak{J}(K) = (X^{p^m} - X)$. Si $\text{car } K = 0$, entonces K es un campo infinito. Si existiera un polinomio P , tal que para todo elemento $\mathbf{x} := (x_1, \dots, x_n) \in K^n$, $P(\mathbf{x}) = 0$, entonces x_n sería una raíz del polinomio $P(x_1, \dots, x_n, X_n) \in K[X_n]$, para todo $x_n \in K$, lo cual no es posible, ya que K es infinito. Por otra parte es obvio que $\mathfrak{J}(\emptyset) = K[X_1, \dots, X_n] = (1)$.
2. Si $\mathfrak{a} \subseteq \mathfrak{b}$, entonces es obvio que si \mathbf{x} es raíz de todo polinomio de \mathfrak{b} , también será raíz de todo polinomio de \mathfrak{a} , por consiguiente $\mathfrak{B}_K(\mathfrak{b}) \subseteq \mathfrak{B}_K(\mathfrak{a})$.
3. Si $P \in \mathfrak{J}(U)$, entonces P es un polinomio que se anula sobre U , como $V \subseteq U$, P se anula sobre V , por lo que $P \in \mathfrak{J}(V)$.
4. Sabemos que $\mathfrak{J}(V) \subseteq r(\mathfrak{J}(V))$. Sea $P \in r(\mathfrak{J}(V))$, entonces, existe un entero positivo n , tal que $P^n \in \mathfrak{J}(V)$ y $P^n(\mathbf{x}) = 0, \forall \mathbf{x} \in V$. Ahora bien

$$P^n(\mathbf{x}) = \underbrace{P(\mathbf{x}) \cdots P(\mathbf{x})}_n = 0 \Rightarrow P(\mathbf{x}) = 0,$$

ya que K no posee divisores de 0. Por lo tanto $P \in \mathfrak{J}(V)$ y la igualdad subsiste.

5. Por definición

$$\mathfrak{B}_K(\mathfrak{J}(V)) = \{\mathbf{x} \in K^n \mid P(\mathbf{x}) = 0, \forall P \in \mathfrak{J}(V)\}.$$

Si $\mathbf{x} \in V = \mathfrak{B}_K(\mathfrak{a})$ y $P \in \mathfrak{J}(V)$, entonces $P(\mathbf{x}) = 0$ y $\mathbf{x} \in \mathfrak{B}_K(\mathfrak{J}(V))$, por lo que $V \subseteq \mathfrak{B}_K(\mathfrak{J}(V))$. Por otra parte si $P \mathfrak{a}$, entonces por definición de V , P se anula sobre todo V , por lo que $P \in \mathfrak{J}(V)$ y $\mathfrak{a} \subseteq \mathfrak{J}(V)$, de donde, por inciso 2, $\mathfrak{B}_K(\mathfrak{J}(V)) \subseteq \mathfrak{B}_K(\mathfrak{a}) = V$. Por lo tanto $V = \mathfrak{B}_K(\mathfrak{J}(V))$.

6. $V \subseteq V \cup U$ y $U \subseteq V \cup U$ implica que $\mathfrak{J}(V \cup U) \subseteq \mathfrak{J}(V)$ y $\mathfrak{J}(V \cup U) \subseteq \mathfrak{J}(U)$, de donde resulta que $\mathfrak{J}(V \cup U) \subseteq \mathfrak{J}(V) \cap \mathfrak{J}(U)$. Por otra parte, si $P \in \mathfrak{J}(V) \cap \mathfrak{J}(U)$, entonces P se anula sobre U y sobre V , por consiguiente sobre $U \cup V$. Por lo tanto $\mathfrak{J}(V) \cap \mathfrak{J}(U) \subseteq \mathfrak{J}(V \cup U)$. Lo que muestra la primera igualdad. Para la segunda igualdad: de $V \subseteq V \cup U$ y $U \subseteq V \cup U$, se obtiene que $\mathfrak{J}(V) \cdot \mathfrak{J}(U) \subseteq \mathfrak{J}(V \cup U)$

y $\mathfrak{J}(V) \cdot \mathfrak{J}(U) \subseteq \mathfrak{J}(U)$, resulta que $V \cup U \subseteq \mathfrak{V}_K(\mathfrak{J}(V) \cdot \mathfrak{J}(U))$. Por otra parte si $\mathbf{x} \in \mathfrak{V}(\mathfrak{J}(V) \cdot \mathfrak{J}(U))$, entonces $P(\mathbf{x}) = 0$, $\forall P \in \mathfrak{J}(V) \cdot \mathfrak{J}(U)$. Por definición de producto de dos ideales, existen polinomios $G \in \mathfrak{J}(V)$ y $H \in \mathfrak{J}(U)$, tales que $P = GH$, entonces $P(\mathbf{x}) = 0$, Ssi $G(\mathbf{x}) = 0$ o $H(\mathbf{x}) = 0$, lo que implica que también $\mathfrak{V}_K(\mathfrak{J}(V) \cdot \mathfrak{J}(U)) \subseteq V \cup U$. Lo que muestra la segunda igualdad.

7. De

$$\mathfrak{J}(V_i) \subseteq \left(\sum_{i \in I} \mathfrak{J}(V_i) \right), \quad \forall i \in I,$$

se obtiene

$$\mathfrak{V}_K \left(\sum_{i \in I} \mathfrak{J}(V_i) \right) \subseteq V_i, \quad \forall i \in I.$$

lo que implica que

$$\mathfrak{V}_K \left(\sum_{i \in I} \mathfrak{J}(V_i) \right) \subseteq \bigcap_{i \in I} V_i.$$

por otra parte para $\mathbf{x} \in \bigcap_{i \in I} V_i$ y $P \in \sum_{i \in I} \mathfrak{J}(V_i)$, por definición de ideal suma, P es combinación lineal de polinomios P_i que anulan a V_i , por consiguiente $P(\mathbf{x}) = 0$ y $\mathbf{x} \in \mathfrak{V}_K \left(\sum_{i \in I} \mathfrak{J}(V_i) \right)$. Lo que muestra la igualdad.

□

El lector habrá notado la similitud que existe entre \mathfrak{V}_K y \mathfrak{J} definidos aquí y los definidos, en el caso abstracto, en la subsección 9.3.2. En el caso abstracto \mathfrak{J} es una biyección, entre los subconjuntos de $\text{Spec } A$ y los ideales radicales del anillo A , mientras que en el caso concreto, para un campo en general K , es, por los incisos 2 y 5, del teorema 11.47 una inyección entre los subconjuntos algebraicos de K^n y los ideales radicales de $K[X_1, \dots, X_n]$, pero no necesariamente sobreyectiva. En efecto, tomemos como ejemplo $K := \mathbb{R}$ y consideremos el polinomio primo $P := X^2 + 1 \in \mathbb{R}[X]$. $\mathfrak{V}_K(P) = \emptyset$, pero $\mathfrak{J}(\emptyset) = \mathbb{R}[X]$. Entonces el ideal radical (P) no es imagen de \mathfrak{J} .

Si \mathfrak{p} es un ideal primo en $K[X_1, \dots, X_n]$, entonces se dice también que $\mathfrak{V}_K(\mathfrak{p})$ es una K -variedad algebraica.

Dada una K -variedad $V := \mathfrak{V}_K(\mathfrak{p})$, donde \mathfrak{p} es un ideal primo de $K[X_1, \dots, X_n]$, en la geometría algebraica se la asigna a V la K -álgebra $A_K(V) := K[X_1, \dots, X_n]/\mathfrak{p}$, llamada la K -álgebra afín, de la variedad V y se estudia el espectro $\text{Spec } A_K(V)$. (Ver, por ejemplo, [7]).

11.4.1. Topología de Zariski. En la subsección 9.3.2, vimos como, con ayuda de los conjuntos algebraicos abstractos, podíamos definir una topología, la topología abstracta de Zariski, sobre el conjunto $\text{Spec } A$, para un anillo comutativo con unidad A . De igual forma el teorema 11.47, nos da la base para definir, por medio de los conjuntos algebraicos de K^n , una topología sobre K^n , llamada también la topología de Zariski.

Del teorema 11.47 se deducen, de forma inmediata, las siguientes propiedades para los conjuntos algebraicos, que resumiremos en el siguiente:

TEOREMA 11.48. *Dado un campo K , entonces*

- a) K y \emptyset son conjuntos algebraicos
- b) Si U, V son conjuntos algebraicos, entonces $U \cup V$ es un conjunto algebraico
- c) Dada una familia $(V_i)_{i \in I}$ de conjuntos algebraicos, entonces

$$V := \bigcap_{i \in I} V_i$$

es un conjunto algebraico.

El teorema 11.48 nos dice que los conjuntos algebraicos satisfacen las condiciones de los subconjuntos cerrados de una topología sobre K^n , ver, por ejemplo [8], llamada la *topología de Zariski de K^n* .

Para el caso en que K es el campo de los números reales \mathbb{R} o de los números complejos \mathbb{C} , los conjuntos algebraicos son todos los subconjuntos finitos de K , ya que son raíces de polinomios. Entonces la topología de Zariski sobre K coincide con la llamada topología cofinita, cuyos conjuntos abiertos son aquellos cuyos complementos son finitos. (Ver [8]).

A continuación ilustramos algunos ejemplos de hipersuperficies en \mathbb{R}^2 y en \mathbb{R}^3 .

La inconexidad de la curva ilustrada en la figura 11.6, es porque ningún punto $\mathbf{x} = (x, y) \in \mathbb{R}^2$, con x en el intervalo $(0, 1)$ puede ser raíz del polinomio $P := Y^2 - X^3 + X$.

Las figuras 11.5 y 11.6 representan hipersuperficies, o sea curvas planas, en el plano real \mathbb{R}^2 , mientras que las figuras 11.7 y 11.8 representan hipersuperficies en el espacio real \mathbb{R}^3 .

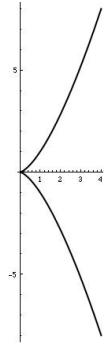


FIGURA 11.5. $X^3 - Y^2 = 0$

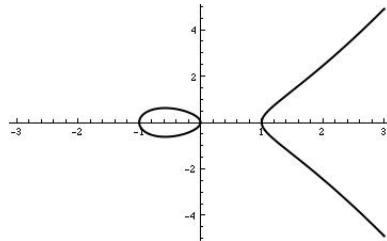
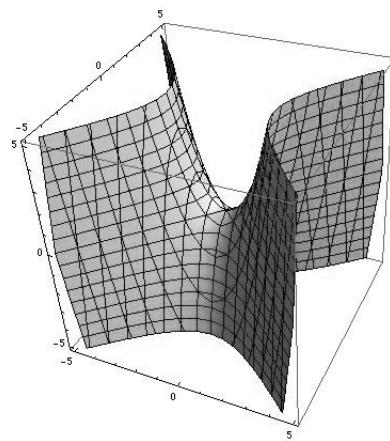
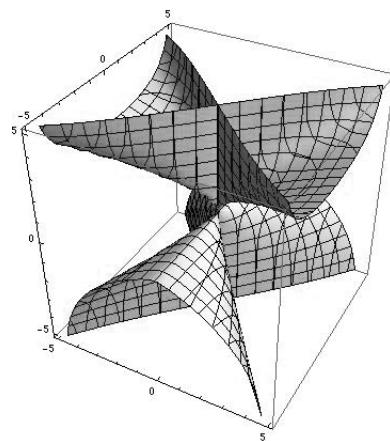


FIGURA 11.6. $Y^2 - X^3 + X = 0$

FIGURA 11.7. $X^2 - Y^2 - Z = 0$ FIGURA 11.8. $X^4 + (Y^2 - X^2Z^2) = 0$

CAPÍTULO 12

EXTENSIÓN DE CAMPOS Y TEORÍA DE GALOIS

En este capítulo estudiaremos exhaustivamente las extensiones de campos y sus propiedades fundamentales. Introduciremos los conceptos de extensión algebraica, extensión normal y extensión trascendental, así como el concepto de grado de una extensión. Para el caso de campos de característica $p \neq 0$ introduciremos el concepto de extensión separable y grado de separabilidad. Introduciremos también los conceptos de campo algebraicamente cerrado, elementos algebraicos y elementos trascendentales de un campo.

12.1. Extensión de Campos

Decimos que el campo K es una *extensión* del campo κ , si existe un homomorfismo de campos

$$\varphi : \kappa \rightarrow K.$$

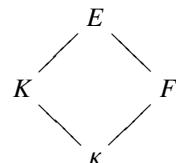
Como homomorfismo de campos φ es inyectiva y K posee un subcampo κ' isomorfo a κ . Por abuso de lenguaje y facilidad en la notación, identificaremos κ con κ' . Si $\kappa \subsetneq K$, entonces se dice que K es una extensión propia de κ .

En particular estudiaremos extensiones en las cuales el campo κ permanece invariante bajo el homomorfismo φ .

Si K es una extensión de κ , se suele escribir

$$\begin{array}{c} K \\ \downarrow \\ \kappa \end{array}$$

y también como $K : \kappa$, lo que interpretaremos como $\kappa \subseteq K$. Así el diagrama



lo interpretaremos como que el campo E es una extensión de los campos κ, K y F y K, F extensiones de κ . En este caso no hay ninguna relación entre K y F .

Las siguientes extensiones son ampliamente conocidas:

$$\begin{array}{ccccccc} \mathbb{R} & & \mathbb{C} & & \text{resultando} & & \mathbb{C} \\ | & & | & & & & | \\ \mathbb{Q} & & \mathbb{R} & & & & \mathbb{R} \\ & & & & & & | \\ & & & & & & \mathbb{Q} \end{array}$$

Vimos también, en la demostración del teorema 11.35, que si P es un polinomio primo en $\kappa[X]$, entonces, $K := \kappa[X]/(P)$ es un campo que contiene al campo κ , por consiguiente

$$\begin{array}{c} \kappa[X]/(P) \\ | \\ K \end{array}$$

es una extensión de campos, en la cual existe, al menos, una raíz de P .

En particular, si $\kappa := \mathbb{Q}$, y $P := X^2 - 2 \in \mathbb{Q}[X]$, entonces P posee todas sus raíces en la extensión de \mathbb{Q} , $\mathbb{Q}[X]/(X^2 - 2)$. Si ξ es la clase de X (mód (P)), entonces ξ es un elemento, tal que $\xi^2 = 2$ en el campo $\mathbb{Q}[X]/(X^2 - 2)$ y lo designaremos por $\sqrt{2}$. En efecto, $P = (X + \xi)(X - \xi) = (X + \sqrt{2})(X - \sqrt{2}) \in \mathbb{Q}[X]/(X^2 - 2)$. Si $G \in \kappa[X]$, entonces, por el algoritmo euclídeo, $G = PQ + R$, donde $\text{grad } R < \text{grad } P$, o $R = 0$, por lo que todo elemento de $\mathbb{Q}[X]/(X^2 - 2)$ es de la forma $a + b\xi = a + b\sqrt{2}$, $a, b \in \mathbb{Q}$. (Ver caso general en la demostración del teorema 12.9). Entonces tendremos que

$$\mathbb{Q}[X]/(X^2 - 2) = \mathbb{Q}[\sqrt{2}] := \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}.$$

Una forma de obtener siempre una extensión propia de cualquier campo κ es formando el campo de fracciones del anillo de polinomios $K[X_1, \dots, X_n]$.

Dejamos al lector la sencilla demostración del siguiente

TEOREMA 12.1. *Si K es una extensión de campos, entonces K es un κ -espacio vectorial.*

$$\begin{array}{c} | \\ K \\ | \\ \kappa \end{array}$$

rial.

$[K : \kappa] := \dim_{\kappa} K$ recibe el nombre de *grado* de la extensión K . $[K, \kappa]$ puede ser finito

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

o infinito, entonces diremos que K es una *extensión finita*, respectivamente una *extensión infinita*.

$$\begin{array}{c} | \\ K \\ | \\ \kappa \end{array}$$

infinita.

En el ejemplo precedente tenemos $[\mathbb{Q}[X]/(X^2 - 2) : \mathbb{Q}] \leq 2$, ya que los elementos $1, \xi, \xi^2$ son linealmente dependientes, pues $\xi^2 + 0\xi - 2 \cdot 1 = \xi^2 - 2 = 0$. Como todo elemento de $\mathbb{Q}[X]/(X^2 - 2)$ es de la forma $a + b\xi$, $a, b \in \mathbb{Q}$, $[\mathbb{Q}[X]/(X^2 - 2) : \mathbb{Q}] = \dim_{\mathbb{Q}} \mathbb{Q}[X]/(X^2 - 2) = 2$. Es decir que la extensión

$$\begin{array}{c} \mathbb{Q}[X]/(X^2 - 2) \\ | \\ \mathbb{Q} \end{array}$$

es finita de grado 2.

12.1.1. Extensiones Finitas y Algebraicas. Consideremos, para el teorema y corolario siguientes, las extensiones de campos

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

y mostremos el siguiente

TEOREMA 12.2. *Si $[K : \kappa]$ y $[E : K]$ son finitos, entonces E es una extensión finita de κ y*

$$(12.1) \quad [E : \kappa] = [E : K][K : \kappa]$$

DEMOSTRACIÓN. Supongamos que $[E : K] := m$ y $[K : \kappa] = n$, entonces E posee una base

$$\{e_1, \dots, e_m\}$$

sobre K y K posee una base

$$\{k_1, \dots, k_n\}$$

sobre κ .

Dado $v \in E$, entonces

$$(12.2) \quad v = \sum_{\mu=1}^m \alpha_\mu e_\mu, \quad \alpha_\mu \in K, \mu = 1, 2, \dots, m.$$

Como $\{k_1, \dots, k_n\}$ es base de K sobre κ , cada elemento $\alpha_\mu \in K$, se escribe como

$$(12.3) \quad \alpha_\mu = \sum_{v=1}^n a_{\mu v} k_v, \quad a_{\mu v} \in \kappa, v = 1, 2, \dots, n.$$

De (12.2) y (12.3), se obtiene

$$(12.4) \quad v := \sum_{\mu}^m \sum_{v=1}^n a_{\mu v} k_v e_\mu, \quad a_{\mu v} \in \kappa, \quad k_v e_\mu \in E.$$

Esto quiere decir que los $m \cdot n$ elementos del conjunto $\{k_v \cdot e_\mu\}_{\substack{1 \leq \mu \leq m \\ 1 \leq v \leq n}}$ generan todo el campo E . Vamos a mostrar que estos $m \cdot n$ elementos son linealmente independientes. En efecto, supongamos que se tiene

$$(12.5) \quad 0 = \sum_{\mu}^m \sum_{v=1}^n a_{\mu v} k_v e_\mu = \sum_{\mu}^m \left(\sum_{v=1}^n a_{\mu v} k_v \right) e_\mu = \sum_{\mu=1}^m b_\mu e_\mu,$$

donde

$$b_\mu := \sum_{v=1}^n a_{\mu v} k_v, \quad b_\mu \in K.$$

Como los e_μ son linealmente independientes sobre K resulta que $b_\mu = 0$, $\forall \mu = 1, \dots, m$, y como también los k_v son linealmente independientes sobre κ , resulta, entonces, que para todo $\mu = 1, \dots, m$ y $v = 1, \dots, n$, $a_{\mu v} = 0$. Por consiguiente los $m \cdot n$ vectores $k_v e_\mu$ son linealmente independientes sobre κ y $[E : \kappa] = m \cdot n = [E : K][K : \kappa]$. \square

COROLARIO 12.3. *Si $[E : \kappa]$ es finito, entonces $[K : \kappa]$ es finito y divide a $[E : \kappa]$.*

DEMOSTRACIÓN. Como $K \subseteq E$, K es un κ -subespacio vectorial de E y

$$[K : \kappa] := \dim_{\kappa} K \leq \dim_{\kappa} E = [E : \kappa],$$

por lo que $[K : \kappa]$ es finito. De forma análoga, ya que $[E : \kappa]$ es finito y $\kappa \subseteq K$, resulta también que $[E : K]$ es finito, por lo que las condiciones del teorema 12.2 se cumplen y

$$[E : \kappa] = [E : K][K : \kappa].$$

Por lo tanto $[K : \kappa]$ divide a $[E : \kappa]$. \square

TEOREMA 12.4. *Sea K una extensión finita del campo κ , de grado $[K : \kappa] = n$. Entonces, dado cualquier elemento $u \in K$, existen elementos $a_0, \dots, a_n \in \kappa$, tales que*

$$(12.6) \quad a_0 + a_1 u + a_2 u^2 + \cdots + a_n u^n = 0.$$

DEMOSTRACIÓN. En efecto, como $\dim_{\kappa} K = n$, los $n+1$ elementos $1, u, \dots, u^n$ son linealmente dependientes sobre κ . Por lo tanto existen elementos $a_0, \dots, a_n \in \kappa$, tales que (12.6), vale. \square

Como un corolario inmediato del teorema 12.4 se obtiene el siguiente resultado:

COROLARIO 12.5. *Si K es una extensión finita del campo κ , de grado $[K : \kappa] = n$, entonces para cada $u \in K$, existe un polinomio de grado n*

$$P := a_0 + a_1 X + \cdots + a_n X^n,$$

tal que u es raíz de P .

Decimos que K es una *extensión algebraica* del campo κ , si todo elemento de K es raíz de algún polinomio de $\kappa[X]$.

Entonces el corolario 12.5 se puede formular de la siguiente forma:

Toda extensión finita K de un campo κ es una extensión algebraica.

Decimos que un elemento $u \in K$ es *algebraico* sobre κ , si u es raíz de algún polinomio $P \in \kappa[X]$

En particular un número real o complejo α es algebraico, si es algebraico sobre \mathbb{Q} .

Los elementos de K que no son algebraicos sobre κ se llaman elementos *trascendentes* sobre κ .

Una extensión que no es algebraica sobre κ la llamaremos una extensión *trascendente* sobre κ .

En particular un número real o complejo α es *trascendente*, si es trascendente sobre \mathbb{Q} .

De la teoría de números y del análisis real sabemos que la gran mayoría de números reales son trascendentales sobre \mathbb{Q} . De hecho se tiene el siguiente

TEOREMA 12.6. *El conjunto de todos los números algebraicos es un conjunto contable.*

DEMOSTRACIÓN. Los números algebraicos, por definición son todas las raíces complejas de polinomios en $\mathbb{Q}[X]$. Como \mathbb{Q} es un conjunto contable, es el conjunto de todos los polinomios de grado $\leq m$, para cada entero positivo m , contable. Entonces $\mathbb{Q}[X]$ es también un conjunto contable. Como cada polinomio en $\mathbb{Q}[X]$, posee únicamente un número finito de raíces en \mathbb{C} , es el conjunto de todas ellas contable. \square

Las extensiones

$$\begin{array}{ccc} \mathbb{R} & & \mathbb{C} \\ | & & | \\ \mathbb{Q} & & \mathbb{Q} \end{array}$$

son extensiones trascendentales, por consiguiente infinitas, mientras que la extensión

$$\begin{array}{c} \mathbb{C} \\ | \\ \mathbb{R} \end{array}$$

es una extensión algebraica. El siguiente resultado, cuya demostración la dejamos al lector como ejercicio, nos será útil, para el concepto de adjunción de un elemento de un campo K a un subcampo $\kappa \subseteq K$.

LEMA 12.7. *Sea K un campo y $(\kappa_i)_{i \in I}$ una familia de subcampos de K . Entonces*

$$\kappa := \bigcap_{i \in I} \kappa_i$$

es un subcampo de K .

TEOREMA 12.8. *Sean κ un campo, K una extensión de κ y $a \in K \setminus \kappa$. Entonces existe un campo minimal que contiene tanto a κ como a a , el cual será denotado por $\kappa(a)$ y diremos que $\kappa(a)$ es el campo obtenido de κ por adjunción del elemento a .*

DEMOSTRACIÓN. En efecto, sea

$$\mathfrak{M} := \{E \subseteq K \mid E \text{ subcampo, } a \in E, \kappa \subseteq E\},$$

entonces $\mathfrak{M} \neq \emptyset$, ya que $K \in \mathfrak{M}$ y

$$\kappa(a) := \bigcap_{E \in \mathfrak{M}} E.$$

□

Nótese que $F(a)$ está formado por el conjunto de los elementos de la forma

$$b_0 + b_1 a + \cdots + b_n a^n, \quad b_v \in \kappa, v = 1, \dots, n, \quad n \in \mathbb{N}$$

y sus elementos inversos respectivos, que no necesariamente son de esta forma.

TEOREMA 12.9. *El elemento $a \in K$ es algebraico sobre κ . Ssi $\kappa(a)$ es una extensión finita de κ .*

DEMOSTRACIÓN. Si $[\kappa(a) : \kappa]$ es finito, entonces, por corolario 12.5, $\kappa(a)$ es una extensión algebraica de κ y por consiguiente a es algebraico sobre κ .

Por otra parte, si a es algebraico sobre κ , entonces a es raíz de algún polinomio en $\kappa[X]$. Consideremos el homomorfismo

$$\psi : \kappa[X] \rightarrow \kappa(a),$$

definido por $\psi(P) := P(a)$, $\forall P \in \kappa[X]$ y $\ker \psi \neq (0)$, ya que a es algebraico. Como $\kappa[X]$ es un anillo principal, existe un polinomio $P \in \kappa[X]$, tal que $\ker \psi = (P)$. P es el polinomio de grado mínimo que está en $\ker \psi$ y es irreducible en $\kappa[X]$, por lo que $\ker \psi = (P)$ es un ideal maximal en $\kappa[X]$. Entonces $\kappa[X]/(P)$ es un campo que contiene a A y a κ y es isomorfo a un subcampo de $\kappa(a)$. Como $\kappa(a)$ es minimal entre todos los campos que contienen a κ y a a , resulta que $\kappa(a)$ es isomorfo a $\kappa[X]/(P)$.

Si

$$P := a_n X^n + \cdots + a_0,$$

entonces

$$0 = a_n \xi^n + \cdots + a_0, \quad a_v \in \kappa, v = 1, 2, \dots, n,$$

y los elementos $1, \xi, \dots, \xi^n$ son linealmente dependientes sobre κ . Vamos a mostrar que el conjunto

$$B := \{1, \xi, \dots, \xi^{n-1}\}$$

es una base de $\kappa[X]/(P)$ sobre κ . En efecto, los vectores de B son linealmente independientes, ya que, en caso contrario, existiría un polinomio $P' \in \ker \psi$ cuyo grado sería menor

que el grado de P , lo cual, por definición de P , no sería posible. Dado $G \in \kappa[X]$, entonces, por el algoritmo euclídeo, $G = PQ + R$, donde $\text{grad } R < \text{grad } P$ o $R = 0$ y $\bar{G} = R(\xi)$. Si

$$R := b_0 + b_1X + \cdots + b_{n-1}X^{n-1}, \quad \text{entonces } R(\xi) = b_0 + b_1\xi + \cdots + b_{n-1}\xi^{n-1},$$

y todo elemento de $\kappa[X]/(P)$ es de esta forma. Por consiguiente $\dim_{\kappa} \kappa(a) = n = \text{grad } P$. \square

Si a es un elemento algebraico sobre κ , al polinomio mónico P que genera al núcleo del homomorfismo

$$\psi : \kappa[X] \rightarrow \kappa(a)$$

lo llamamos el *polinomio minimal* de a . Si $\text{grad } P = n$, entonces se dice que a es un elemento algebraico de grado n sobre κ .

TEOREMA 12.10. *Si $a, b \in K$ son elementos algebraicos sobre κ , entonces $a \pm b, a - b, ab$ son también algebraicos sobre κ , de grado, a lo sumo, $m \cdot n$. Si $a \neq 0$, entonces también a^l es algebraico sobre κ . Es decir que el conjunto de todos los elementos algebraicos sobre κ es un subcampo de K .*

DEMOSTRACIÓN. Supongamos que $[\kappa(a) : \kappa] = m$ y $[\kappa(b) : \kappa] = n$. Entonces, si $E := \kappa(a)(b)$, $[E : \kappa(a)]$ es finito, ya que b algebraico sobre κ , implica b algebraico sobre $\kappa(a)$. Si P, \tilde{P} son los polinomios minimales de b en $\kappa[X]$ y $\kappa(a)[X]$ respectivamente, entonces $\text{grad } \tilde{P} \leq \text{grad } P$, ya que P podría ser reducible en $\kappa(a)$. Entonces $[E : \kappa] = [E : \kappa(a)][\kappa(a) : \kappa] \leq m \cdot n$. Por lo tanto E es una extensión algebraica de κ que contiene a $a, b, a \pm b$ y a a^{-1} , si $a \neq 0$. \square

La extensión $\kappa(a)(b)$ se suele denotar por $\kappa(a, b)$ y de forma inductiva definiremos $\kappa(a_1, \dots, a_n) := \kappa(a_1, \dots, a_{n-1})(a_n)$.

TEOREMA 12.11. *Si K es una extensión algebraica de κ y E una extensión algebraica de K , entonces E es una extensión algebraica de κ .*

DEMOSTRACIÓN. Hay que mostrar que si $u \in E$, entonces u es algebraico sobre κ . En efecto, como u es algebraico sobre K , u es raíz de un polinomio $P \in K[X]$. Supongamos

$$P := a_nX^n + \cdots + a_0, \quad a' \in K, v = 0, \dots, n.$$

Ahora bien, como los a_v son algebraicos sobre κ , entonces $F := \kappa(a_0, \dots, a_n)$ es una extensión algebraica sobre κ . Como u es raíz de $P \in F[X]$, E es algebraico sobre F y $F(u)$ es una extensión finita de F . Entonces $[F(u) : \kappa] = [F(u) : F][F : \kappa] < \infty$. Por lo tanto, por teorema 12.9 u es algebraico sobre κ . \square

TEOREMA 12.12. *Sea $P \in \kappa[X]$ un polinomio irreducible en $\kappa[X]$, de grado $n \geq 1$. entonces existe una extensión K de κ , de grado $[K : \kappa] = n$, tal que P posee una raíz en K .*

DEMOSTRACIÓN. En efecto, del teorema 11.35, sabemos que $K := \kappa[X]/(P)$ es una extensión del campo κ que contiene una raíz de P y, por teorema 12.9, $[K : \kappa] = \text{grad } P = n$. \square

Para el caso en que el polinomio P no es irreducible en $\kappa[X]$, obtenemos el siguiente

COROLARIO 12.13. *Si P es un polinomio en $\kappa[X]$, de grado n , entonces existe una extensión finita K de κ , en la cual P posee una raíz y $[K : \kappa] \leq n = \text{grad } P$.*

DEMOSTRACIÓN. Si P es irreducible en $\kappa[X]$, se tiene el teorema 12.12. Si P es reducible en $\kappa[X]$, se aplica el teorema 12.12, a una componente irreducible P' de P , de $\text{grad } P' < \text{grad } P$. \square

El siguiente teorema, que es una versión más completa del teorema 11.36, nos garantiza, que dado un polinomio $P \in \kappa[X]$, siempre será posible, por medio de extensiones finitas, encontrar una extensión en la cual P tiene todas sus raíces. En particular, nos dice que dado un polinomio $P \in \kappa[X]$, podemos obtener su campo de descomposición K_P , como una extensión finita del campo κ .

TEOREMA 12.14. *Sea $P \in \kappa[X]$ un polinomio de grado $n \geq 1$, entonces existe una extensión E , de grado, a lo sumo $n!$, tal que P se descompone en $E[X]$ en todos sus factores lineales.*

DEMOSTRACIÓN. Por el corolario 12.13, existe una extensión E_1 de κ , tal que $[E_1 : \kappa] \leq n$ y P posee una raíz $\alpha_1 \in E_1$. Entonces

$$P = (X - \alpha_1)P_1, \quad P_1 \in E_1[X], \quad \text{grad } P_1 = n - 1.$$

Aplicando nuevamente el corolario 12.13, existe una extensión E_2 de E_1 , tal que $[E_2 : E_1] \leq n - 1$ y P_1 posee una raíz α_2 en E_2 y $[E_2 : \kappa] \leq n(n - 1)$. Continuando el proceso $n - 1$ veces, obtenemos la cadena de extensiones

$$E_0 := \kappa \subseteq E_1 \subseteq \cdots \subseteq E_{n-1},$$

donde $[E_{\nu+1} : E_\nu] = n - \nu$, $\nu = 0, 1, \dots, n - 2$ y

$$P = (X - \alpha_1) \cdots (X - \alpha_{n-1})P_{n-1}, \quad P_{n-1} \in E_{n-1}[X],$$

y $\text{grad } P_{n-1} = 1$. Entonces $P_1 := aX - b$, donde $a, b \in E_{n-1}$, posee su raíz en E_{n-1} y P se descompone en $E[X]$ como

$$P = a(X - \alpha_1) \cdots (X - \alpha_{n-1})(X - b).$$

Entonces

$$[E_{n-1} : \kappa] = [E_{n-1} : E_{n-2}] \cdots [E_1 : \kappa] \leq n!.$$

□

LEMA 12.15. *Sean $\tau : \kappa \rightarrow \tilde{\kappa}$ un isomorfismo de campos, $\kappa[X], \tilde{\kappa}[Y]$ los anillos de polinomios en las indeterminadas X, Y , sobre κ y $\tilde{\kappa}$ respectivamente. Entonces existe un isomorfismo*

$$\tau_* : \kappa[X] \rightarrow \tilde{\kappa}[Y]$$

que hace commutar al diagrama

(12.7)

$$\begin{array}{ccc} \kappa & \xrightarrow{\tau} & \tilde{\kappa} \\ i_1 \downarrow & & \downarrow i_2 \\ \kappa[X] & \xrightarrow{\tau_*} & \tilde{\kappa}[Y] \end{array}$$

donde i_1, i_2 son las inclusiones respectivas.

DEMOSTRACIÓN. En efecto, el homomorfismo definido por $\tau_*(aX) := \tau(a)T$, $\forall a \in \kappa$, satifase las condiciones deseadas. □

Del lema 12.15 y del tercer teorema de isomorfía para anillos 9.7, se obtiene el siguiente

COROLARIO 12.16. *Sean $P \in \kappa[X]$ un polinomio irreducible y $\tilde{P} \in \tilde{\kappa}[Y]$ su imagen bajo el isomorfismo τ_* . Entonces τ induce un isomorfismo de campos*

$$\tilde{\tau}_* : \kappa[X]/(P) \rightarrow \tilde{\kappa}[Y]/(\tilde{P}),$$

que hace commutar al diagrama

(12.8)

$$\begin{array}{ccc} \kappa & \xrightarrow{\tau} & \tilde{\kappa} \\ i_1 \downarrow & & \downarrow i_2 \\ \kappa[X] & \xrightarrow{\tau_*} & \tilde{\kappa}[Y] \\ \pi_1 \downarrow & & \downarrow \pi_2 \\ \kappa[X]/(P) & \xrightarrow{\tilde{\tau}_*} & \tilde{\kappa}[Y]/(\tilde{P}) \end{array}$$

en todas sus componentes.

En particular nos interesa el caso en que τ es la identidad sobre κ , pues nos interesa determinar la relación que existe entre dos campos de descomposición K_P y \tilde{K}_P de un polinomio P , obtenidos por procedimientos distintos. Nuestro objetivo es mostrar que existe un isomorfismo de campos

$$\sigma : K_P \rightarrow \tilde{K}_P,$$

y que éste puede ser escogido de modo que $\sigma|_{\kappa} = 1_{\kappa}$.

TEOREMA 12.17. *Sean $\tau : \kappa \rightarrow \tilde{\kappa}$ un isomorfismo de campos, $P \in \kappa[X]$ un polinomio irreducible en $\kappa[X]$, $\tilde{P} := \tau_*(P)$ y v una raíz de P en una extensión K de κ . Entonces $\kappa(v)$ es isomorfo a $\tilde{\kappa}(w)$, donde w es una raíz de \tilde{P} en una extensión \tilde{K} de $\tilde{\kappa}$. Además el isomorfismo*

$$\sigma : \kappa(v) \rightarrow \tilde{\kappa}(w)$$

puede ser escogido de modo que:

1. $\sigma(v) = w$.
2. $\sigma(\alpha) = \tau(\alpha)$.

En particular, si $\kappa = \tilde{\kappa}$ y si v, w poseen el mismo polinomio minimal sobre κ , entonces $\sigma|_{\kappa} = 1_{\kappa}$.

DEMOSTRACIÓN. Sea v una raíz de P en una extensión K de κ , entonces, como se vió en la demostración del teorema 12.9, se tiene un isomorfismo

$$\hat{\phi} : \kappa[X]/(P) \rightarrow \kappa(v)$$

donde v se identifica con la clase ξ de X (mód (P)) y se tiene el diagrama commutativo

(12.9)

$$\begin{array}{ccc} \kappa[X] & \xrightarrow{\varphi} & \kappa(v) \\ \pi \downarrow & \nearrow \hat{\phi} & \\ \kappa[X]/(P) & & \end{array}$$

Como τ_* es un isomorfismo, también \tilde{P} es irreducible en $\tilde{\kappa}[Y]$ y se tiene también un isomorfismo de campos

$$\tilde{\phi} : \tilde{\kappa}[Y]/(\tilde{P}) \rightarrow \tilde{\kappa}(w)$$

y el diagrama comutativo

$$(12.10) \quad \begin{array}{ccc} \tilde{\kappa}[Y] & \xrightarrow{\tilde{\varphi}} & \tilde{\kappa}(w) \\ \pi \downarrow & \nearrow \tilde{\varphi} & \\ \kappa[Y]/(\tilde{P}) & & \end{array}$$

Juntando los diagramas (12.9) y (12.10) obtenemos el diagrama comutativo en todas sus componentes

$$(12.11) \quad \begin{array}{ccc} K & \xrightarrow{\tau} & \tilde{K} \\ i_1 \downarrow & & \downarrow i_2 \\ \kappa[X] & \xrightarrow{\tau_*} & \tilde{\kappa}[Y] \\ \pi_1 \downarrow & & \downarrow \pi_2 \\ \kappa[X]/(P) & \xrightarrow{\tilde{\tau}_*} & \tilde{\kappa}[Y]/(\tilde{P}) \\ \hat{\varphi} \downarrow & & \downarrow \tilde{\varphi} \\ \kappa(v) & \xrightarrow[\sigma]{} & \tilde{\kappa}(w) \end{array}$$

donde $\sigma := \tilde{\varphi} \circ \tilde{\tau}_* \circ \hat{\varphi}^{-1}$ es un isomorfismo entre $\kappa(v)$ y $\tilde{\kappa}(w)$ que cumple con lo deseado. En particular si $\kappa = \tilde{\kappa}$, $\tau = 1_\kappa$ y $X = T$, σ es un isomorfismo que deja fijos a los elementos de κ , es decir $\sigma|_\kappa = 1_\kappa$. \square

El siguiente teorema constituye la piedra angular que nos llevará a la teoría de Galois.

TEOREMA 12.18. *Cualesquiera campos de descomposición K_P , $\tilde{K}_{\tilde{P}}$ de los polinomios $P \in \kappa[X]$ y $\tilde{P} := \tau_*(P) \in \tilde{\kappa}[Y]$ respectivamente, son isomorfos, con un isomorfismo*

$$\sigma : K_P \rightarrow \tilde{K}_{\tilde{P}},$$

tal que el diagrama

$$(12.12) \quad \begin{array}{ccc} K & \xrightarrow{\tau} & \tilde{K} \\ i_1 \downarrow & & \downarrow i_2 \\ K_P & \xrightarrow[\sigma]{} & \tilde{K}_{\tilde{P}} \end{array}$$

es comutativo. En particular si $\kappa = \tilde{\kappa}$ y $\tau = 1_\kappa$, entonces σ es un isomorfismo entre dos campos de descomposición de P , que deja fijos todos los elementos de κ .

DEMOSTRACIÓN. Por inducción sobre el grado $[K : \kappa]$ de la extensión.

Si $[K : \kappa] = 1$, entonces $K = \kappa$ y P se descompone en factores lineales en $\kappa[X]$ y \tilde{P} se descompone en factores lineales en $\tilde{\kappa}[Y]$. Entonces $\sigma := \tau$ satisface lo deseado.

Supongamos, por hipótesis de inducción, que el resultado sea cierto para cualquier campo κ_0 y cualquier polinomio P_0 cuyo campo de descomposición K_0 sea tal, que $[K_0 : \kappa_0] < n$, $n > 1$.

Sea K , $[K := \kappa] = n > 1$ el campo de descomposición del polinomio $P \in \kappa[X]$. Como $n > 1$, P posee en $\kappa[X]$ un factor G irreducible, de grado $\text{grad } G = r > 1$ y su correspondiente \tilde{P} , posee en $\tilde{\kappa}[Y]$ un factor irreducible \tilde{G} .

Como P se descompone en K en factores lineales, también lo hará G y existe, entonces,

$v \in K$, tal que $G(v) = 0$. Entonces $[\kappa(v) : \kappa] = r > 1$. En forma análoga, para \tilde{G} , existe $w \in \tilde{K}$, tal que $\tilde{G}(w) = 0$ y $[\tilde{\kappa}(w) : \tilde{\kappa}] = r > 1$. Por el teorema 12.17, existe un isomorfismo

$$\tilde{\sigma} : \kappa(v) \rightarrow \tilde{\kappa}(w),$$

tal que el diagrama

(12.13)

$$\begin{array}{ccc} \kappa & \xrightarrow{\tau} & \tilde{\kappa} \\ i_1 \downarrow & & \downarrow i_2 \\ \kappa(v) & \xrightarrow{\tilde{\sigma}} & \tilde{\kappa}(w) \end{array}$$

es comutativo. Como $[\kappa(v) : \kappa] = r > 1$, resulta de

$$[K : \kappa] = [K : \kappa(v)][\kappa(v) : \kappa] = n = [K : \kappa(v)]r$$

que

$$[E : \kappa(v)] = \frac{n}{r} < n.$$

Como K es campo de descomposición de $P \in \kappa[X]$, también lo será de $P \in \kappa(v)[X]$, por lo que podemos aplicar la hipótesis de inducción a la extensión

$$\begin{array}{c} K \\ |_{<n} \\ \kappa(v) \end{array}$$

En forma análoga procederemos para la extensión

$$\begin{array}{c} \tilde{K} \\ |_{<n} \\ \tilde{\kappa}(w) \end{array}$$

Entonces existe un isomorfismo

$$\sigma : K \rightarrow \tilde{K}$$

que hace conmutar al diagrama

(12.14)

$$\begin{array}{ccc} \kappa(v) & \xrightarrow{\tau} & \tilde{\kappa}(w) \\ i_1 \downarrow & & \downarrow i_2 \\ K & \xrightarrow{\sigma} & \tilde{K} \end{array}$$

De la commutatividad de los diagramas (12.13) y (12.14), resulta la commutatividad del diagrama (12.12).

Si $\kappa = \tilde{\kappa}$, tomamos $\tau := 1_\kappa$ y entonces, si K y \tilde{K} son campos de descomposición de P , existe un isomorfismo

$$\sigma : K \rightarrow \tilde{K}$$

que deja fijos los elementos de κ .

□

12.1.2. Ejercicios y Complementos.

1. Mostrar el teorema 12.1.
2. Mostrar el lema 12.7
3. Sea \mathbb{Q} el campo de los números racionales y sea $\sqrt[3]{2} := \xi$, la clase de X (mód $(X^3 - 2)$). Si definimos $\mathbb{Q}[\xi] = \mathbb{Q}[\sqrt[3]{2}] := \mathbb{Q}[X]/(X^3 - 2)$, mostrar que $\mathbb{Q}[\sqrt[3]{2}]$ es un campo, extensión algebraica de \mathbb{Q} y que

$$\mathbb{Q}[\sqrt[3]{2}] = \{a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2 \mid a, b, c \in \mathbb{Q}\}.$$

Es decir que $\mathbb{Q}(\sqrt[3]{2}) = \mathbb{Q}(\sqrt[3]{2})$ y que $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$.

4. Sea $\sigma : \mathbb{Q}(\sqrt[3]{2}) \rightarrow \mathbb{Q}(\sqrt[3]{2})$ un isomorfismo que deja fijos los elementos de \mathbb{Q} . Mostrar que

- a) $\sigma(a + b\sqrt[3]{2}) = a + \sigma(\sqrt[3]{2})$
- b) Si $\sigma(\sqrt[3]{2}) = \alpha + \beta\sqrt[3]{2}$, entonces, para que σ sea un homomorfismo $\alpha = 0$ y $\beta = \pm 1$. (Ayuda: Considerar que $\sigma(2) = 2 = \sigma(\sqrt[3]{2})(\sigma(\sqrt[3]{2}))$).
5. Si $\alpha \in K$, donde K es una extensión de κ es un elemento trascendente sobre el campo κ y $\kappa[\alpha]$ es el anillo formado por todas las combinaciones lineales de las potencias de α con los elementos de κ , mostrar que $\kappa[\alpha]$ es isomorfo a $\kappa[X]$ y que $\kappa(\alpha)$ es isomorfo a $\mathbb{Q}(\kappa[X])$. Por lo que si α no es algebraico sobre κ , $\kappa[\alpha] \neq \kappa(\alpha)$. Mostrar además que $[\kappa(\alpha) : \kappa] = \infty$ y por consiguiente también $[K : \kappa] = \infty$.
6. Sea

$$\mathfrak{G}(K : \kappa) := \{\sigma : K \rightarrow K \mid \sigma \text{ es un isomorfismo que deja fijo al subcampo } \kappa \subseteq K\}.$$

Mostrar que $(\mathfrak{G}(K : \kappa), \circ)$, donde \circ es la composición de homomorfismos, es un grupo, llamado el *grupo de Galois* de la extensión

$$\begin{array}{c} K \\ \downarrow \\ \kappa \end{array}$$

7. Consideremos la extensión

$$\begin{array}{c} \mathbb{Q}(\sqrt[3]{2}) \\ \downarrow \\ \mathbb{Q} \end{array}$$

Usar el resultado en el ejercicio 4, para mostrar que $\mathfrak{G}(\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q})$ es isomorfo al grupo $(\mathbb{Z}_2, +)$.

8. Sea $\sigma : \kappa \rightarrow \kappa$ un isomorfismo de campos. Si $\alpha \in \kappa$ es una raíz de $P \in \kappa[X]$, mostrar que $\sigma(\alpha)$ es una raíz de $\sigma_*(P)$.
9. Sea $\sigma \in \mathfrak{G}_\kappa$. Probar que si α es raíz de un polinomio $P \in \kappa[X]$, entonces también $\sigma(\alpha)$ es raíz de P .
10. Si κ es un campo de característica $p \neq 0$, mostrar que toda extensión K de κ debe ser también de la misma característica p .
11. Sea E un campo intermedio de la extensión

$$\begin{array}{c} K \\ \downarrow \\ E \\ \downarrow \\ \kappa \end{array}$$

Entonces, si $\alpha \in K$ es un elemento algebraico sobre κ también lo será sobre E . Mostrar que el polinomio minimal de α sobre E es un divisor del polinomio minimal de α sobre κ . (Ayuda: considerar el polinomio minimal \tilde{P} de α sobre E y aplicar algoritmo euclídeo al polinomio minimal P de α sobre κ y a \tilde{P} en $E[X]$).

12. Mostrar que una extensión de campos

$$\begin{array}{c} K \\ | \\ \kappa \end{array}$$

es finita, Ssi existen elementos algebraicos sobre κ , $\alpha_1, \dots, \alpha_n \in K$, tales que $K := \kappa(\alpha_1, \dots, \alpha_n)$.

12.1.3. Envolvente Algebraica y Clausura Algebraica.

Sea

$$\begin{array}{c} K \\ | \\ \kappa \end{array}$$

una extensión de campos. Al conjunto

$$H_a(K : \kappa) := \{x \in K \mid x \text{ algebraico sobre } \kappa\}$$

lo llamamos la *envolvente algebraica cerrada* de κ . Por teorema 12.10, $H_a(K : \kappa)$ es un campo y es el campo más pequeño que contiene al campo κ y todos los elementos algebraicos sobre κ .

Decimos que κ es *algebraicamente cerrado* en K , si $H_a(K : \kappa) = \kappa$.

Decimos que un campo K es *algebraicamente cerrado*, si todo polinomio en $K[X]$ posee una raíz en K . De forma equivalente podemos decir que un campo K es algebraicamente cerrado, Ssi todo polinomio $P \in K[X]$ se descompone en factores lineales en $K[X]$.

De la definición de algebraicamente cerrado se deduce el siguiente

TEOREMA 12.19. κ es un campo algebraicamente cerrado, Ssi para cualquier extensión K de κ , $H_a(K : \kappa) = \kappa$.

DEMOSTRACIÓN. En efecto, si κ es algebraicamente cerrado, entonces todo polinomio en $\kappa[X]$ se descompone en factores lineales en $\kappa[X]$, es decir que todas sus raíces están en κ , entonces si α es un elemento algebraico sobre κ , α es raíz de un polinomio en $\kappa[X]$ y por consiguiente $\alpha \in \kappa$. Por lo tanto $H_a(K : \kappa) = \kappa$, para cualquier extensión K de κ .

Por otra parte si $H_a(K : \kappa) = \kappa$, para cualquier extensión K de κ y $\alpha \in K$ una raíz de un polinomio cualquiera $P \in \kappa[X]$, entonces α es algebraico sobre κ y, por hipótesis, $\alpha \in \kappa$, por consiguiente P se descompone en factores lineales en $\kappa[X]$, por lo que κ es algebraicamente cerrado. \square

TEOREMA 12.20. Para cualquier extensión K del campo κ

$$H_a(K : H_a(K : \kappa)) = H_a(K : \kappa).$$

Es decir que todo elemento algebraico sobre $H_a(K : \kappa)$ es ya algebraico sobre κ .

DEMOSTRACIÓN. Sea $\alpha \in K$ un elemento algebraico sobre $H_a(K : \kappa)$, entonces α es raíz de un polinomio $P \in H_a(K : \kappa)$

$$P := \sum_{v=0}^n a_v X^v, \quad a_v \in H_a(K : \kappa), \quad v = 0, \dots, n.$$

Si $K_1 := \kappa(a_0, \dots, a_n)$, entonces, K_1 es una extensión algebraica sobre κ y $K_2 := H_a(K : \kappa)$ es una extensión algebraica de K_1 , ya que es extensión algebraica de $\kappa \subseteq K_1$. Entonces

$$[K_2(\alpha) : \kappa] = [K_2(\alpha) : K_2][K_2 : K_1][K_1 : \kappa] < \infty.$$

Por consiguiente α es algebraico sobre κ y $H_a(K : H_a(K : \kappa)) \subseteq H_a(K : \kappa)$. La otra inclusión es obvia, ya que $\kappa \subseteq H_a(K : \kappa)$, por lo que todo elemento algebraico sobre κ lo es también sobre $H_a(K : \kappa)$. \square

TEOREMA 12.21. κ es algebraicamente cerrado en la extensión K , Ssi ningún polinomio irreducible $P \in \kappa[X]$, de grado $\text{grad } P \geq 2$, posee raíces en K .

DEMOSTRACIÓN. κ es algebraicamente cerrado en K , Ssi para cualquier elemento $\alpha \in K$ algebraico sobre κ el polinomio minimal es de grado 1.

Si $\alpha \in K$ fuera raíz de un polinomio irreducible $P \in \kappa[X]$ con $\text{grad } P \geq 2$, entonces P sería el polinomio minimal de α y $[\kappa(\alpha) : \kappa] \geq 2$ y $\alpha \notin \kappa$.

Por otra parte, si ningún polinomio irreducible de grado ≥ 2 posee raíces en K y κ no fuera algebraicamente cerrado en K , entonces existiría un elemento algebraico $\alpha \in K$, tal que $\alpha \notin \kappa$, con lo que el polinomio minimal de α sería un polinomio irreducible de grado ≥ 2 , con raíces en K , lo cual es contradictorio. \square

12.1.4. Extensiones Simples.

Decimos que

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

es una *extensión simple*, si $K = \kappa(\alpha)$, para algún $\alpha \in K$. Entonces diremos que α es un *elemento primitivo* de la extensión K . Así, por ejemplo, si K es el campo de descomposición del polinomio $P := X^2 - 2 \in \mathbb{Q}[X]$, $K = \mathbb{Q}[\sqrt{2}]$ es una extensión simple de \mathbb{Q} , con elemento primitivo $\sqrt{2}$. También la extensión

$$\begin{array}{c} \mathbb{C} \\ | \\ \mathbb{R} \end{array}$$

es una extensión simple, ya que $\mathbb{C} = \mathbb{R}[i]$, donde $i^2 = -1$ es un elemento primitivo.

El siguiente teorema nos da la clave para encontrar un campo intermedio de una extensión algebraica simple.

TEOREMA 12.22. Sea

(12.15)

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

una extensión finita simple, con elemento primitivo $\alpha \in K$ y E un campo intermedio, $\kappa \subseteq E \subseteq K$. Si

$$G := \sum_{v=0}^n b_v^n X^v, \quad b_v \in E, \quad v = 0, \dots, n,$$

el polinomio minimal de α sobre E , entonces $E = \kappa(b_0, \dots, b_n)$.

DEMOSTRACIÓN. Sea $E_0 := \kappa(b_0, \dots, b_n)$. Entonces $\kappa \subseteq E_0 \subseteq E \subseteq K$. Como $G \in E_0[X]$ es el polinomio minimal de α sobre E , G es irreducible en $E[X]$ y por consiguiente también

irreducible en $E_0[X]$, por lo que también es el polinomio minimal de α sobre E_0 . Como α es elemento primitivo de la extensión (12.15), también lo es de la extensión

(12.16)

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

Como $K = \kappa(\alpha)$, tenemos

$$[K : E_0] = [K : E] = \text{grad } G$$

y

$$[K : E_0] = [K : E][E : E_0] = [K : E_0][E : E_0].$$

Por lo tanto $[E : E_0] = 1$ y $E = E_0$. \square

TEOREMA 12.23 (Steinitz). *Una extensión*

$$\begin{array}{c} K \\ | \\ \kappa \end{array}$$

finita es simple, Ssi posee sólo un número finito de campos intermedios.

DEMOSTRACIÓN. Del teorema 12.22, si K es una extensión simple, entonces cualquier campo intermedio E es de la forma $\kappa(b_0, \dots, b_n)$, donde los $b_v, v = 0, \dots, n$ son los coeficientes del polinomio minimal del elemento primitivo α sobre E .

Sea $P \in \kappa[X]$ el polinomio minimal de α sobre κ . Para cada factor mónico G de P en $K[X]$, consideremos el campo intermedio $K_G := \kappa(a_0, \dots, a_m)$, donde los $a_\mu \in K$, $\mu = 0, \dots, m$ son los coeficientes de $G \in K[X]$. Dado un campo intermedio cualquiera E , por ejercicio 12.1.2, 11, el polinomio minimal \tilde{P} de α sobre E es un divisor P en $K[X]$ y $K_{\tilde{P}} = E$, por lo que la aplicación $G \mapsto K_G$ es sobreyectiva, por lo que no pueden haber más campos intermedios que los factores monicos de P en $K[X]$. Por lo tanto sólo pueden existir un número finito de campos intermedios.

Por otra parte, supongamos que sólo existen un número finito de campos intermedios en la extensión

$$\begin{array}{c} K \\ | \\ \kappa \end{array}$$

Si κ es un campo finito, entonces K también es finito, ya que $[K : \kappa] < \infty$. Si α es un generador del grupo cíclico K^* , de los elementos invertibles de K , entonces $K = \kappa(\alpha)$, por lo que K es una extensión simple con elemento primitivo α .

Sea, entonces, κ un campo infinito. Como K es una extensión finita de κ , por ejercicio 12.1.2.12, existen $\alpha_1, \dots, \alpha_n \in K$, tales que $K = \kappa(\alpha_1, \dots, \alpha_n)$. Vamos a mostrar que si ξ, η son cualesquier elementos en K , entonces $\kappa(\xi, \eta)$ es una extensión simple.

Dado $a \in \kappa$, sea $\kappa_a := \kappa(\xi + a\eta)$, como κ contiene infinitos elementos y, por hipótesis, sólo existe un número finito de campos intermedios, debe existir un $b \in \kappa$, $b \neq a$, tal que $\kappa_b = \kappa_a$. Entonces $\xi + a\eta, \xi + b\eta \in \kappa_a$ y por consiguiente $(b - a)\eta = (\xi + a\eta) - (\xi + b\eta) \in \kappa_a$, como $a \neq b$, $a - b \neq 0$ y $\eta = (a - b)^{-1}(a - b)\eta \in \kappa_a$. Con η , también $b\eta \in \kappa_a$, por lo que $\xi = \xi + b\eta - b\eta \in \kappa_a$. Entonces $\kappa(\xi, \eta) \subseteq \kappa_a$ y $\kappa_a \subseteq \kappa(\xi, \eta)$. Por lo tanto $\kappa(\xi, \eta)$ es simple. Siguiendo un proceso inductivo, se concluye que $K = \kappa(\alpha_1, \dots, \alpha_n)$ es simple. \square

Como una consecuencia inmediata del teorema 12.23, se tiene el

COROLARIO 12.24. Si

$$\begin{array}{c} K \\ \downarrow \\ \kappa \end{array}$$

es una extensión finita y simple, entonces

$$\begin{array}{c} K \\ \downarrow \\ E \end{array}$$

es una extensión simple, para cualquier campo intermedio E .

12.1.5. Extensiones Normales. Decimos que la extensión

$$\begin{array}{c} K \\ \downarrow \\ \kappa \end{array}$$

es una *extensión normal* sobre κ , si K es una extensión algebraica y si todo polinomio que posee, al menos una, raíz en K , se descompone en factores lineales en $K[X]$.

Decimos que dos elementos $\alpha, \beta \in K$ son *conjugados* sobre κ , si poseen el mismo polinomio minimal.

Por ejemplo en la extensión

$$\begin{array}{c} \mathbb{Q}[\sqrt{2}] \\ \downarrow \\ \mathbb{Q} \end{array}$$

$\sqrt{2}$ y $-\sqrt{2}$ son conjugados.

TEOREMA 12.25. Sea

$$\begin{array}{c} K \\ \downarrow \\ \kappa \end{array}$$

una extensión, entonces, dos elementos $\alpha, \beta \in K$ son conjugados sobre κ , Ssi existe un κ -homomorfismo

$$\varphi : \kappa(\alpha) \rightarrow \kappa(\beta)$$

tal que $\varphi(\alpha) = \beta$.

DEMOSTRACIÓN. Vamos a mostrar que los ideales (P_α) y (P_β) generados por los polinomios minimales correspondientes son iguales, si φ es un κ -isomorfismo. En efecto, sea $G \in (P_\alpha)$, entonces $0 = \varphi(G(\alpha)) = G(\beta)$, lo que implica que $G \in (P_\beta)$. Por otra parte, aplicando φ^{-1} a $H \in (P_\beta)$, se obtiene que $H \in (P_\alpha)$. Por consiguiente $(P_\alpha) = (P_\beta)$, de donde $P_\alpha = P_\beta$.

La conversa resulta del teorema 12.18. □

TEOREMA 12.26 (Teorema de Normalidad Finita). Sea

(12.17)

$$\begin{array}{c} K \\ \downarrow \\ \kappa \end{array}$$

una extensión finita. Las siguientes condiciones son equivalentes:

1. K es campo de descomposición de un polinomio en $\kappa[X]$.
2. si

$$\begin{array}{c} E \\ \downarrow \\ K \end{array}$$

es una extensión de K y

$$\varphi : K \rightarrow E$$

un κ -homomorfismo, entonces $\varphi[K] \subseteq K$.

3. Lo mismo que en 2, si

$$\varphi : E \rightarrow E$$

es un κ -homomorfismo.

4. La extensión (12.17) es normal.

DEMOSTRACIÓN. 1 \Rightarrow 2: Sea K el campo de descomposición del polinomio $P \in \kappa[X]$, entonces

$$P = a(X - a_1) \cdots (X - a_n), \quad a, a_1, \dots, a_n \in K = \kappa(a_1, \dots, a_n).$$

Si

$$\begin{array}{c} E \\ \downarrow \\ K \end{array}$$

es una extensión y

$$\varphi : K \rightarrow E$$

un κ -homomorfismo, entonces $\varphi(P(a_v)) = P(\varphi(a_v)) = 0$, por lo que $\varphi[\{a_1, \dots, a_n\}] \subseteq \{a_1, \dots, a_n\} \subseteq K$. Por lo tanto $\varphi[K] \subseteq K$.

2 \Rightarrow 3: Resulta de 2, al considerar $\varphi|_K$.

3 \Rightarrow 4: Sea $G \in \kappa[X]$ un polinomio irreducible en $\kappa[X]$, y sin limitación de la generalidad podemos asumir que sea mónico, y $\alpha \in K$ una raíz de G . Como K es una extensión finita sobre κ , existen elementos $\alpha_1, \dots, \alpha_m$, tales que $K = \kappa(\alpha_1, \dots, \alpha_m)$. Podemos suponer que $\alpha = \alpha_1$. Si P_μ es el polinomio minimal de α_μ , entonces $P_1 = G$. Sea $P := P_1 P_2 \cdots P_m$ y E el campo de descomposición de P sobre K . Si M es el conjunto de todas las raíces de P , entonces $\{a_1, \dots, a_n\} \subseteq M$ y

$$E = K(A) = \kappa(a_1, \dots, a_n)(A) = \kappa(\alpha)(A).$$

entonces E es también el campo de descomposición de P sobre $\kappa(\alpha)$. Si $\beta \in K$ es una raíz cualquiera de G , entonces, por teorema 12.18, existe un κ -isomorfismo

$$\tau : \kappa(\alpha) \rightarrow \kappa(\beta)$$

tal que $\tau(\alpha) = \beta$. Igualmente se muestra que E es campo de descomposición de P sobre $\kappa(\beta)$ y τ se extiende a un κ -isomorfismo

$$\varphi : E \rightarrow E,$$

tal que $\varphi|_{\kappa(\alpha)} = \tau$. Entonces, por hipótesis $\beta = \varphi(\alpha) \in K = \kappa(\alpha_1, \dots, \alpha_m)$, $\alpha_1 = \alpha$. Lo que muestra que K es el campo de descomposición de G . Por consiguiente la extensión (12.17) es normal.

4 \Rightarrow 1: Sea $K = \kappa(\alpha_1, \dots, \alpha_m)$ y P el polinomio definido arriba. Entonces, como la extensión (12.17) es normal, P se descompone en factores lineales en $K = \kappa(\alpha_1, \dots, \alpha_m) = \kappa(A)$. Por lo tanto K es campo de descomposición de P . \square

TEOREMA 12.27. *Toda extensión de grado 2 es normal*

DEMOSTRACIÓN. En efecto, si $[K : \kappa] = 2$ y P un polinomio irreducible, con una raíz $\alpha \in K$, entonces $\text{grad } P = [\kappa(\alpha) : \kappa] \leq [K : \kappa] = 2$. Por lo tanto P se descompone en factores lineales en $K[X]$. \square

TEOREMA 12.28. *Si K es normal sobre κ , entonces K es normal sobre cualquier campo intermedio E de la extensión*

(12.18)

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

DEMOSTRACIÓN. Como la extensión (12.18) es algebraica, entonces, para cualquier campo intermedio E , la extensión

(12.19)

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

es también algebraica. Sea P un polinomio en $E[X]$ con una raíz $\alpha \in K$ y sea G el polinomio minimal de α sobre κ , entonces $P \mid G$ en $E[X]$ Y existe $H \in E[X]$, tal que $G = PH$, como, por hipótesis, G se descompone en factores lineales en $K[X]$, también P debe descomponerse en factores lineales en $K[X]$. Por lo tanto la extensión (12.19) es normal. \square

TEOREMA 12.29. *Toda extensión finita*

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

está contenida en una extensión normal

(12.20)

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

DEMOSTRACIÓN. Sea $K = \kappa(\alpha_1, \dots, \alpha_n)$, donde $\alpha_1, \dots, \alpha_n \in K$, elementos algebraicos sobre κ y $P := P_1 \cdots P_n$, donde $P_v, v = 1, \dots, n$ es el polinomio minimal de α_v . Entonces si E es el campo de descomposición de P sobre K , también lo será de P sobre κ , (ver demostración del teorema 12.26), y $[E : K] < \infty$, de donde resulta que la extensión (12.20), es normal. \square

TEOREMA 12.30. *Si K es un campo intermedio de la extensión normal y finita*

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

entonces todo κ -homomorfismo

$$\varphi : K \rightarrow E$$

posee una extensión a un κ -automorfismo

$$\hat{\varphi} : E \rightarrow E.$$

DEMOSTRACIÓN. Como E es normal y finita sobre κ , entonces E es el campo de descomposición de un polinomio $P \in \kappa[X]$ y $E = \kappa(\alpha_1, \dots, \alpha_n)$, donde para cada $v = 1, \dots, n$, α_v es raíz de P en E . Sea

$$\varphi : K \rightarrow E$$

un κ -homomorfismo y

$$\varphi_* : K[X] \rightarrow E[X]$$

el homomorfismo inducido por φ . Como φ es un κ -homomorfismo, se tiene que $\varphi_*(P) = P$ y E es también el campo de descomposición de $\varphi_*(P)$ y sus raíces son las mismas. Si P no posee ninguna raíz en K , entonces $E = K(\alpha_1, \dots, \alpha_n) = \kappa(\alpha_1, \dots, \alpha_n)$ y φ no actúa sobre el conjunto M de raíces de P . Si

$$\sigma : M \rightarrow M$$

es una permutación sobre M , entonces, considerando que cada elemento de E es una combinación lineal de los elementos de M y de κ , σ induce un κ -automorfismo

$$\hat{\varphi} : E \rightarrow E.$$

por medio de

$$\hat{\varphi}\left(\sum_{v=1}^n a_v \alpha_v\right) := \sum_{v=0}^n a_v \sigma(\alpha_v).$$

Si P posee m raíces en K , entonces $m < n$, pues de lo contrario $E = K$. Sin limitación de la generalidad podemos asumir que

$$N := \{\alpha_1, \dots, \alpha_m\}$$

es el conjunto de raíces de P en K y $\varphi[N] \subseteq M$. Si

$$\sigma : M \setminus N \rightarrow M^* := M \setminus \varphi[N]$$

es una biyección, entonces, por medio de

$$\hat{\varphi}\left(\sum_{v=0}^n a_v \alpha_v\right) := \sum_{v=0}^m a_v \varphi(\alpha_v) + \sum_{v=m+1}^n a_v \sigma(\alpha_v)$$

se obtiene un κ -automorfismo

$$\hat{\varphi} : E \rightarrow E.$$

que es una extensión de φ sobre E . □

De los teoremas 12.25 y 12.30 se obtiene el siguiente corolario, cuya demostración dejamos al lector, como un ejercicio.

COROLARIO 12.31. *Sea*

$$\begin{array}{c} E \\ \downarrow \\ K \end{array}$$

una extensión normal y finita. Dos elementos $\alpha, \beta \in E$ son conjugados sobre κ , Ssi existe un κ -automorfismo

$$\hat{\varphi} : E \rightarrow E,$$

tal que $\hat{\varphi}(\alpha) = \beta$.

Para el caso en que

$$\begin{array}{c} K \\ \downarrow \\ \kappa \end{array}$$

es una extensión algebraica no finita, se tiene el siguiente resultado, cuya demostración dejamos al lector, como un sencillo ejercicio:

TEOREMA 12.32. *Una extensión no finita*

$$\begin{array}{c} E \\ \downarrow \\ \kappa \end{array}$$

es normal, Ssi E es unión de campos de descomposición de polinomios en $\kappa[X]$.

12.1.6. Extensiones Separables e Inseparables. Decimos que un elemento $\alpha \in K$ es *separable* sobre κ , si α es raíz de un polinomio separable en $\kappa[X]$. Decimos que K es una *extensión separable* de κ , si todo elemento de K es separable sobre κ . Un elemento algebraico de K que no es separable sobre κ se llama un elemento *inseparable*. Si todos los elementos de la extensión K son inseparables sobre κ , entonces se dice que K es una extensión *inseparable pura*.

Obviamente si el campo κ es de característica 0, toda extensión algebraica sobre κ es separable.

TEOREMA 12.33. *Sea $K := \kappa(\beta, \alpha_1, \dots, \alpha_n)$, donde $\beta, \alpha_1, \dots, \alpha_n$ son separables sobre el campo κ . Entonces E es una extensión simple de κ .*

DEMOSTRACIÓN. Si κ es un campo finito, entonces el teorema vale siempre, aún sin la condición de separabilidad, ya que entonces E es finito y es una extensión simple de su campo primo κ_p , cuyo elemento primitivo es un generador del grupo cíclico E^* .

Sea, entonces κ un campo infinito. Como $\kappa(\beta, \alpha_1, \dots, \alpha_n) = \kappa(\beta, \alpha_1, \dots, \alpha_{n-1})(\alpha_n)$, basta mostrar el teorema para el caso $n = 1$.

Sea entonces $n = 1$, $\alpha := \alpha_1$ y $P \in \kappa[X]$ su polinomio minimal sobre κ . De forma análoga, sea

$$G := \sum_{\mu=0}^m a_\mu X^\mu$$

el polinomio minimal de G sobre κ . Trataremos de encontrar un elemento $a \in \kappa$, tal que nuestro elemento primitivo sea de la forma $\xi := a\alpha + \beta$, lo cual se logra si podemos escoger a de forma tal, que $a\alpha \in \kappa(\xi)$, pues entonces también $\alpha \in \kappa(\xi)$ y $\beta = \xi - a\alpha \in \kappa(\xi)$ y por consiguiente $\kappa(\beta, \alpha) = \kappa(\xi)$.

Vamos a ver que para lograr esto, es suficiente escoger $a \in \kappa$, tal que $(X - \alpha)$ sea un máximo común divisor de P y del polinomio $H := G(\xi - aX)$, en $E[X]$, donde E es una extensión de κ .

En efecto, si $(X - \alpha)$ es un máximo común divisor de P y H en $E[X]$, entonces, por corolario ??, existe un elemento $e \in E^*$, tal que $e(X - \alpha)$ es un máximo común divisor de P, H en $\kappa(\xi)[X]$, por lo que $(eX - e\alpha) \in \kappa(\xi)[X]$ y por consiguiente $e, ea, \alpha \in \kappa(\xi)$.

Sea, entonces, E el campo de descomposición de PG sobre K y $b_1, \dots, b_l, c_1, \dots, c_m$ las raíces en E de P y G respectivamente y escogidas de forma tal, que $b_1 = \alpha$ y $c_1 = \beta$. Vamos a mostrar que si escogemos $a \in \kappa$ de forma tal, que $\xi = ab_\lambda \neq c_\mu$, $\forall \lambda = 2, \dots, l$, $\mu = 1, \dots, m$, entonces a satisface lo deseado. Esta escogencia es posible, ya que el conjunto de elementos $a_{\lambda\mu}$, tales que $\xi - a_{\lambda\mu} = c_\mu$, es decir $a_{\lambda\mu} = \frac{c_\mu - \beta}{\alpha - b_\lambda}$ es finito, mientras que κ posee infinitos elementos.

En efecto, bajo estas condiciones $H_a = G(\xi - a\alpha) = G(\beta) = 0$, por lo que α es una raíz común de P y de H en K , y es la única, ya que, para $\lambda \geq 2$, $H(b_\lambda) = G(\xi - ab_\lambda) \neq 0$, pues por la escogencia de a , $\xi - ab_\lambda \neq c_\mu$, $\forall \mu = 1, \dots, m$. Entonces un máximo común divisor de P, H en $E[X]$, es de la forma $(X - \alpha)^q$, $q \geq 1$. Como P es irreducible y separable sobre κ , por teorema 11.42, α es una raíz simple de P y por consiguiente $q = 1$. \square

De la definición de campo perfecto y del teorema 12.33, se obtiene de forma inmediata el siguiente

COROLARIO 12.34. *Si κ es un campo perfecto, entonces toda extensión finita sobre κ es simple. En particular, toda extensión finita sobre un campo de característica 0 es simple.*

12.1.7. Ejercicios y Complementos.

1. Si

$$\begin{array}{c} K \\ \downarrow \\ \kappa \end{array}$$

es una extensión y $\alpha \in K$ es un elemento algebraico sobre κ , mostrar que las siguientes condiciones son equivalentes:

- a) α es separable sobre κ .
- b) α es raíz simple de su polinomio minimal P .
- c) $P'(\alpha) = 0$.

En particular si κ es un campo perfecto, entonces α es separable Ssi α es algebraico. Entonces en un campo de característica 0 el concepto de separabilidad coincide con el de algebraico.

2. Completar la demostración del corolario 12.34.

3. Si E es un campo intermedio de la extensión

$$\begin{array}{c} K \\ \downarrow \\ \kappa \end{array}$$

y $\alpha \in K$ separable sobre κ , mostrar que entonces α es separable sobre E . (Ayuda: usar el hecho que el polinomio minimal de α sobre E divide al polinomio minimal de α sobre κ).

12.1.8. Separabilidad en Campos de Característica $p \neq 0$. Como en todo campo de característica 0 el concepto de separabilidad coincide con el de algebraico, procede analizar aquí el caso en que κ es un campo de característica $p \neq 0$.

TEOREMA 12.35. *Si*

(12.21)

$$\begin{array}{c} K \\ \downarrow \\ \kappa \end{array}$$

es una extensión sobre un campo κ de característica $p \neq 0$, entonces para todo elemento algebraico $\alpha \in K$, existe $e \in \mathbb{N}$, tal que α^{p^e} es separable sobre κ .

DEMOSTRACIÓN. Si $\alpha \in K$ es separable sobre κ , entonces $e = 0$. Supongamos que α no sea separable sobre κ , entonces su polinomio minimal $P \in \kappa[X]$ es un polinomio en X^{p^e} , para algún $e \in \mathbb{N}$ y existe un polinomio $G \in \kappa[Y]$, separable sobre κ , tal que $P = G(X^{p^e})$. Por consiguiente α^{p^e} es separable sobre κ . \square

Decimos que un elemento $\alpha \in K$, donde K es una extensión del campo κ es *inseparable puro*, sobre κ , si existe $e \in \mathbb{N}$, tal que $\alpha^{p^e} \in \kappa$. Éste es el caso cuando α es inseparable y el grado reducido del polinomio minimal P de α sobre κ es 1. Es decir que $P = X^{p^e} - a$, $a \in \kappa$. El siguiente teorema nos dice que esta propiedad caracteriza a los elementos inseparables puros.

TEOREMA 12.36. *Sea κ un campo de característica $p \neq 0$. Si $a \in \kappa$ es tal que no es p -potencia de ningún elemento de κ , entonces $P := X^{p^e} - a$ es irreducible en $\kappa[X]$, para cualquier $e \in \mathbb{N}$.*

DEMOSTRACIÓN. Sea α una raíz de P en alguna extensión K de κ , entonces $\alpha^{p^e} = a$ y, por teorema 11.44, $P = (X - \alpha)^{p^e}$. Si G es un divisor irreducible y mónico de P en $\kappa[X]$, vamos a mostrar que $G = P$. En efecto supongamos que $G = (X - \alpha)^{p^m}$, donde $m \in \mathbb{N}$, $0 \leq m \leq e$, entonces $G = X^{p^m} - \alpha^{p^m} \in \kappa[X]$, entonces $\alpha^{p^m} \in \kappa$ y $(\alpha^{p^m})^{p^{e-m}} = \alpha^{p^e} = a$, entonces $m = e$, pues de lo contrario a sería una p^{e-m} -potencia de un elemento de κ , lo cual no puede ser, por la hipótesis sobre a . Por lo tanto $\text{grad } G = \text{grad } P$ y $P = G$. Por consiguiente P es irreducible en $\kappa[X]$. \square

Como consecuencia del teorema 12.36, se tiene el siguiente

COROLARIO 12.37. *Si el elemento $\alpha \in K$, donde*

$$\begin{array}{c} K \\ | \\ \kappa \end{array}$$

es una extensión del campo κ , de característica $p \neq 0$, es inseparable puro sobre κ , entonces el polinomio minimal de α sobre κ es $X^{p^e} - \alpha^{p^e}$, donde e es el menor número natural, tal que $\alpha^{p^e} \in \kappa$.

DEMOSTRACIÓN. El caso $e = 0$ es trivial, ya que si $\alpha \in \kappa$, entonces $X - \alpha$ es el polinomio minimal. Sea entonces $e > 0$ y $a := \alpha^{p^e}$ y consideremos el polinomio $P := X^{p^e} - a$. Entonces por el teorema 12.36, P es irreducible en $\kappa[X]$ si a no es p -potencia de algún elemento en κ . Supongamos que existe $b \in \kappa$, tal que $b^p = a$, entonces $b^p = a = \alpha^{p^e} = (\alpha^{p^{e-1}})^p$, lo que implicaría que $b = \alpha^{p^{e-1}}$, ya que la aplicación $x \mapsto x^p$ es inyectiva en E . De aquí resultaría que $\alpha^{p^{e-1}} \in \kappa$, en contradicción a la minimalidad de e . Por lo tanto P es irreducible y es el polinomio minimal de α en κ . \square

El concepto de separable no es contradictorio con el de inseparable puro, como nos lo dice el siguiente ejercicio:

EJERCICIO 1. *Mostrar que $\alpha \in K$, donde*

$$\begin{array}{c} K \\ | \\ \kappa \end{array}$$

es una extensión sobre el campo κ de característica $p \neq 0$ es separable e inseparable puro, Ssi $\alpha \in \kappa$.

Cabe preguntarse ¿Qué relación existe entre una extensión inseparable pura y elemento inseparable puro? La respuesta nos la da el siguiente

TEOREMA 12.38. *Una extensión*

(12.22)

$$\begin{array}{c} K \\ | \\ \kappa \end{array}$$

es inseparable pura, Ssi cada elemento de K es inseparable puro sobre κ .

DEMOSTRACIÓN. Supongamos que la extensión (12.22), es inseparable pura sobre κ y $\alpha \in K$. Entonces existe, por teorema 12.35, $e \in \mathbb{N}$, tal que α^{p^e} es separable, y, por hipótesis de inseparabilidad pura $\alpha^{p^e} \in \kappa$. Por lo tanto α es inseparable puro.

Por otra parte, si cada elemento de K es inseparable puro, entonces los elementos de $K \setminus \kappa$ son todos inseparables y por consiguiente la extensión (12.22), es inseparable pura. \square

COROLARIO 12.39. Si

$$\begin{array}{c} K \\ \downarrow \\ \kappa \end{array}$$

es una extensión finita, inseparable pura, sobre el campo κ de característica $p \neq 0$, entonces $[K : \kappa]$ es una potencia de p .

DEMOSTRACIÓN. Si $\alpha \in K$ es inseparable puro, y $K = \kappa(\alpha)$, entonces su polinomio minimal es de la forma $P = X^{p^e} - a$ y $[\kappa(\alpha) : \kappa] = p^e$. Supongamos ahora que $K = \kappa(\alpha_1, \dots, \alpha_n)$. Entonces para cada v , $a \leq v \leq n$, el elemento α_v es inseparable puro sobre $\kappa(\alpha_1, \dots, \alpha_{v-1})$ y por consiguiente la extensión $\kappa(\alpha_1, \dots, \alpha_v)$ es inseparable pura sobre $\kappa(\alpha_1, \dots, \alpha_{v-1})$. Entonces las extensiones

$$\begin{array}{ccccccc} \kappa(\alpha_1) & \kappa(\alpha_1, \alpha_2) & \dots & \kappa(\alpha_1, \dots, \alpha_n) \\ \downarrow & \downarrow & & \downarrow \\ \kappa & \kappa(\alpha_1) & & \kappa(\alpha_1, \dots, \alpha_{n-1}) \end{array}$$

son todas extensiones inseparables puras y su grado es respectivamente una potencia de p , en cada caso. Por lo tanto $[K : \kappa] = [\kappa(\alpha_1, \dots, \alpha_n) : \kappa]$ es una potencia de p . \square

Dado un campo cualquiera K de característica $p \neq 0$, denotamos por K^p al conjunto

$$K^p := \{x^p \mid x \in K\}.$$

Es decir que K^p es la imagen de K bajo el homomorfismo de campos

$$\varphi : K \rightarrow K,$$

tal que $\varphi(x) := x^p$, $\forall x \in K$.

TEOREMA 12.40. Si

$$\begin{array}{c} K \\ \downarrow \\ \kappa \end{array}$$

es una extensión separable sobre el campo κ de característica $p \neq 0$, entonces $\kappa(K^p) = K$. Por otra parte, si $\kappa(K^p) = K$ y $[K : \kappa] < \infty$, entonces K es separable sobre κ .

DEMOSTRACIÓN. Si K es separable sobre κ , y $\alpha \in K$, entonces, como $\alpha^p \in K^p$, α es inseparable puro sobre $\kappa(K^p)$. Por otra parte, si α es separable sobre κ , lo es también, por ejercicio 12.1.7, 3, sobre el campo intermedio $\kappa(K^p)$ y por el ejercicio 1, $\alpha \in \kappa(K^p)$. Por consiguiente $\kappa(K^p) = K$.

Para mostrar la segunda parte utilizaremos el hecho que, si $\alpha_1, \dots, \alpha_n$ son κ -linealmente independientes, también lo son $\alpha_1^p, \dots, \alpha_n^p$. (Ver ejercicio 2 abajo).

Supongamos que $\alpha \in K$ no sea separable sobre κ . Entonces su polinomio minimal P sobre κ no es separable y es un polinomio en X^p , de la forma

$$P := \sum_{\mu=0}^m a_\mu X^{\mu p}, \quad m \geq 1, \quad \text{grad } P = mp.$$

Como

$$0 = P(\alpha) = \sum_{\mu=0}^m a_\mu \alpha^{\mu p},$$

resulta, entonces, que los elementos $1, \alpha, \alpha^p, \dots, \alpha^{mp}$ son κ -linealmente dependientes, lo cual es una contradicción al hecho que los elementos $1, \alpha, \dots, \alpha^m$, son κ -linealmente independientes, ya que $m < \text{grad } P = [\kappa(\alpha) : \kappa]$. Por lo tanto α es separable sobre κ . \square

EJERCICIO 2. *Probar que si κ es un campo de característica $p \neq 0$ y K una extensión finita de κ , tal que $\kappa(K^p) = K$, entonces*

$\alpha_1, \dots, \alpha_n \in K$ κ -linealmente independientes $\Rightarrow \alpha_1^p, \dots, \alpha_m^p$ κ -linealmente independiente, donde $1 \leq m \leq n := [K : \kappa]$.

(Ayuda: Si $m < n$ completar $\alpha_1, \dots, \alpha_m$ a una base $\alpha_1, \dots, \alpha_n$. Notar que $\alpha_1^p, \dots, \alpha_n^p$ generan $\kappa[K^p] = \kappa(K^p) = K$ y que todo elemento de K es combinación lineal de los elementos $\alpha_1^p, \dots, \alpha_n^p$).

TEOREMA 12.41. *Sea*

$$\begin{array}{c} K \\ | \\ \kappa \end{array}$$

una extensión del campo κ de característica $p \neq 0$. Las siguientes condiciones son equivalentes:

- a) $\alpha \in K$ es separable sobre κ .
- b) $\kappa(\alpha) = \kappa(\alpha^p)$.
- c) $\kappa(\alpha)$ es separable sobre κ .

DEMOSTRACIÓN.

- a) \Rightarrow b) Si α es separable sobre κ , entonces también sobre $\kappa(\alpha^p)$. Por otra parte α es inseparable puro sobre $\kappa(\alpha^p)$, por consiguiente $\alpha \in \kappa(\alpha^p)$ y $\kappa(\alpha^p) = \kappa(\alpha)$.
- b) \Rightarrow c) Sea $E := \kappa(\alpha)$. Por b) $E = \kappa(\alpha^p) = \kappa(E^p)$, además $[E : \kappa] = \text{grad } P_\alpha$, donde $P_\alpha < \infty$ es el polinomio minimal de α sobre κ . Entonces, por teorema 12.40, E es separable sobre κ .
- c) \Rightarrow a) Obvio de la definición.

\square

TEOREMA 12.42. *Sea E un campo intermedio de la extensión*

$$\begin{array}{c} K \\ | \\ \kappa \end{array}$$

sobre el campo κ de característica $p \neq 0$. E separable sobre κ . Si $\alpha \in E$ es separable sobre E , entonces α es separable sobre κ .

DEMOSTRACIÓN. Sea

$$P := \sum_{v=0}^n a_v X^v$$

el polinomio minimal de α sobre E y $E_0 := \kappa(a_0, \dots, a_n)$. Entonces, como $E_0 \subseteq E$, E_0 es separable sobre κ . Sea $E_1 := E_0(\alpha)$. Como α separable sobre E_0 , entonces $E_1 = E_0(E_1^p)$.

Como E_0 separable sobre κ , se tiene $E_0 = \kappa(E_0^p)$. Entonces $E_1 = E_0(E_1^p) = \kappa(E_0^p)(E_1^p) = \kappa(E_0^p \cup E_1^p) = \kappa(E_1^p)$. Como $[E_1 : \kappa] < \infty$, resulta, entonces, que α es separable sobre κ . \square

Como consecuencia inmediata del teorema 12.42 se obtiene el siguiente

COROLARIO 12.43. *Si*

$$\begin{array}{ccc} K & & E \\ | & & | \\ E & & \kappa \end{array}$$

son extensiones separables, entonces

$$\begin{array}{c} K \\ | \\ \kappa \end{array}$$

es separable.

12.1.9. Envoltorio Separable y Grado de Separabilidad. Dada una extensión

$$\begin{array}{c} K \\ | \\ \kappa \end{array}$$

al conjunto

$$H_s(K : \kappa) := \{x \in K \mid x \text{ separable sobre } \kappa\}$$

lo llamamos la *envoltorio separable* de κ en K .

Las propiedades esenciales de la envoltorio separable las resumimos en el siguiente teorema, cuya sencilla demostración dejamos al lector, como un ejercicio.

TEOREMA 12.44. *Sea*

(12.23)

$$\begin{array}{c} K \\ | \\ \kappa \end{array}$$

una extensión del campo κ . Entonces

- a) $H_s(K : \kappa)$ es un campo intermedio de la extensión (12.23).
- b) $H_s(K : H_s(K : \kappa)) = H_s(K : \kappa)$
- c) $H_s(K : \kappa) \subseteq H_a(K : \kappa)$ y $H_a(K : \kappa)$ es una extensión inseparable pura sobre κ .

Como consecuencia del teorema 12.44, se tiene la siguiente cadena de inclusiones

(12.24)

$$\kappa \subseteq H_s(K : \kappa) \subseteq H_a(K : \kappa) \subseteq K.$$

A $[H_s(K : \kappa) : \kappa]$ lo llamamos el *grado de separabilidad* de K sobre κ , al cual denotaremos por $[K : \kappa]_s$.

De forma análoga a $[K : H_s(K : \kappa)]$ lo llamamos el *grado de inseparabilidad* de K sobre κ y lo denotaremos por $[K : \kappa]_i$.

Si la extensión

$$\begin{array}{c} K \\ | \\ \kappa \end{array}$$

es finita, obviamente vale que $[K : \kappa] = [K : \kappa]_s [K : \kappa]_i$.

Si κ es de característica 0, entonces $H_s(K : \kappa) = H_a(K : \kappa)$.

TEOREMA 12.45. Si

(12.25)

$$\begin{array}{c} K \\ \downarrow \\ \kappa \end{array}$$

es una extensión algebraica simple, con elemento primitivo α , del campo κ de característica $p \neq 0$, entonces:

- a) $[K : \kappa]_s = m$, donde m es el grado reducido del polinomio minimal P de α sobre κ
- b) $[K : \kappa]_i = p^e$, si $\text{grad } P = mp^e$.

DEMOSTRACIÓN. Como α es elemento primitivo de la extensión (12.25), su polinomio minimal es de la forma $P = G(X^{p^e})$, donde $G \in \kappa[Y]$ es un polinomio mónico, separable e irreducible en $\kappa[Y]$. Si $\beta := \alpha^{p^e}$, entonces G es el polinomio minimal de β sobre κ y $\text{grad } P = \text{grad } G = [\kappa(\beta) : \kappa]$. Basta mostrar que $H_s(K : \kappa) = \kappa(\beta)$. Como G es separable sobre κ , entonces $\kappa(\beta) \subseteq H_s(K : \kappa)$. Para mostrar la otra inclusión, basta mostrar que K es inseparable puro sobre $\kappa(\beta)$.

Sea $\gamma \in K = \kappa(\alpha)$, entonces existen elementos $a_0, \dots, a_n \in \kappa$, tales que

$$\gamma := \sum_{\nu=0}^n a_\nu \alpha^\nu, \quad n := \text{grad } P - 1,$$

y

$$\gamma^{p^e} := \sum_{\nu=0}^n a_\nu^{p^e} \alpha^{\nu p^e} = \sum_{\nu=0}^n a_\nu^{p^e} \beta^\nu \in \kappa(\beta).$$

Entonces de $[E : \kappa] = \text{grad } P = \text{grad } G \cdot p^e = [E : \kappa]_s [E : \kappa]_i$, resulta lo deseado. \square

TEOREMA 12.46. Una extensión finita

(12.26)

$$\begin{array}{c} K \\ \downarrow \\ \kappa \end{array}$$

sobre un campo κ de característica $p \neq 0$ es campo de descomposición de un polinomio separable en $\kappa[X]$. Si K es normal y separable sobre κ .

DEMOSTRACIÓN. Si K es campo de descomposición de un polinomio separable P sobre κ , entonces la extensión (12.26) es normal sobre κ . Si $\alpha_1, \dots, \alpha_n$ son las raíces de P , $K = \kappa(\alpha_1, \dots, \alpha_n)$ y el polinomio minimal P_ν de cada α_ν , $\nu = 1, \dots, n$, como factor irreducible de P es separable sobre κ . Por lo tanto la extensión (12.26), es también separable sobre κ .

Por otra parte, si la extensión (12.26) es normal y separable sobre κ , entonces K es campo de descomposición de un polinomio $P \in \kappa[X]$. Si G es un factor irreducible de P en $\kappa[X]$, entonces también G se descompone en factores lineales en $K[X]$ y G es el polinomio minimal de un elemento separable sobre κ . Por lo tanto G es separable. \square

Como en característica 0 $H_s(K : \kappa) = H_a(K : \kappa)$, el grado de separabilidad $[K : \kappa]_s$, coincide con el grado algebraico $[K : \kappa]_a$ de la extensión. El resultado que demostraremos a continuación y que constituye un pilar fundamental para la teoría de Galois, es válido para cualquier característica.

TEOREMA 12.47. *Si E es un campo intermedio de la extensión normal y finita*

$$\begin{array}{c} K \\ \downarrow \\ \kappa \end{array}$$

entonces existen tantos κ -homomorfismos distintos de E en K , como $[E : \kappa]_s$.

DEMOSTRACIÓN. Sean $E_s := H_s(E : \kappa)$, $M := \text{hom}_\kappa(E, K)$ y $M_s := \text{hom}_\kappa(E_s, E)$. Sea

$$\tau : M \rightarrow M_s$$

la aplicación definida por $\tau(\varphi) := \varphi|_{E_s}$.

τ es inyectiva: Si $\text{car } \kappa = 0$, entonces $E_s = E$ y no hay nada que mostrar. Sea entonces $\text{car } \kappa = p \neq 0$, $\varphi \in M$ y $\alpha \in E$. Entonces existe $e \in \mathbb{N}$, tal que $\beta := \alpha^{p^e}$ es separable sobre κ , es decir $\beta \in E_s$. De $\varphi(\beta) = \varphi(\alpha^{p^e}) = (\varphi(\alpha))^{p^e}$, resulta que $\varphi(\alpha)$ es raíz del polinomio $P := X^{p^e} - \varphi(\beta) = (X^{p^e} - (\varphi(\alpha)))^{p^e} = (X - \varphi(\alpha))^{p^e} \in K[X]$. Si τ no fuera inyectiva, entonces existiría $\psi \in M$, $\psi \neq \varphi$, tal que $\varphi|_{E_s} = \psi|_{E_s}$. Tomando $\alpha \in E$, tal que $\psi(\alpha) \neq \varphi(\alpha)$, tendríamos que $\psi(\alpha)$ sería también raíz de $(X - \varphi(\alpha))^{p^e}$, lo cual no es posible. Por consiguiente τ es inyectiva.

τ es sobreyectiva: Sea $\varphi \in M_s$, entonces, por teorema 12.30, φ posee una extensión

$$\hat{\varphi} : E \rightarrow K$$

y $\tau(\hat{\varphi}) = \varphi$.

Entonces, por la biyectividad de τ , basta mostrar el teorema para $E = E_s$. Entonces E es una extensión finita y separable, y, por teorema 12.33, E es una extensión simple y existe un elemento primitivo $\gamma \in E$, tal que $E = \kappa(\gamma)$ y tal que su polinomio minimal P es separable sobre κ . Como K es normal sobre κ y P posee una raíz en K , entonces P posee todas sus raíces en K . Sean éstas $\gamma = \gamma_1, \dots, \gamma_m$. Para cada $1 \leq \mu \leq m := \text{grad } P$, existe un κ -homomorfismo

$$\varphi_\mu : \kappa(\gamma) \rightarrow \kappa_{\gamma_\mu},$$

tal que $\varphi(\gamma) := \gamma_\mu$. Por lo que M contiene, como mínimo, a estos m homomorfismos. Si $\psi \in M$ es otro κ -homomorfismo, entonces $\psi(\gamma)$ es raíz de P , es decir $\psi(\gamma) = \gamma_\mu$, para algún μ , $1 \leq \mu \leq m$, por lo que $\psi = \varphi_\mu$. Por lo tanto M posee exactamente

$$m = \text{grad } P = [\kappa(\gamma) : \kappa] = [E : \kappa] = [E : \kappa]_s$$

elementos. □

12.2. Teoría de Galois

La teoría de Galois estudia la solubilidad de una ecuación polinómica, por medio de radicaciones sucesivas, a partir del estudio de un cierto grupo de permutaciones de sus raíces, llamado el grupo de Galois. La solubilidad de la ecuación polinómica, como se demuestra en dicha teoría, está íntimamente relacionada con la solubilidad de su grupo de Galois correspondiente. El trabajo de Galois no fue reconocido que hasta después de su muerte prematura, a raíz de un duelo. En su lecho de muerte encarga a su hermano Alfredo y a su amigo matemático Auguste Chevallier solicitar, públicamente, la opinión de Gauss y de Jacobi sobre su trabajo, ya que durante su vida nunca logró que Augustin Cauchy se interesara por su trabajo. Chevallier se encarga de recopilar su obra y la presenta al matemático francés Joseph Liouville, quien reconoce la importancia de su trabajo y presenta sus principales resultados ante la Academia de Ciencias de Francia y los publica en la revista *Journal de Mathématiques pures et Appliquées*, que él dirigía.



FIGURA 12.1. Évariste Galois

Abel había demostrado la imposibilidad de solucionar, por medio de radicación, la ecuación polinómica general de quinto grado. Sin embargo con la teoría de Galois fue posible demostrar que la ecuación polinómica general de grado $n > 4$ no es soluble por dicho método e incluso determinar en qué casos sí lo es.

12.2.1. Grupo de Galois de una Extensión. Nuestro objetivo es asociar a una extensión de campos

$$\begin{array}{c} K \\ \downarrow \\ K \end{array}$$

un grupo y estudiar las propiedades de la extensión en función de las propiedades del grupo asociado.

Dada una extensión

$$\begin{array}{c} K \\ \downarrow \\ K \end{array}$$

se construirá una biyección entre un subconjunto del conjunto de subcampos de K y el conjunto de subgrupos finitos de $\text{Aut}_K K$. Si E es un subcampo de K , a la extensión

$$\begin{array}{c} K \\ \downarrow \\ E \end{array}$$

se le asocia el grupo $\mathfrak{G}(K : E) := \text{Aut}_E K$, llamado el *grupo de Galois* de la extensión

$$\begin{array}{c} K \\ \downarrow \\ K \end{array}$$

Si K es un campo y H un subgrupo de $\text{Aut } K$, definimos

$$\text{Fix } H := \{x \in K \mid \varphi(x) = x, \forall \varphi \in H\}$$

$\text{Fix } H$ es un subcampo de K (ejercicio), llamado el *campo fijo* del subgrupo H .

Sean

$$\mathcal{T}(K) := \{E \subseteq K \mid E \text{ subcampo de } K\}, \quad \mathcal{U}(K) := \{H \subseteq \text{Aut } K \mid H \text{ subgrupo de } \text{Aut } K\}$$

y las aplicaciones

$$\Phi : \mathcal{T}(K) \rightarrow \mathcal{U}(K), \quad \Psi : \mathcal{U}(K) \rightarrow \mathcal{T}(K)$$

definidas por $\Phi(E) := \mathfrak{G}(K : E)$ y $\Psi(H) := \text{Fix } H$, cuyas propiedades esenciales se resumen en el siguiente teorema, cuya demostración dejamos al lector, como un ejercicio:

TEOREMA 12.48. *Dados $E, E_1, E_2 \in \mathcal{T}(K)$ y $H, H_1, H_2 \in \mathcal{U}(K)$. Entonces vale:*

1. $E_1 \subseteq E_2 \Rightarrow \Phi(E_2) \subseteq \Phi(E_1)$.
2. $H_1 \subseteq H_2 \Rightarrow \Psi(H_2) \subseteq \Psi(H_1)$.
3. $(\Psi \circ \Phi)(E) = \text{Fix } \mathfrak{G}(K : E) \supseteq E$ y $(\Phi \circ \Psi)(H) = \mathfrak{G}(K : \text{Fix } H) \supseteq H$.

TEOREMA 12.49. *Sea*

$$\begin{array}{c} K \\ | \\ \kappa \end{array}$$

una extensión finita, entonces $\circ(\mathfrak{G}(K : \kappa)) \leq [K : \kappa]_s \leq [K : \kappa]$. Si K es normal sobre κ , entonces $\circ(\mathfrak{G}(K : \kappa)) = [K : \kappa]$.

DEMOSTRACIÓN. Como K es una extensión finita sobre κ , entonces, por teorema 12.29, existe una extensión \tilde{K} de K , tal que la extensión

$$\begin{array}{c} \tilde{K} \\ | \\ \kappa \end{array}$$

es normal y finita y, por teorema 12.47, el número de κ -homomorfismos distintos de K en \tilde{K} es igual a $[K : \kappa]_s$. Entonces como todo elemento de $\mathfrak{G}(K : \kappa)$ puede ser visto como un κ -homomorfismo de K en \tilde{K} , resulta la primera afirmación.

Respecto de la segunda: Si K es normal sobre κ , podemos tomar $\tilde{K} = K$ y todo κ -homomorfismo de K en K es un κ -automorfismo. Por lo tanto $\circ(\mathfrak{G}(K : \kappa)) = [K : \kappa]_s$. \square

Consideremos ahora los siguientes subconjuntos:

$$\mathcal{T}_0(K) := \{E \in \mathcal{T}(K) \mid [K : E] < \infty\}, \quad \mathcal{U}_0(K) := \{H \in \mathcal{U}(K) \mid \circ(H) < \infty\}.$$

TEOREMA 12.50 (Teorema de Artin). *Sean K un campo y $H \in \mathcal{U}_0(K)$. Entonces la extensión*

$$\begin{array}{c} K \\ | \\ \text{Fix } H \end{array}$$

es normal y separable. Además $[K : \text{Fix } H] = \circ(H)$. Es decir que $\Psi[\mathcal{U}_0(K)] \subseteq \mathcal{T}_0(K)$.

DEMOSTRACIÓN. Desarrollaremos, para su mejor comprensión, la demostración en las siguientes dos partes:

- a) $x \in K$ separable sobre $\text{Fix } H$, $\forall x \in K$. $[(\text{Fix } H)(x) : \text{Fix } H] \leq \circ(H)$ y la extensión

(12.27)

$$\begin{array}{c} K \\ | \\ \text{Fix } H \end{array}$$

es normal.

- b) $[K : \text{Fix } H] \leq \circ(H)$ y $[K : \text{Fix } H] \geq \circ(H)$.

Procedamos, pues a la demostración:

- a) Dado $x \in K$, definimos el conjunto

$$M := \{\varphi(x) \mid \varphi \in H\}.$$

Como H es finito, M lo es también y denotemos sus elementos por x_1, \dots, x_n , donde $n \leq \circ(H)$. $x \in M$, ya que $1_K \in H$. Para cualquier $\psi \in H$, $\psi|_M$ es una permutación sobre M . En efecto, ψ es inyectiva, ya que ψ es un automorfismo

sobre K . Dado $x_\nu \in M$, $\nu = 1, \dots, n$, existe un $\varphi_\nu \in H$, tal que $x_\nu = \varphi_\nu(x)$. Entonces $\psi(x_\nu) = \psi(\varphi_\nu(x)) = (\psi \circ \varphi_\nu)(x) \in M$, ya que $(\psi \circ \varphi) \in H$. Es decir que $\psi|_M$ es una aplicación inyectiva

$$\psi|_M : M \rightarrow M.$$

$\psi|_M$ es sobreyectiva: Dado $x_\nu \in M$, como $\psi \in H \Rightarrow \psi^{-1} \in H$ y $\psi^{-1}(x_\nu) = (\psi^{-1} \circ \varphi_\nu)(x) \in M$, entonces $x_\nu = \psi(\psi^{-1}(x_\nu))$. Por lo tanto $\psi|_M$ es sobreyectiva.

Consideremos ahora el polinomio

$$P := \prod_{\nu=1}^n (X - x_\nu) = \sum_{\nu=0}^n a_\nu X^\nu \in K[X].$$

Entonces P es separable en $K[X]$, pues todas sus raíces son simples. x es raíz de P y P se transforma por φ_* inducido por un $\varphi \in H$ en el polinomio

$$\varphi_*(P) = \sum_{\nu=0}^n \varphi(a_\nu) X^\nu = \prod_{\nu=1}^n (X - \varphi(x_\nu)) = \prod_{y \in M} (X - y) = \sum_{\nu=0}^n a_\nu X^\nu.$$

Entonces $\varphi(a_\nu) = a_\nu$, $a_\nu \in \text{Fix } H$, $\forall \nu = 1, \dots, n$ y $P \in (\text{Fix } H)[X]$. Como $P \in (\text{Fix } H)[X]$ separable, entonces x separable sobre $\text{Fix } H$, ya que es raíz de un polinomio en $(\text{Fix } H)[X]$ separable.

Entonces K resulta ser la unión de campos de descomposición de polinomios sobre $\text{Fix } H$, por lo que, por teorema 12.32teo:normnofin, la extensión (12.27) es normal. Si P_x es el polinomio minimal de x en $(\text{Fix } H)[X]$, entonces $P_x \mid P$ y $[(\text{Fix } H)(x) : \text{Fix } H] = \text{grad } P_x \leq \text{grad } P = n \leq \text{o}(H)$.

- b) Supongamos que $[K : \text{Fix } H] > \text{o}(H)$, entonces, por adjunción de elementos, podemos formar un campo intermedio $E \subseteq K$, tal que E separable y finito sobre $\text{Fix } H$ y $[E : \text{Fix } H] > \text{o}(H)$. Entonces por teorema 12.33, E es una extensión simple y existe $y \in E$, tal que $E = (\text{Fix } H)(y)$, entonces $[(\text{Fix } H)(y) : \text{Fix } H] > \text{o}(H)$, en contradicción a lo obtenido en a). Por lo tanto debe valer $[K : \text{Fix } H] \leq \text{o}(H)$.

Por otra parte $H \subseteq \mathfrak{G}(K : \text{Fix } H)$ y $\text{o}(H) \leq \text{o}(\mathfrak{G}(K : \text{Fix } H)) \leq [K : \text{Fix } H]$. Por lo tanto $[K : \text{Fix } H] = \text{o}(H)$.

□

Decimos que una extensión

$$\begin{array}{c} K \\ \downarrow \\ E \end{array}$$

es una *extensión de Galois*, si $E \in \text{Im } \Psi$. Es decir, si existe un subgrupo $H \subseteq \text{Aut } K$, tal que $E = \text{Fix } H$.

TEOREMA 12.51. *Las siguientes condiciones son equivalentes para una extensión*

(12.28)

$$\begin{array}{c} K \\ \downarrow \\ E \end{array}$$

- a) la extensión (12.28) es una extensión de Galois
- b) $(\Psi \circ \Phi)(E) = \text{Fix } \mathfrak{G}(K : E) = E$.
- c) $\forall x \in K \setminus E, \exists \varphi \in \mathfrak{G}(K : E)$, tal que $\varphi(x) \neq x$.

DEMOSTRACIÓN. a) \Rightarrow b) Como, por hipótesis, la extensión (12.28) es de Galois, existe $H \in \mathcal{U}(K)$, tal que $E = \Psi(H)$. Del teorema 12.48 tenemos $\Phi(E) = \Phi(\Psi(H)) \supseteq H$ y $\Psi(\Phi(E)) \subseteq \Psi(H) = E$. Por otra parte vale $E \subseteq \Psi(\Phi(E))$.

b) \Rightarrow a) Por definición

b) \Rightarrow c) Obvio.

c) \Rightarrow b) Si c) vale, entonces $\text{Fix } \mathfrak{G}(K : E) \subseteq E$, pero $E \subseteq \text{Fix } \mathfrak{G}(K : E)$, por consiguiente $\Psi(\Phi(E)) = E$.

□

Para el caso de extensiones finitas, las extensiones de Galois se pueden caracterizar de la siguiente forma:

TEOREMA 12.52. *Las siguientes condiciones son equivalentes en una extensión finita*

(12.29)

$$\begin{array}{c} K \\ \downarrow \\ E \end{array}$$

- a) La extensión (12.29) es de Galois.
- b) La extensión (12.29) es normal y separable
- c) $\circ(\mathfrak{G}(K : E)) = [K : E]$.

DEMOSTRACIÓN. a) \Rightarrow b) Como la extensión (12.29) es finita, $\circ(\mathfrak{G}(K : E)) = [K : E]_s \leq [K : E] < \infty$, por lo que $\mathfrak{G}(K : E) \in \mathcal{U}_0(K)$. Como, por hipótesis, la extensión (12.29) es de Galois, $E = \text{Fix } \mathfrak{G}(K : E)$ y por el teorema de Artin (12.29) es normal y separable.

b) \Rightarrow c) Como la extensión (12.29) es normal y finita, vale que $\circ(\mathfrak{G}(K : E)) = [K : E]_s = [K : E]$, ya que (12.29) es separable.

c) \Rightarrow a) $E \subseteq \text{Fix } \mathfrak{G}(K : E) \subseteq K$, entonces

$$[K : E] = [K : \text{Fix } \mathfrak{G}(K : E)][\text{Fix } \mathfrak{G}(K : E) : E] = \circ(\mathfrak{G}(K : E)) = [K : \text{Fix } \mathfrak{G}(K : E)] \text{ (por Artin).}$$

Entonces $[\text{Fix } \mathfrak{G}(K : E) : E] = 1$, lo que implica que $\text{Fix } \mathfrak{G}(K : E) = E$.

□

Del teorema de Artin y del teorema 12.52 podemos deducir los siguientes resultados: Si $H \in \mathcal{U}_0$, entonces, por Artin, la extensión

$$\begin{array}{c} K \\ \downarrow \\ \text{Fix } H \end{array}$$

es normal, separable y finita, ya que $[K : \text{Fix } H] = \circ(H) < \infty$, y por consiguiente de Galois.

Si

$$\mathcal{T}_*(K) := \{E \in \mathcal{T}_0(K) \mid K \text{ es de Galois sobre } E\},$$

entonces $\Psi[\mathcal{U}_0(K)] \subseteq \mathcal{T}_*(K)$.

Por otra parte si $E \in \mathcal{T}_*(K)$, entonces $E \in \Psi[\mathcal{U}_0(K)]$, por lo que $\mathcal{T}_*(K) = \Psi[\mathcal{U}_0(K)]$.

Además se tiene que $\Phi(E) = \mathfrak{G}(K : E) \in \mathcal{U}_0(K)$.

Esto nos lleva al siguiente teorema, que es considerado el teorema principal de Galois:

TEOREMA 12.53 (Teorema Principal de Galois). *Sea K un campo. Entonces las aplicaciones*

$$\Phi|_{\mathcal{T}_*(K)} : \mathcal{T}_*(K) \rightarrow \mathcal{U}_0(K) \quad \text{y} \quad \Psi|_{\mathcal{U}_0(K)} : \mathcal{U}_0(K) \rightarrow \mathcal{T}_*(K)$$

son biyectivas e inversas la una de la otra.

DEMOSTRACIÓN. Debemos mostar que :

- a) Sobre $\mathcal{T}_*(K)$, $\Psi \circ \Phi = 1_{\mathcal{T}_*(K)}$.
- b) Sobre $\mathcal{U}_0(K)$, $\Phi \circ \Psi = 1_{\mathcal{U}_0(K)}$.
- a) Ya fue mostrado, pues si la extensión

$$\begin{array}{c} K \\ \downarrow \\ E \end{array}$$

es de Galois, $\Psi(\Phi(E)) = E$, por consiguiente, para todo $E \in \mathcal{T}_*(K)$, Ψ es la inversa de $\Phi|_{\mathcal{T}_*(K)}$.

- b) Sea $H \in \mathcal{U}_0(K)$, entonces $H \subseteq \Phi(\Psi(H)) = \mathfrak{G}(K : \text{Fix } H)$. Si mostramos que $\circ(\mathfrak{G}(K : \text{Fix } H)) \leq \circ(H)$, estamos listos.

Por el teorema de Artin $\circ(H) = [K : \text{Fix } H] \geq [E : \text{Fix } H]_s = \circ(\mathfrak{G}(K : \text{Fix } H))$. Lo que muestra el teorema.

□

Del teorema principal de Galois resulta, de forma inmediata, el siguiente

COROLARIO 12.54. *Sean $E_1, E_2 \in \mathcal{T}_*(K)$. Entonces*

$$E_1 \subseteq E_2, \quad \text{Ssi} \quad \mathfrak{G}(K : E_2) \subseteq \mathfrak{G}(K : E_1).$$

Si un campo F es obtenido de un campo $E \in \mathcal{T}_*(K)$, como imagen de un automorfismo $\varphi \in \text{Aut } K$, la relación que existe entre sus grupos de Galois correspondientes, nos lo da el siguiente

TEOREMA 12.55. *Sean $E \in \mathcal{T}_*(K)$ y $\varphi \in \text{Aut } K$. Entonces $\varphi[E] \in \mathcal{T}_*(K)$ y $\mathfrak{G}(K : \varphi[E]) = \varphi \mathfrak{G}(K : E)\varphi^{-1}$. Es decir los grupos de Galois de E y $\varphi[E]$ son conjugados respecto de φ .*

DEMOSTRACIÓN.

$$\begin{aligned} \varphi[E] &= \varphi[\text{Fix } \mathfrak{G}(K : E)] = \{\varphi(x) \mid x \in K \text{ y } \psi(x) = x, \forall \psi \in \mathfrak{G}(K : E)\} \\ &= \{y \mid y \in K \text{ y } (\varphi\psi\varphi^{-1})(y) = y, \forall \psi \in \mathfrak{G}(K : E)\} = \text{Fix } \varphi \mathfrak{G}(K : E)\varphi^{-1}. \end{aligned}$$

Entonces $\varphi[E] \in \mathcal{T}_*(K)$.

Como $\varphi \mathfrak{G}(K : E)\varphi^{-1} \in \mathcal{U}_0(K)$, entonces

$$\varphi[E] = \text{Fix } \varphi \mathfrak{G}(K : E)\varphi^{-1} = \Psi(\varphi \mathfrak{G}(K : E)\varphi^{-1}) \in \mathcal{T}_*(K)$$

y

$$\mathfrak{G}(K : \varphi[E]) = \Phi(\varphi[E]) = \varphi \mathfrak{G}(K : E)\varphi^{-1}.$$

□

TEOREMA 12.56. *Sean $E_1, E_2 \in \mathcal{T}_*(K)$ y $\varphi \in \text{Aut } K$. Entonces vale:*

- a) $\varphi[E_1] = E_2$, Ssi $\varphi \mathfrak{G}(K : E_1)\varphi^{-1} = \mathfrak{G}(K : E_2)$.
- b) $\varphi[E_1] \subseteq E_2$, Ssi $\mathfrak{G}(K : \varphi[E_2]) \subseteq \mathfrak{G}(K : E_1)$.

DEMOSTRACIÓN.

- a) $E_1 \in \mathcal{T}_*(K)$ implica que $\varphi(E_1) \in \mathcal{T}_*(K)$. Como Φ biyectiva: $\Phi(E_1) = E_2$, Ssi $\mathfrak{G}(K : \varphi(E_1)) = \mathfrak{G}(K : E_2) = \varphi \mathfrak{G}(K : E_1)\varphi^{-1}$.

- b) $\varphi(E_1) \subseteq E_2$, Ssi $\Phi(E_2) \subseteq \Phi(\varphi(E_1))$, Ssi $\mathfrak{G}(K : E_2) \subseteq \mathfrak{G}(K : \varphi(E_1)) = \varphi(\mathfrak{G}(K : E_1)\varphi^{-1})$.

□

Los resultados del teorema principal de Galois se pueden relativizar a campos intermedios.

Si E es un campo intermedio de la extensión

$$\begin{array}{c} K \\ \downarrow \\ \kappa \end{array}$$

entonces $\mathfrak{G}(K : E) \subseteq \mathfrak{G}(K : \kappa)$.

Por otra parte, si $H \subseteq \mathfrak{G}(K : \kappa)$ es un subgrupo, $\text{Fix } H$ es un campo intermedio de la extensión

$$\begin{array}{c} K \\ \downarrow \\ H \\ \downarrow \\ \kappa \end{array}$$

Entonces para los subconjuntos

$$\mathcal{T}(K : \kappa) := \{E \subseteq K \mid E \text{ es un campo intermedio de la extensión } K : \kappa\} \subseteq \mathcal{T}(K)$$

y

$$\mathcal{U}(K : \kappa) := \{H \subseteq \mathfrak{G}(K : \kappa) \mid H \text{ subgrupo}\} \subseteq \mathcal{U}(K)$$

$\Phi(\mathcal{T}(K : \kappa)) \subseteq \mathcal{U}(K : \kappa)$ y $\Psi(\mathcal{U}(K : \kappa)) \subseteq \mathcal{T}(K : \kappa)$ y restringidas a $\mathcal{T}_*(K)$ y a $\mathcal{U}_0(K)$, se obtiene el siguiente

TEOREMA 12.57. *Dada la extensión*

$$\begin{array}{c} K \\ \downarrow \\ \kappa \end{array}$$

entonces las aplicaciones

$$\Phi|_{\mathcal{T}_*(K) \cap \mathcal{T}(K : \kappa)} : \mathcal{T}_*(K) \cap \mathcal{T}(K : \kappa) \rightarrow \mathcal{U}_0(K) \cap \mathcal{U}(K : \kappa)$$

y

$$\Psi|_{\mathcal{U}_0(K) \cap \mathcal{U}(K : \kappa)} : \mathcal{U}_0(K) \cap \mathcal{U}(K : \kappa) \rightarrow \mathcal{T}(K : \kappa) \cap \mathcal{T}_*(K)$$

son biyectivas e inversas la una de la otra.

En el caso de una extensión finita de Galois se obtiene e siguiente

TEOREMA 12.58. *Si E es un campo intermedio de la extensión finita de Galois*

(12.30)

$$\begin{array}{c} K \\ \downarrow \\ \kappa \end{array}$$

entonces la extensión

(12.31)

$$\begin{array}{c} K \\ \downarrow \\ E \end{array}$$

es también una extensión de Galois.

DEMOSTRACIÓN. La extensión (12.30) es, por ser de Galois y finita, normal y separable, entonces también la extensión (12.31) es finita, normal y separable y por lo tanto de Galois. \square

Como consecuencia inmediata a los teorema 12.57 y 12.58, se obtiene el siguiente

COROLARIO 12.59. *Si*

$$\begin{array}{c} K \\ | \\ \kappa \end{array}$$

es una extensión finita de Galois, entonces las restricciones

$$\Phi|_{\mathcal{T}(K:\kappa)} : \mathcal{T}(K:\kappa) \rightarrow \mathcal{U}(K:\kappa) \quad y \quad \Psi|_{\mathcal{U}(K:\kappa)} : \mathcal{U}(K:\kappa) \rightarrow \mathcal{T}(K:\kappa)$$

son biyectivas e inversas la una de la otra.

Esto quiere decir que en una extensión finita de Galois, existe una correspondencia biunívoca entre el conjunto de todos los campos intermedios y el conjunto de todos los subgrupos de $\mathfrak{G}(K:\kappa)$.

Entonces si se tiene una cadena de campos intermedios

$$E_0 := \kappa \subseteq E_1 \subseteq \cdots \subseteq E_n := K$$

se tiene también una cadena de subgrupos

$$\mathfrak{G}_n := \mathbf{e} \subseteq \mathfrak{G}_1 \subseteq \cdots \subseteq \mathfrak{G}_0,$$

donde $\mathfrak{G}_v := \mathfrak{G}(K:E_v)$, $v = 0, \dots, n$ y \mathbf{e} representa al subgrupo trivial de $\text{Aut } K$.

TEOREMA 12.60. *Sea E un campo intermedio de la extensión finita de Galois*

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

Entonces vale:

- a) *La extensión $E : \kappa$ es de Galois, Ssi $\mathfrak{G}(K : E)$ es subgrupo normal de $\mathfrak{G}(K : \kappa)$*
- b) *Si la extensión $E : \kappa$ es de Galois, entonces existe un isomorfismo natural*

$$\psi : \mathfrak{G}(E : \kappa) \rightarrow \mathfrak{G}(K : \kappa) / \mathfrak{G}(K : E)$$

DEMOSTRACIÓN.

- a) Por el teorema 12.26, de normalidad finita, la extensión $E : \kappa$ es normal, Ssi para todo κ -automorfismo $\varphi \in \text{Aut}_\kappa K$, $\varphi[E] \subseteq E$. Como $[K : E] < \infty$, $\varphi[E] \subseteq E$ es equivalente a $\varphi[E] = E$, ya que φ es, entonces, κ -lineal e inyectiva. O sea que $E : \kappa$ es normal, Ssi para todo $\varphi \in \mathfrak{G}(K : \kappa)$ vale:

$$\mathfrak{G}(K : E) = \mathfrak{G}(K : \varphi[E]) = \varphi \mathfrak{G}(K : E) \varphi^{-1},$$

Ssi $\mathfrak{G}(K : E)$ es normal en $\mathfrak{G}(E : \kappa)$.

- b) Si la extensión

$$\begin{array}{c} E \\ | \\ \kappa \end{array}$$

es de Galois, entonces es normal y $\varphi[E] = E$, por lo que $\varphi|_E \in \mathfrak{G}(E : \kappa)$. Dados $\varphi, \psi \in \mathfrak{G}(K : \kappa)$ ($\varphi \circ \psi)|_E = \varphi|_E \circ \psi|_E$, por lo que la restricción induce un homomorfismo

$$\eta : \mathfrak{G}(K : \kappa) \rightarrow \mathfrak{G}(E : \kappa),$$

definido por $\eta(\varphi) := \varphi|_E$, el cual por teorema 12.30, es sobreyectivo de núcleo $\mathfrak{G}(K : E)$, y por el teorema de isomorfía 4.35, η induce un isomorfismo

$$\hat{\eta} : \mathfrak{G}(K : \kappa)/\mathfrak{G}(K : E) \rightarrow \mathfrak{G}(E : \kappa)$$

que hace conmutar al diagrama

$$\begin{array}{ccc} \mathfrak{G}(K : \kappa) & \xrightarrow{\eta} & \mathfrak{G}(E : \kappa) \\ \pi \downarrow & \nearrow \hat{\eta} & \\ \mathfrak{G}(K : \kappa)/\mathfrak{G}(K : E) & & \end{array}$$

Entonces $\psi := \hat{\eta}^{-1}$.

□

OBSERVACIÓN. Si conocemos $\mathfrak{G}(K : E)$ y $\mathfrak{G}(E : \kappa)$, entonces se puede calcular $\mathfrak{G}(K : \kappa)$ de la siguiente forma: se extienden los elementos $\varphi \in \mathfrak{G}(E : \kappa)$ a elementos $\tilde{\varphi} \in \mathfrak{G}(K : \kappa)$, entonces

$$\mathfrak{G}(K : \kappa) = \{\tilde{\varphi} \circ \psi \mid \varphi \in \mathfrak{G}(E : \kappa), \psi \in \mathfrak{G}(K : E)\} = \bigcup_{\varphi \in \mathfrak{G}(E : \kappa)} \tilde{\varphi} \mathfrak{G}(K : E).$$

(Si $\alpha \in \mathfrak{G}(K : \kappa)$, α está en la clase de $\tilde{\alpha}$, donde $\tilde{\alpha}$ es una extensión de $\alpha|_E$ a todo K).

TEOREMA 12.61. *Si*

$$\begin{array}{c} K \\ \downarrow \\ K \end{array}$$

es una extensión finita y separable, entonces, existe una extensión \tilde{K} de K , tal que

$$\begin{array}{c} \tilde{K} \\ \downarrow \\ K \end{array}$$

es una extensión finita de Galois.

DEMOSTRACIÓN. Sean $\alpha_1, \dots, \alpha_n \in K$ separables sobre κ , tales que $E = \kappa(\alpha_1, \dots, \alpha_n)$. Para cada $v, v = 1, \dots, n$, sea $P_v \in \kappa[X]$ el polinomio minimal de α_v sobre κ y $P := P_1 \cdots P_n$. P es separable sobre κ , por ser producto de polinomios separables irreducibles. Si \tilde{K} es el campo de descomposición de P sobre K , entonces \tilde{K} es el campo de descomposición de P sobre κ . Entonces \tilde{K} es finito, normal y separable y, por consiguiente, de Galois. □

OBSERVACIÓN. Si nos interesa encontrar los campos intermedios de una extensión finita y separable

$$\begin{array}{c} K \\ \downarrow \\ K \end{array}$$

entonces nos damos una extensión \tilde{K} de K , tal que

$$\begin{array}{c} \tilde{K} \\ | \\ K \end{array}$$

sea de Galois y los campos intermedios serán, entonces, aquellos campos E que corresponden a los subgrupos de $\mathfrak{G}(\tilde{K} : K)$, que contienen a $\mathfrak{G}(\tilde{K} : K)$.

12.2.2. Teorema Fundamental del Álgebra. Como una aplicación de los resultados obtenidos en este capítulo, vamos a demostrar el famoso teorema de Gauss, conocido como el teorema fundamental del álgebra.

TEOREMA 12.62 (Teorema Fundamental del Álgebra de Gauss). *, El campo de los números complejos \mathbb{C} es algebraicamente cerrado y, por consiguiente, todo polinomio con coeficientes en \mathbb{C} posee una raíz en \mathbb{C} .*

La demostración del teorema fundamental la obtendremos como resultado de tres lemas, de los cuales el primero, el lema de Weierstrass es una consecuencia inmediata del teorema del valor intermedio del cálculo diferencial e integral.

LEMA 12.63 (Weierstrass). *Todo polinomio $P \in \mathbb{R}[X]$ de grado impar, posee, al menos, una raíz real*

DEMOSTRACIÓN. Ver teorema del valor intermedio del cálculo diferencial e integral. \square

LEMA 12.64. *Si $[E : \mathbb{R}]$ es impar, para una extensión E de \mathbb{R} , entonces $E = \mathbb{R}$.*

DEMOSTRACIÓN. Como \mathbb{R} es perfecto y E es algebraica sobre \mathbb{R} , entonces E es separable sobre \mathbb{R} y, por corolario 12.34, E es una extensión simple, por lo que existe un elemento primitivo $\alpha \in E$, tal que $E = \mathbb{R}(\alpha)$. Entonces el polinomio minimal $P \in \mathbb{R}[X]$ de α sobre \mathbb{R} es de grado impar y, por el lema de Weierstrass, posee, al menos, una raíz en \mathbb{R} . Entonces por la irreducibilidad de P en $\mathbb{R}[X]$, P debe ser de grado 1. Por lo tanto $E = \mathbb{R}$. \square

LEMA 12.65. *Si $[E : \mathbb{C}] \leq 2$ para una extensión E de \mathbb{C} , entonces $E = \mathbb{C}$. O sea que $[E : \mathbb{C}] = 2$ no puede ocurrir.*

DEMOSTRACIÓN. Si $[E : \mathbb{C}] \leq 2$, y $\alpha \in E$ es algebraico sobre \mathbb{C} , entonces $\text{grad } P \leq 2$, donde P es el polinomio minimal de α . Para mostrar que $E = \mathbb{C}$ basta mostrar que todo polinomio de la forma $Q := X^2 + pX + q$, donde $p, q \in \mathbb{C}$ posee raíces en \mathbb{C} . Sin limitación de la generalidad podemos asumir que $p = 0$, ya que por medio de la transformación $X \mapsto (X - \frac{p}{2})$, se obtiene un polinomio $Q' = X'^2 - q'$.

En efecto, si $p = 0$, entonces $Q = X^2 + q$. Buscamos $z \in \mathbb{C}$, tal que

$$(12.32) \quad z^2 + q = 0.$$

Dado $q := a + bi \in \mathbb{C}$, y poniendo: $z := x + iy$, la ecuación (12.32) se transforma en la ecuación :

$$(12.33) \quad (x^2 - y^2) + 2xyi + a + bi = 0,$$

la cual nos lleva al sistema de ecuaciones reales:

$$(12.34) \quad x^2 - y^2 + a = 0$$

$$(12.35) \quad 2xy + b = 0$$

de la ecuación (12.35) se obtiene

$$y = \frac{-b}{2x}, \quad x \neq 0$$

substituyendo en la ecuación (12.34) nos da la ecuación

$$(12.36) \quad 4x^4 - 4ax^2 - b^2 = 0,$$

la cual, por medio de la sustitución $u := x^2$, se transforma en

$$(12.37) \quad 4u^2 - 4au - b^2 = 0,$$

cuyas soluciones vienen dadas por

$$(12.38) \quad u_{1,2} = \frac{a \pm \sqrt{a^2 + b^2}}{2}$$

Tanto u_1 , como $-u_2$ son reales positivos, por lo que existen números reales, c, d , tales que

$$c^2 = \frac{a + \sqrt{a^2 + b^2}}{2}, \quad d^2 = \frac{-a + \sqrt{a^2 + b^2}}{2}$$

de donde

$$c^2 - d^2 = a, \quad 4c^2d^2 = b^2.$$

Escogiendo los signos de c, d , de forma tal, para que $b = 2cd$, entonces $z := c + id$ es raíz de Q , ya que

$$z^2 = (c + id)^2 = (c^2 - d^2) + 2cdi = a + ib = q.$$

Entonces, como $\text{grad } Q \leq 2$, Q se descompone en factores lineales en $\mathbb{C}[X]$. \square

Procedamos ahora a la demostración del teorema fundamental del álgebra:

DEMOSTRACIÓN. Vamos a mostrar que se

$$\begin{array}{c} E \\ \downarrow \\ \mathbb{C} \end{array}$$

es una extensión algebraica y finita de \mathbb{C} , entonces $E = \mathbb{C}$.

Sin limitación de la generalidad, podemos asumir que

$$\begin{array}{c} E \\ \downarrow \\ \mathbb{R} \end{array}$$

es una extensión de Galois y que \mathbb{C} es un campo intermedio. Entonces

$$[E : \mathbb{R}] = [E : \mathbb{C}][\mathbb{C} : \mathbb{R}] = 2^{n+1}q,$$

donde $n \in \mathbb{N}$ y q un número impar. Entonces

$$\circ(\mathfrak{G}(E : \mathbb{R})) = [E : \mathbb{R}] = 2^{n+1}q$$

y por los teoremas de Sylow, existe un subgrupo H_0 de $\mathfrak{G}(E : \mathbb{R})$, tal que $\circ(H_2) = 2^{n+1}$. Por el teorema de Artin, se tiene $[E : \text{Fix } H_0] = \circ(H_0)$, por lo que $[\text{Fix } H_0 : \mathbb{R}] = q$, como q es impar, resulta, del lema 12.64, que $\text{Fix } H_0 = \mathbb{R}$ y $q = 1$. Entonces, como $[\mathbb{C} : \mathbb{R}] = 2$

$$[E : \mathbb{R}] = 2^{n+1} = 2[E : \mathbb{C}] \quad y \quad [E : \mathbb{C}] = 2^n.$$

Supongamos que $n \geq 1$. Entonces $\mathfrak{G}(E : \mathbb{C})$ posee un subgrupo H , tal que

$$\circ(H) = 2^{n-1} = [E : \text{Fix } H]$$

y resultaría que $[\text{Fix } H : \mathbb{C}] = 2$, lo cual, por lema 12.65, no es posible. Por lo tanto $n = 0$ y $E = \mathbb{C}$. \square

12.2.3. Cálculo del Grupo de Galois. En general, calcular el grupo de Galois que corresponde a una determinada ecuación polinómica no es tarea sencilla. En esta subsección daremos algunas técnicas que nos permitirán, en casos sencillos, determinar el grupo de Galois.

Si P es un polinomio separable sobre un campo κ , entonces por definición $P := G_1^{m_1} \cdots G_n^{m_n}$, donde, para cada ν , $1 \leq \nu \leq n$, G_ν es separable e irreducible en $\kappa[X]$. Si $l_\nu := \text{grad } G_\nu$ y E_P el campo de descomposición de P , entonces cada G_ν se descompone en E_P en l_ν raíces distintas.

Si M_ν es el conjunto de raíces de G_ν y $\varphi \in \text{Aut}_\kappa E_P$, entonces $\varphi|_{M_\nu}$ es una permutación sobre M_ν . Si $\mu \neq \nu$, entonces $M_\nu \cap M_\mu = \emptyset$, ya que los G_ν son primos relativos entre sí. Si

$$M := \bigcup_{\nu=1}^m M_\nu,$$

entonces M es un conjunto de cardinalidad

$$l := \sum_{\nu=1}^n l_\nu$$

y $\varphi|_M$ sigue siendo una permutación sobre M . Entonces, para cada $\varphi \in \text{Aut}_\kappa E_P$, existe una permutación $\sigma_\varphi \in \mathfrak{S}_l$, tal que $\varphi(\alpha_\lambda) = \alpha_{\sigma_\varphi(\lambda)}$, ($1 \leq \lambda \leq l$, y se tiene, entonces una aplicación

$$\Phi : \mathfrak{G}(E_P : \kappa) \rightarrow \mathfrak{S}_l$$

tal que $\Phi(\varphi) := \sigma_\varphi$.

Dados $\varphi, \psi \in \mathfrak{G}(E_P : \kappa)$, si $\Phi(\varphi) := \sigma$ y $\Phi(\psi) := \tau$, entonces $(\varphi \circ \psi)(\alpha_\lambda) = \varphi(\psi(\alpha_\lambda)) = \varphi(\alpha_{\sigma(\tau(\lambda))}) = \alpha_{\sigma(\sigma \circ \tau)(\lambda)}$, es decir que $\Phi(\varphi \circ \psi) = \Phi(\varphi) \circ \Phi(\psi)$. Entonces Φ es un homomorfismo de grupos. Φ es inyectiva, pues si $\Phi(\varphi)\sigma = \tau = \Phi(\psi)$, entonces φ, ψ coinciden sobre M y por consiguiente sobre $E_P = \kappa(M)$. Si $m = \text{grad } P$, entonces $l \leq m$ y $\mathfrak{S}_l \subseteq \mathfrak{S}_m$ y podemos considerar a Φ , como un homomorfismo

$$\Phi : \mathfrak{G}(E_P : \kappa) \rightarrow \mathfrak{S}_m.$$

Lo arriba expuesto lo podemos resumir en el siguiente

TEOREMA 12.66. *Si $P \in \kappa[X]$ es un polinomio separable de grado m y E_P su campo de descomposición sobre κ , entonces vale:*

- a) *Existe una inyección natural*

$$\Phi : \mathfrak{G}(E_P : \kappa) \rightarrow \mathfrak{S}_m.$$

- b) $[E_P : \kappa] = \circ(\mathfrak{G}(E_P : \kappa)) \mid m! = \circ(\mathfrak{S}_m).$

En general $\mathfrak{G}(E_P : \kappa)$ no es isomorfo a todo el grupo de simetría \mathfrak{S}_m , ya que no todas las raíces de P deben de ser distintas y si lo son, no necesariamente serán conjugadas. Como vimos anteriormente en el teorema 12.25, los κ -homomorfismos mapean raíces conjugadas en raíces conjugadas.

El siguiente teorema nos será de gran utilidad para encontrar explícitamente un campo intermedio de una extensión finita y de Galois.

TEOREMA 12.67. *Dada una extensión finita y de Galois*

$$\begin{array}{c} K \\ \downarrow \\ K \end{array}$$

Si

$$H := \{\varphi_1, \dots, \varphi_n\}$$

es un subgrupo de $\mathfrak{G}(K : \kappa)$ y α un elemento primitivo de la extensión, entonces

$$G := \prod_{v=1}^n (X - \varphi_v(\alpha)) = \sum_{v=0}^n a_v X^v$$

es el polinomio minimal de α sobre el campo intermedio $E := \text{Fix } H$. Por lo que $\text{Fix } H = \kappa(a_0, \dots, a_n)$

DEMOSTRACIÓN. En efecto $G(\alpha) = 0$, ya que para algún v_0 , φ_{v_0} es la identidad. Como

$$[\kappa(\alpha) : E] = [\kappa(\alpha) : \text{Fix } H] = \circ(H) = n = \text{grad } G,$$

basta mostrar que $G \in E[X] = (\text{Fix } H)[X]$. Sea $\varphi \in H$, entonces

$$\varphi_*(G) = \sum_{v=0}^n \varphi(a_v) X^v = \prod_{v=1}^n (X^v - (\varphi \circ \varphi_v)(\alpha)) = \prod_{v=1}^n (X - \varphi_v(\alpha)) = \sum_{v=0}^n a_v X^v$$

ya que $\varphi[H] = H$, para cualquier $\varphi \in H$. Entonces $a_v \in \text{Fix } H$, $\forall v = 0, \dots, n$ y G es el polinomio minimal de α sobre $\text{Fix } H$. \square

EJEMPLO 12.1. Sean $\kappa := \mathbb{Q}(i)$, $PX^4 - 2$. Sea $K := E_P$ el campo de descomposición de P y queremos calcular $\mathfrak{G}(K_P)$:

rac(i) y $\mathcal{T}(K)$. Las raíces de P , son $\alpha_1 := \sqrt[4]{2}, \alpha_2 := i\sqrt[4]{2}, \alpha_3 := -\sqrt[4]{2}, \alpha_4 := -i\sqrt[4]{2}$. Como $i \in \kappa$, entonces $\sqrt[4]{2}$ es un elemento primitivo de la extensión

$$\begin{array}{c} K \\ \downarrow \\ K \end{array}$$

y $K = E_P = \kappa(\sqrt[4]{2}) = \kappa(i, \sqrt[4]{2})$. Como P es irreducible en $\mathbb{Q}[X]$, es el polinomio minimal de $\sqrt[4]{2}$ sobre \mathbb{Q} , por lo que $[\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] = \text{grad } P = 4$ y $[\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}(\sqrt[4]{2})] = 2$. Entonces

$$[E_P : \mathbb{Q}] = [E_P : \mathbb{Q}(\sqrt[4]{2})][\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] = 8 = [E_P : \mathbb{Q}(i)][\mathbb{Q}(i) : \mathbb{Q}] = 2[E_P : \mathbb{Q}(i)].$$

Esto implica, entonces, que $[E_P : \kappa] = 4$, por lo que P es también el polinomio minimal de $\sqrt[4]{2}$ sobre κ . En este caso

$$M := \{\alpha_1, \alpha_2, \alpha_3, \alpha_4\}$$

es el conjunto de toda las raíces de P y todas son conjugadas, pues P es el polinomio minimal de cada α_v , $1 \leq v \leq 4$.

Sabemos que $\circ(\mathfrak{G}(E_P : \kappa)) = [E_P : \kappa] = 4$ y que es isomorfo a un subgrupo de \mathfrak{S}_4 . También sabemos que para cada v , $1 \leq v \leq 4$, existe un único $\varphi_v \in \mathfrak{G}(E_P : \kappa)$, tal que $\varphi_v(\alpha_1) := \alpha_v$, entonces

$$\mathfrak{G}(E_P : \kappa) = \{\varphi_1, \varphi_2, \varphi_3, \varphi_4\},$$

φ_1 es la identidad, pues cada α_v se obtiene multiplicando α_1 por un elemento de κ .

Analicemos como actúa φ_2 :

$$\begin{aligned}\varphi_2(\alpha_1) &= \alpha_2 = i\alpha_1 \\ \varphi_2(\alpha_2) &= \varphi_2(i\alpha_1) = i\alpha_2 = \alpha_3 = -\alpha_1 \\ \varphi_2(\alpha_3) &= \varphi_2(-\alpha_1) = -\alpha_2 = \alpha_4 \\ \varphi_2(\alpha_4) &= \alpha_1\end{aligned}$$

Entonces φ_2 corresponde al ciclo

$$(1 \ 2 \ 3 \ 4) \in \mathfrak{S}_4,$$

el cual genera un grupo cíclico de orden 4. O sea que

$$\mathfrak{G}(E_P : \kappa) \simeq \langle (1 \ 2 \ 3 \ 4) \rangle \subset \mathfrak{S}_4.$$

Por los teoremas de Sylow para grupos abelianos, como $\text{o}(\mathfrak{G}(E_P : \kappa)) = 4 = 2^2$, $\mathfrak{G}(E_P : \kappa)$ posee un único subgrupo de orden 2, que es el subgrupo

$$H := \{\varphi_1, \varphi_2^2\}.$$

Entonces $F := \text{Fix } H$ es el único campo intermedio de la extensión

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

Para encontrar F vamos a utilizar el teorema 12.67, para

$$H := \{\varphi_1, \varphi_2^2\}.$$

Entonces

$$G = (X - \varphi_1(\alpha_1))(X - \varphi_2^2(\alpha_1)) = (X - \sqrt[4]{2})(X + \sqrt[4]{2}) = X^2 - \sqrt{2}.$$

Entonces $F := \text{Fix } H = \kappa(\sqrt{2}) = \mathbb{Q}(i, \sqrt{2})$.

12.2.4. Raíces de la Unidad. Recordamos al lector que un elemento de un grupo $g \in G$ es de orden finito si existe un entero positivo n , tal que $g^n = e$, donde e es el elemento neutro de G . Al entero positivo más pequeño, tal que $g^n = e$ lo llamamos el *orden* del elemento g . En el caso particular de un campo K , un elemento x de su grupo multiplicativo K^* es de orden finito, si existe un entero n , tal que $x^n = 1$, es decir, si x es una n -raíz del polinomio $X^n - 1$.

A las raíces del polinomio $X^n - 1$ en un campo K las llamamos las *n-raíces de la unidad*.

TEOREMA 12.68. *Las n-raíces de la unidad en un campo K , $n \geq 1$, forman un subgrupo cíclico de K^* , de orden $\leq n$.*

DEMOSTRACIÓN. El conjunto N de las n -raíces de la unidad posee, a lo sumo, n elementos, por consiguiente $\text{o}(N) \leq n$. Por otra parte, si $\alpha, \beta \in N$, entonces $(\alpha\beta)^n = \alpha^n\beta^n = 1$, lo que implica que $\alpha\beta \in N$. Por teorema 11.31, N es subgrupo cíclico de K^* . \square

En cualquier campo K las 2-raíces del polinomio $X^2 - 1$ son 1 y -1 . Si $\text{car } K = 2$, entonces $1 = -1$ y $X^2 - 1 = (X - 1)^2$ y 1 es entonces una raíz doble.

Por $E_n(K)$ denotaremos al campo de descomposición del polinomio $X^n - 1$ sobre K . Por lo anteriormente visto, siempre vale que $E_1(K) = K = E_2(K)$.

Dados dos enteros positivos n, r , entonces una n -raíz de la unidad es también una nr -raíz de la unidad, ya que $(\alpha)^{nr} = (\alpha^n)^r = (1)^r = 1$. Entonces la aplicación identidad nos induce un K -homomorfismo

$$j : E_n(K) \rightarrow E_{nr}(K)$$

y podemos considerar a $E_{nr}(K)$ como una extensión de $E_n(K)$.

En el caso particular de un campo de característica $p \neq 0$ se obtiene el siguiente

TEOREMA 12.69. *Sea K un campo de característica $p \neq 0$ y $n = p^m q$ un entero positivo, tal que $p \nmid q$. Entonces el conjunto de las n -raíces de la unidad en K es igual al conjunto de las q -raíces de la unidad en K .*

DEMOSTRACIÓN. En efecto

$$(X^n - 1) = (X^{p^m q} - 1) = (X^q - 1)^{p^m},$$

por lo que $X^q - 1$ y $X^n - 1$ poseen las mismas raíces en K y el mismo campo de descomposición sobre K . \square

En el caso particular en que $K := \mathbb{Z}_p$, $p \neq 0$, se puede calcular explícitamente el campo $E_{p^m-1}(\mathbb{Z}_p)$, ya que las raíces de $X^{p^m-1} - 1$ son las raíces $\neq 0$ del polinomio $X^{p^m} - X$, que son, precisamente, los elementos del campo con p^m elementos K_{p^m} . O sea que $E_{p^m-1}(\mathbb{Z}_p) = K_{p^m}$.

Si K es un campo finito cualquiera de característica $p \neq 0$, entonces K es isomorfo a un K_{p^m} , para algún entero positivo m y por consiguiente igual a $E_{p^m-1}(\mathbb{Z}_p)$.

Si $\text{car } K = 0$, sabemos que todas las raíces de $X^n - 1$ están en \mathbb{C} y que vienen dadas por

$$\omega_k := e^{i \frac{2\pi k}{n}}, \quad k = 0, \dots, n-1.$$

TEOREMA 12.70. *Sea κ un campo y n un entero positivo. Entonces la extensión*

(12.39)

$$\begin{array}{ccc} E_n(\kappa) \\ | \\ \kappa \end{array}$$

es de Galois.

DEMOSTRACIÓN. Por ser $E_n(\kappa)$ campo de descomposición del polinomio $X^n - 1$ sobre κ , la extensión (12.39) es normal. Por el teorema 12.69, podemos asumir que n no sea múltiplo de p , en el caso en que $\text{car } \kappa = p \neq 0$. Entonces la derivada $nX^{n-1} \neq 0$ sólo posee al 0 como raíz, que no es raíz de $X^n - 1$, por lo que $E_n(\kappa)$ es separable sobre κ . Por lo tanto la extensión (12.39) es de Galois, por ser finita, normal y separable. \square

OBSERVACIÓN 12.1. $[E_n(\kappa) : \kappa]$ y la estructura de $\mathfrak{G}(E_n(\kappa) : \kappa)$ dependen de la descomposición de $X^n - 1$ en elementos irreducibles en $\kappa[X]$.

Como las n -raíces de la unidad forman un subgrupo cíclico de $E_n^*(\kappa)$, las potencias de los elementos que son generadores, recorren todas las raíces y constituyen elementos primitivos de la extensión

$$\begin{array}{ccc} E_n(\kappa) \\ | \\ \kappa \end{array}$$

recibiendo el nombre de *n-raíces primitivas de la unidad*. Una n -raíz de la unidad α es una raíz primitiva, Ssi $\text{o}(\alpha) = n$.

TEOREMA 12.71. *Sea κ un campo y n un entero positivo, que no es múltiplo de la característica de κ . Entonces existen exactamente $\phi(n)$ n -raíces primitivas de la unidad en $E_n(\kappa)$, donde ϕ es la función de Euler. (Ver definición 3.4).*

DEMOSTRACIÓN. Sea $P := X^n - 1$. Entonces, como $p \nmid n$, $P' = nX^{n-1} \neq 0$ y posee sólo 0 como raíz, el cual no es raíz de P . Entonces P posee únicamente raíces simples en $E_n(\kappa)$, por lo que el conjunto de las n -raíces de la unidad es un subgrupo cíclico de orden n y por ejercicio 4.2.4.??, posee exactamente $\phi(n)$ generadores. \square

Dados un campo κ de característica $p \geq 0$, un entero positivo n , tal que $p \nmid n$ y el conjunto

$$\mathcal{P}_n := \{x \in E_n(\kappa) \mid x \text{ es } n\text{-raíz primitiva de la unidad}\},$$

definimos el *n-polinomio de división del círculo* o *n-polinomio ciclotómico*, como el polinomio

$$F_{n,p} := \prod_{x \in \mathcal{P}_n} (X - x)$$

de grado $\text{grad } F_{n,p} = \phi(n)$. Si $\text{car } \kappa = 0$ escribiremos sólo F_n .

TEOREMA 12.72. *Sean κ un campo de característica $\text{car } \kappa = p \geq 0$ y n un entero positivo, tal que $p \nmid n$, entonces el n-polinomio de división del círculo $F_{n,p}$ es un polinomio en $\kappa_p[X]$ de grado $\text{grad } F_{n,p} = \phi(n)$, cuyo campo de descomposición sobre κ_p es $E_n(\kappa_p)$ y*

$$X^n - 1 = \prod_{d|n} F_{d,p} \quad y \quad n = \sum_{d|n} \phi(d).$$

DEMOSTRACIÓN. Sea $\varphi \in \text{Aut}_{\kappa_p} E_n(\kappa_p)$, entonces $\varphi|_{\mathcal{P}_n}$ es una permutación sobre \mathcal{P}_n y

$$\varphi_*(F_{n,p}) = \prod_{x \in \mathcal{P}_n} (X - \varphi(x)) = \prod_{y \in \mathcal{P}_n} (X - y) = F_{n,p},$$

por lo que los coeficientes de $F_{n,p}$ están en $\text{Fix } \mathfrak{G}(E_n(\kappa_p) : \kappa_p) = \kappa_p$, ya que la extensión

$$\begin{array}{ccc} E_n(\kappa_p) & & \\ \downarrow & & \\ \kappa_p & & \end{array}$$

es de Galois. Obviamente $E_n(\kappa_p)$ es el campo de descomposición sobre κ_p de $F_{n,p}$.

Por otra parte, si $x \in E_n(\kappa_p)$ es una raíz de algún $F_{d,p}$, donde $d \mid n$, entonces, como $n = dn_1$, x es también una raíz de $X^n - 1$ y $F_{d,p} \mid (X^n - 1)$, $\forall d \mid n$, entonces

$$\prod_{d|n} F_{d,p} \mid (X^n - 1).$$

Dada x una raíz de $X^n - 1$, si x es primitiva, entonces x es también una raíz de $F_{n,p}$. Si x no es primitiva, entonces existe una raíz primitiva $y \in \mathcal{P}_n$, tal que $x = y^m$, para algún entero positivo m . Si d es el máximo común divisor de m, n , entonces $n = dn_1$ y $m = dm_1$ y

$$x^{n_1} = y^{mn_1} = y^n m_1 = 1$$

por lo que x es de orden n_1 y por consiguiente raíz de $F_{n_1,p}$, donde $n_1 \mid n$. Por consiguiente

$$X^n - 1 = \prod_{d|n} F_{d,p} \quad y \quad n = \sum_{d|n} \phi(d).$$

\square

TEOREMA 12.73. *Sea n un entero positivo. Entonces F_n es un polinomio mónico con coeficientes en \mathbb{Z} . Si p es un número primo, tal que $p \nmid n$, entonces F_{np} puede ser obtenido de F_n tomando las clases de los coeficientes de F_n , (mód p).*

DEMOSTRACIÓN. Por inducción sobre n :

Si $n = 1$, $F_{1,p} = (X - 1)$ y no hay nada que mostrar. Sea $n > 1$: Por teorema 12.72,

$$X^n - 1 = F_{n,p}G_{np},$$

donde

$$G_{np} := \prod_{\substack{d|n \\ d \neq n}} F_{dp},$$

Como $d < n$, por hipótesis de inducción, para $\text{car } \kappa = 0$, F_d es un polinomio mónico en $\mathbb{Z}[X]$ y por consiguiente G_n , como producto de polinomios mónicos con coeficientes en \mathbb{Z} es también un polinomio mónico en $\mathbb{Z}[X]$.

Por el algoritmo euclídeo en $\mathbb{Z}[X]$, existen polinomios $Q, R \in \mathbb{Z}[X]$, tales que

$$X^n - 1 = QG_n + R, \quad R = 0 \text{ o } \text{grad } R < \text{grad } G_n.$$

Esta representación también vale en $E_n(\mathbb{Q})$, donde ya sabemos que

$$X^n - 1 = F_n G_n.$$

Como esta representación es única, resulta entonces que $Q = F_n$ y $R = 0$. Por lo tanto $F_n \in \mathbb{Z}[X]$. Obviamente F_n es también un polinomio mónico.

Sea ahora p un número primo, tal que $p \nmid n$. Si P es un polinomio con coeficientes en \mathbb{Z} , por \bar{P} denotaremos al polinomio en $\mathbb{Z}_p[X]$, cuyos coeficientes son las clases en \mathbb{Z}_p de los coeficientes de P . Entonces, por hipótesis de inducción, $F_{d,p} = \bar{F}_d$, para cada d , tal que $d \mid n$, $d < n$ y $G_{n,p} = \bar{G}_n$. Entonces

$$X^n - 1 = \overline{F_n G_n} = \bar{F}_n \bar{G}_n = F_{n,p} G_{n,p}$$

Por lo tanto $F_{n,p} = \bar{F}_n$, ya que $\mathbb{Z}_p[X]$ es un dominio entero. \square

El siguiente lema nos será útil en la demostración del teorema 12.75:

LEMA 12.74. *La aplicación*

$$\varphi_p : \mathbb{Z}_p[X] \rightarrow \mathbb{Z}_p[X],$$

definida por $\varphi_p(P) := P^p$, deja fijos los elementos de \mathbb{Z}_p .

DEMOSTRACIÓN. En efecto, si $a = 0$, no hay nada que mostrar. Si $a \neq 0$, entonces $a \in \mathbb{Z}_p^*$ y es de orden $p - 1$, por lo que $a^p = a$, $\forall a \in \mathbb{Z}_p$. \square

EJEMPLOS 12.2.

1. Si $n = 2$, $P := X^2 - 1$, entonces $F_1 = X - 1$, $F_2 = X - (-1) = X + 1$.
 2. Sea q un número primo, $P := X^q - 1 = (X - 1)(X^{q-1} + X^{q-2} + \dots + 1)$. Entonces $F_1 = X - 1$, $F_q = (X^{q-1} + X^{q-2} + \dots + 1)$.
- F_q es irreducible en $\mathbb{Z}[X]$ y por consiguiente también en $\mathbb{Q}[X]$. Sin embargo, dependiendo de q y de la característica p de un determinado campo κ , F_q puede o no ser reducible en algún \mathbb{Z}_p . En efecto F_q sería reducible en algún $\mathbb{Z}_p[X]$, si P poseyera una raíz $\alpha \neq 1$ en \mathbb{Z}_p , es decir si existiera un $\alpha \in \mathbb{Z}_p^*$, de orden q , lo cual sucedería si $q \mid \text{o}(\mathbb{Z}_p^*) = p - 1$.

Así, por ejemplo, si $q := 3$, entonces $F_1 = (X - 1)$, y $F_3 = X^2 + X + 1$ es reducible

en $\mathbb{Z}_7[X]$ e irreducible en $\mathbb{Z}_2[X]$ y $\mathbb{Z}_5[X]$. En efecto, el lector comprobará que en $\mathbb{Z}_7[X]$, $F_{3,7} = (X - \bar{2})(X - \bar{4})$ y $P = (X - \bar{1})(X - \bar{2})(X - \bar{4})$.

Sin embargo en característica 0 se tiene el siguiente

TEOREMA 12.75. *Los polinomios ciclotómicos F_n son irreducibles en $\mathbb{Q}[X]$*

DEMOSTRACIÓN. F_n como polinomio mónico es irreducible en $\mathbb{Q}[X]$, Ssi es irreducible en $\mathbb{Z}[X]$. Supongamos que P sea un factor irreducible y mónico de F_n en $\mathbb{Z}[X]$. Vamos a mostrar que $\text{grad } P = \text{grad } F_n$. Si $\alpha \in E_n(\mathbb{Q})$ es una raíz de P , entonces α es una n -raíz primitiva de la unidad. Si mostramos que toda n -raíz primitiva de la unidad es raíz de P , entonces $\text{grad } F_n \geq \text{grad } P \geq \phi(n) = \text{grad } F_n$ y $\text{grad } P = \text{grad } F_n$.

Como el conjunto de las potencias α^m , donde m es primo relativo con n y α una n -raíz primitiva de la unidad, coincide con el conjunto de todas las n -raíces primitivas de la unidad, basta mostrar que si α es raíz de P , entonces, también α^p , donde p es un primo, tal que $p \nmid n$, ya que entonces, si $m = p_1 \cdots p_l$, $\alpha^m = \alpha^{p_1 \cdots p_l}$ y con α , también α^{p_λ} , $\lambda = 1, \dots, l$ es una raíz de P , entonces, resulta, de forma inductiva:

$$P(\alpha) = 0 = P(\alpha^{p_1}) = P(\alpha^{p_1 p_2}) = \cdots = P(\alpha^{p_1 \cdots p_l}) = P(\alpha^m)$$

Como divisor de F_n , P divide a $X^n - 1$ en $\mathbb{Z}[X]$, por lo que existe un polinomio $G \in \mathbb{Z}[X]$, tal que $X^n - 1 = PG$. Supongamos que α sea una raíz de P , pero para un primo $p \nmid n$, α^p no sea raíz de P . Entonces $\beta := \alpha^p$, es raíz de G , ya que β es raíz de $X^n - 1$ y el polinomio $G(X^p)$ posee a α como raíz. Como P es el polinomio minimal de α sobre \mathbb{Q} , $G(X^p)$ debe ser un múltiplo de P en $\mathbb{Q}[X]$, es decir que existe un polinomio $H \in \mathbb{Q}[X]$, tal que $G(X^p) = PH$.

Afirmamos que $H \in \mathbb{Z}[X]$: En efecto, como P es mónico, podemos efectuar una división de $G(X^p)$ por P en $\mathbb{Z}[X]$, con resto en $\mathbb{Z}[X]$, la cual debe coincidir con la representación de $G(X^p)$ en $\mathbb{Q}[X]$, por lo que $H \in \mathbb{Z}[X]$.

Pasando a \mathbb{Z}_p , tomando las clases de equivalencia $\pmod p$ de los coeficientes de los polinomios y teniendo en cuenta que, por lema 12.74, la aplicación

$$\varphi_p : \mathbb{Z}_p[X] \rightarrow \mathbb{Z}_p[X],$$

deja fijos los elementos de \mathbb{Z}_p , se obtiene

$$\bar{P}\bar{H} = \overline{G(X^p)} = G^p.$$

Entonces, si \bar{P}_0 es un factor irreducible de \bar{P} en $\mathbb{Z}_p[X]$, \bar{P}_0 es un factor irreducible de \bar{G} . Como $X^n - \bar{1} = \bar{P}\bar{G}$, se tendría que $\bar{P}_0^2 \mid (X^n - \bar{1})$ en $\mathbb{Z}_p[X]$, lo que implicaría que $X^n - \bar{1}$ tendría, al menos, una raíz doble. Como $p \nmid n$, $(X^n - \bar{1})' = \bar{n}X^{n-1} \neq 0$, cuya única raíz es 0, que no es n -raíz de la unidad, en contradicción a que $X^n - \bar{1}$ tendría al menos una raíz múltiple. Por lo tanto α^p debe ser una raíz de P . \square

TEOREMA 12.76. *Sea p un número primo, que no divide a n y cuya clase de equivalencia \bar{p} , en \mathbb{Z}_n^* es de orden e . Entonces F_n se descompone en $\mathbb{Z}_p[X]$ en $\frac{\phi(n)}{e}$ factores irreducibles de grado e . F_n es irreducible en $\mathbb{Z}_p[X]$, Ssi \bar{p} genera \mathbb{Z}_n^* .*

DEMOSTRACIÓN. Sea α una raíz de F_n en $E_n(\mathbb{Z}_p)$. Vamos a mostrar que $[\mathbb{Z}_p(\alpha) : \mathbb{Z}_p] = e$. Lo cual es suficiente, ya que F_n no posee factores repetidos.

En efecto, como α es una raíz primitiva de la unidad, $E_n(\mathbb{Z}_p) = \mathbb{Z}_p(\alpha)$ es una extensión finita de grado $[\mathbb{Z}_p(\alpha) : \mathbb{Z}_p] = m$, por lo que $\mathbb{Z}_p(\alpha)$ posee p^m elementos. Vamos a mostrar que $m = e$.

Como $\text{circ}(\alpha) = n$, $n \mid \text{o}(E_n(\mathbb{Z}_p)) = p^m - 1$ y $\bar{p}^m = \bar{1}$, ($\pmod n$). Entonces $e \mid m$. Como

$m \geq 1$, resulta que $e \leq m$. Por otra parte como $p^e \equiv 1 \pmod{n}$, resulta que $n \mid (p^e - 1)$. Como α es una n -raíz de la unidad, vale también que $\alpha^{p^e-1} = 1$, lo que implica $\alpha^{p^e} = \alpha$. Como α es un elemento primitivo de la extensión

$$\begin{array}{ccc} E_n(\mathbb{Z}_p) & & \\ | & & \\ \mathbb{Z}_p & & \end{array}$$

y la aplicación $y \mapsto y^{p^e}$ es un \mathbb{Z}_p -automorfismo de $E_n(\mathbb{Z}_p)$, resulta que $y^{p^e} = y$ y por consiguiente $y^{p^e-1} = 1, \forall y \in E_n^*(\mathbb{Z}_p)$. Como $E_n^*(\mathbb{Z}_p)$ es cíclico de orden $p^m - 1$, debe valer $(p^m - 1) \mid (p^e - 1)$, de donde $e \geq m$ y $e = m$. Entonces cada factor irreducible de F_n es de grado e . Si N es el número de factores irreducibles de F_n en $\mathbb{Z}_p[X]$, entonces $\phi(n) = \text{grad } F_n = Ne$, de donde $N = \frac{\phi(n)}{e}$.

Por otra parte, como $\circ(\mathbb{Z}_n^*) = \phi(n)$, se tiene entonces, que F_n es irreducible en $\mathbb{Z}_p[X]$, Ssi $\phi(n) = e = \bar{p}$. \square

De lo anterior se deduce que el polinomio minimal de una n -raíz primitiva de la unidad es un divisor irreducible de F_n en $\mathbb{Z}_p[X]$.

TEOREMA 12.77. *El grupo de Galois de la extensión*

$$\begin{array}{ccc} E_n(\kappa) & & \\ | & & \\ \kappa & & \end{array}$$

donde n es un entero positivo que no es múltiplo de la característica p de κ , es isomorfo a un subgrupo de \mathbb{Z}_n^* .

DEMOSTRACIÓN. Sea $\alpha \in E_n(\kappa)$ una n -raíz primitiva de la unidad fija. Si β es otra n -raíz primitiva de la unidad, entonces existe un entero positivo r , primo relativo con n , tal que $\beta = \alpha^r$. La clase $\bar{r} \pmod{n}$ está definida de forma única y es un elemento de \mathbb{Z}_n^* .

Si $\varphi \in \mathfrak{G}(E_n(\kappa) : \kappa)$, entonces $\varphi(\alpha)$ es también una n -raíz primitiva de la unidad y existe un único $\bar{r} \in \mathbb{Z}_n^*$, tal que $\varphi(\alpha) = \alpha^r$, para cualquier representante $r \in \bar{r}$. Entonces podemos definir una aplicación

$$\Phi : \mathfrak{G}(E_n(\kappa) : \kappa) \rightarrow \mathbb{Z}_n^*$$

dada por $\Phi(\varphi) := \bar{r}$. Φ es un homomorfismo inyectivo de grupos:

En efecto, dados $\varphi, \psi \in \mathfrak{G}(E_n(\kappa) : \kappa)$, $\varphi(\alpha) := \alpha^r, \psi(\alpha) = \alpha^s$, entonces $(\varphi \circ \psi)(\alpha) = \alpha^{rs}$ y $\Phi(\varphi \circ \psi) = \overline{rs} = \bar{r}\bar{s} = \Phi(\varphi)\Phi(\psi)$. Por otra parte, si $\Phi(\varphi) = \bar{1}$, entonces $r = mn + 1$, para algún $m \in \mathbb{Z}$ y $\alpha^r = \alpha^{mn+1} = (\alpha^n)^m\alpha = \alpha$, por lo que $\varphi = 1_{\mathfrak{G}(E_n(\kappa) : \kappa)}$. Entonces Φ es un isomorfismo de $\mathfrak{G}(E_n(\kappa) : \kappa)$ sobre un subgrupo de \mathbb{Z}_n^* . \square

COROLARIO 12.78. *Se n es un número primo, entonces $\mathfrak{G}(E_n(\kappa) : \kappa)$ es un grupo cíclico, cuyo orden divide a $n - 1$.*

En particular, para el caso en que $\kappa \simeq \mathbb{Q}$ es un campo de característica 0 se obtiene el siguiente resultado:

TEOREMA 12.79. *$\mathfrak{G}(E_n(\mathbb{Q}) : \mathbb{Q})$ es isomorfo a \mathbb{Z}_n^* .*

DEMOSTRACIÓN. Por teorema precedente 12.77, basta mostrar que

$$\circ(\mathfrak{G}(E_n(\mathbb{Q}) : \mathbb{Q})) = [E_n(\mathbb{Q}) : \mathbb{Q}] = \phi(n).$$

En efecto, por teorema 12.75, F_n es irreducible en \mathbb{Q} , por lo que F_n es el polinomio minimal sobre \mathbb{Q} de cualquier elemento primitivo de la extensión

$$\begin{array}{ccc} E_n(\mathbb{Q}) & & \\ \downarrow & & \\ \mathbb{Q} & & \end{array}$$

Entonces $[E_n(\mathbb{Q}) : \mathbb{Q}] = \text{grad } F_n = \phi(n)$. □

Para el caso de característica $p \neq 0$, se tiene también el siguiente resultado:

TEOREMA 12.80. *Si n es un entero positivo que no es múltiplo de la característica p del campo κ , entonces $\mathfrak{G}(E_n(\kappa) : \kappa)$ es un grupo cíclico, cuyo orden divide a $e = \circ(\bar{p})$. En particular $\circ(\mathfrak{G}(E_n(\mathbb{Z}_p) : \mathbb{Z}_p)) = e$.*

DEMOSTRACIÓN. Como $E_n(\mathbb{Z}_p)$ es un campo finito, $\text{Aut } E_n(\mathbb{Z}_p)$ es un grupo cíclico y por consiguiente $\mathfrak{G}(E_n(\mathbb{Z}_p) : \mathbb{Z}_p)$ es cíclico. Si $\alpha \in E_n(\mathbb{Z}_p)$ es una n -raíz primitiva de la unidad, entonces su polinomio minimal $P \in \kappa[X]$ sobre κ es un divisor de F_n de grado e y

$$\circ(\mathfrak{G}(E_n(\mathbb{Z}_p) : \mathbb{Z}_p)) = [E_n(\mathbb{Z}_p) : \mathbb{Z}_p] = \text{grad } P = e.$$

Para el caso general vamos a mostrar que $\mathfrak{G}(E_n(\kappa) : \kappa)$ es isomorfo a un subgrupo de $\mathfrak{G}(E_n(\mathbb{Z}_p) : \mathbb{Z}_p)$.

Sean $E := E_n(\kappa)$ y $E_p := E_n(\mathbb{Z}_p)$. Vamos a construirnos un homomorfismo inyectivo

$$\eta : \mathfrak{G}(E : \kappa) \rightarrow \mathfrak{G}(E_p : \mathbb{Z}_p).$$

Sabemos que el campo primo de κ , κ_p lo podemos identificar con \mathbb{Z}_p .

Construcción de η :

Si $\alpha_1, \dots, \alpha_n$ son las raíces de $X^n - 1$, entonces $E = \kappa(\alpha_1, \dots, \alpha_n)$ y $E_p = \mathbb{Z}_p(\alpha_1, \dots, \alpha_n)$. Dado $\varphi \in \mathfrak{G}(E : \kappa)$, como $\varphi[\{\alpha_1, \dots, \alpha_n\}] = \{\alpha_1, \dots, \alpha_n\}$, resulta que $\varphi[E_p] \subseteq E_p$ y como $[E_p : \mathbb{Z}_p] < \infty$, se tiene que $\varphi[E_p] = E_p$, por lo que $\varphi|_{E_p} \in \text{Aut}_{\mathbb{Z}_p} E_p$ y podemos definir entonces

$$\eta(\varphi) := \varphi|_{E_p}, \quad \forall \varphi \in \mathfrak{G}(E : \kappa).$$

η es un homomorfismo inyectivo:

En efecto, si $\varphi|_{E_p} = 1_{E_p}$, entonces, en particular, $\varphi(\alpha_v) = \alpha_v$, $v = 1, \dots, n$. Como φ es un κ -homomorfismo, resulta que $\varphi = 1_E$. □

12.2.5. Extensiones Radicales Simples y su Caracterización. Sean κ un campo, $a \in \kappa$ y n un entero positivo. A cada una de las n -raíces del polinomio $X^n - a$, en alguna extensión K de κ , la llamamos un *n-radical* sobre κ del elemento a y lo representaremos por $\sqrt[n]{a}$. Entonces diremos que la extensión

$$\begin{array}{ccc} \kappa(\sqrt[n]{a}) & & \\ \downarrow & & \\ \kappa & & \end{array}$$

es una *extensión radical simple*.

Si $X^n - a$ es irreducible en $\kappa[X]$, entonces se dice que $\sqrt[n]{a}$ es un *n-radical irreducible* de a .

Dado $a \in \kappa$ y α, β , raíces de $X^n - a$ en alguna extensión K de κ , entonces

$$(\alpha\beta^{-1})^n = \alpha^n(\beta^n)^{-1} = aa^{-1} = 1,$$

por lo que dos n -radicales de a se diferencian en una n -raíz de la unidad. Es decir, dados dos n -radicales de a , α, β , entonces existe una n -raíz de la unidad ω , tal que $\alpha = \omega\beta$.

En general, dos extensiones radicales simples no son isomorfas, a menos que sean irreducibles. Un criterio de irreducibilidad nos lo da el siguiente

TEOREMA 12.81 (Teorema de Abel). *Sean κ un campo, $a \in \kappa \setminus \{0\}$ y q un número primo. $P := X^q - 1$ es irreducible en $\kappa[X]$, Ssi a no es q -potencia de ningún elemento de κ .*

DEMOSTRACIÓN. Vamos a mostrar que P es reducible en $\kappa[X]$, Ssi existe $b \in \kappa$, tal que $b^q = a$.

En efecto, si $b^q = a$, para algún $b \in \kappa$, entonces $P(b) = 0$ y como $\text{grad } P = q \geq 2$, P es reducible en $\kappa[X]$.

Si P es reducible en $\kappa[X]$, sea $G \in \kappa[X]$ un divisor propio mónico de P , de grado $\text{grad } G = m$, $1 \leq m \leq q$.

Sea E una extensión del campo $E_q(\kappa)$, sobre el cual P se descomponga en factores lineales. Por lo anteriormente visto, existen q -radicales $\omega := \sqrt[q]{1}$ y $\alpha := \sqrt[q]{a}$, tales que las raíces de P se escriben de la forma $\omega^\nu \alpha$, por lo que P se descompone en $E[X]$ en factores de la forma $(X - \omega^\nu \alpha)$ y G es un producto de m de estos factores, por lo que lo podemos escribir como

$$G = (-1)^m c + \sum_{\mu=1}^m a_\mu X^\mu,$$

donde $c := \omega^k \alpha^m$, para algún $k \in \mathbb{N}$ y

$$c^q = \omega^{qk} \alpha^{qm} = (\alpha^q)^m = \alpha^m.$$

Como q es primo y $m < q$, existen enteros r, s , tales que $1 = rq + sm$ y

$$a = a^{(rq+sm)} = a^{rq} a^{ms} = a^{rq} (a^m)^s = a^{rq} (c^q)^s = (a^r)^q (c^s)^q = (a^r c^s)^q,$$

donde $a^r c^s \in \kappa$. □

El siguiente teorema nos caracteriza una extensión radical simple por medio de su grupo de Galois:

TEOREMA 12.82. *Sean n un entero positivo, κ un campo, cuya característica p no divide a n y tal que contenga a todas las n -raíces de la unidad y $a \in \kappa$. Entonces $\kappa(\sqrt[n]{a})$ es una extensión de Galois sobre κ y su grupo de Galois es un grupo cíclico cuyo orden divide a n .*

DEMOSTRACIÓN. El caso $a = 0$ es trivial. Sean entonces $a \neq 0$ y K una extensión de κ que contenga al n -radical $\alpha := \sqrt[n]{a}$. Si ω es una n -raíz primitiva de la unidad en κ , entonces

$$M := \{\omega^\nu \alpha \mid 1 \leq \nu \leq n\}$$

es el conjunto de todas las raíces de $P := X^n - a$ y $E := \kappa(\alpha)$ es el campo de descomposición de P sobre κ y por consiguiente la extensión

(12.40)

$$\begin{array}{ccc} & E & \\ & \downarrow & \\ \kappa & & \end{array}$$

es normal sobre κ .

Por otra parte, como P posee n raíces diferentes, E es también separable sobre κ y por consiguiente la extensión (12.40) es de Galois.

Vamos a mostrar ahora, que existe un homomorfismo inyectivo

$$\Phi : \mathfrak{G}(E : \kappa) \rightarrow (\mathbb{Z}_n, +).$$

En efecto, si $\varphi \in \mathfrak{G}(E : \kappa)$, entonces $\varphi(\alpha) \in M$ y existe una única clase $\bar{r} \in \mathbb{Z}_n$, tal que $\varphi(\alpha) = \omega^r \alpha$, para cualquier $r \in \bar{r}$. Entonces definimos $\Phi(\varphi) := \bar{r}$. Vamos a mostrar que Φ es un homomorfismo inyectivo: Si ψ es otro elemento de $\mathfrak{G}(E : \kappa)$, y $\psi(\alpha) = \omega^s \alpha$, entonces

$$(\varphi \circ \psi)(\alpha) = \varphi(\omega^s \alpha) = \omega^s \omega^r \alpha = \omega^{s+r} \alpha$$

y

$$\Phi(\varphi \circ \psi) = \overline{r+s} = \bar{r} + \bar{s} = \Phi(\varphi) + \Phi(\psi).$$

Por otra parte, si $\Phi(\varphi) = 0$, entonces $\varphi = 1_E$. Por lo tanto Φ es inyectivo. \square

El siguiente teorema es una inversa del precedente:

TEOREMA 12.83. *Bajo las mismas condiciones del teorema precedente, si*

$$\begin{array}{c} E \\ \downarrow \\ \kappa \end{array}$$

es una extensión de Galois de grado n con grupo de Galois, $\mathfrak{G}(E : \kappa)$, cíclico, entonces E es una extensión radical simple sobre κ .

DEMOSTRACIÓN. Sean ω una n -raíz primitiva de la unidad y φ un generador del grupo cíclico $\mathfrak{G}(E : \kappa)$. Para cada $x \in E$, formamos la llamada *resolvente de Lagrange*:

$$R(\omega, x) := \sum_{v=0}^{n-1} \omega^v \varphi^v(x).$$

Supongamos que existe $x \in E$, tal que $R(\omega, x) \neq 0$. Como $\varphi(\omega) = \omega$ y $\varphi^n = 1_E$ se tiene

$$\varphi(R(\omega, x)) = \sum_{v=0}^{n-1} \omega^v \varphi^{v+1}(x) = \omega^{-1} \sum_{v=1}^{n-1} \omega^v \varphi^v(x) = \omega^{-1} R(\omega, x),$$

de donde resulta entonces para un entero positivo $1 \leq \mu \leq n$:

$$\varphi^\mu(R(\omega, x)) = x^{-\mu} R(\omega, x).$$

Como φ es un generador de $\mathfrak{G}(E : \kappa)$ y ω es una n -raíz primitiva de la unidad, el único κ -automorfismo que deja fijo $R(\omega, x)$ es 1_E . Entonces $\mathfrak{G}(E : \kappa(R(\omega, x))) = \{1_E\}$.

Por teorema ?? la extensión

$$\begin{array}{c} E \\ \downarrow \\ \kappa(R(\omega, x)) \end{array}$$

es de Galois y se tiene

$$\kappa(R(\omega, x)) = \text{Fix}\{1_E\} = E.$$

Finalmente

$$\varphi(R(\omega, x))^n = (\varphi(R(\omega, x)))^n = \omega^{-n} (R(\omega, x))^n = (R(\omega, x))^n,$$

lo que implica que $(R(\omega, x))^n \in \text{Fix } \mathfrak{G}(E : \kappa) = \kappa$, ya que φ genera $\mathfrak{G}(E : \kappa)$. Entonces

$$R(\omega, x) = \sqrt[n]{(R(\omega, x))^n}$$

es un radical sobre κ .

Vamos a mostrar ahora, que, en efecto, existe un $x \in E$, tal que $R(\omega, x) \neq 0$. Basta mostrar que si la expresión

$$(12.41) \quad a_0 x + a_1 \varphi(x) + \cdots + a_{n-1} \varphi^{n-1}(x) = 0, \quad \forall x \in E, \quad a_v \in E, v = 0, \dots, n,$$

entonces

$$a_0 = a_1 = \cdots = a_{n-1} = 0.$$

Supongamos que (12.41) valga y sea m el menor entero positivo, entre todas las combinaciones lineales que satisfagan (12.41), para el cual

$$a_0x + a_1\varphi(x) + \cdots + a_m\varphi^m(x) = 0, \quad a_m \neq 0.$$

Entonces $0 < m < n$ y no todos los a_μ , $0 \leq \mu \leq m$ son 0. Sea l el mayor número, para el cual $a_l \neq 0$, $0 \leq l < m$ y $y \in E$, tal que $\varphi^l(y) \neq \varphi^m(y)$. Entonces

$$(12.42) \quad a_0xy + a_1\varphi(xy) + \cdots + a_m\varphi^m(xy) = a_0xy + a_1\varphi(x)\varphi(y) + \cdots + a_m\varphi^m(x)\varphi^m(y) = 0.$$

donde $a_\mu = 0$, para $l < \mu < m$. También

$$(12.43) \quad a_0x\varphi^m(y) + a_1\varphi(x)\varphi^m(y) + \cdots + a_m\varphi^m(x)\varphi^m(y) = 0.$$

Restando las ecuaciones (12.42) y (12.43) obtenemos

$$(12.44) \quad a_0(y - \varphi^m(y))x + \cdots + a_l(\varphi^l(y) - \varphi^m(y))\varphi^l(x) = 0, \quad l < m.$$

Donde (12.44) es de la forma

$$b_0x + b_1\varphi(x) + \cdots + b_l\varphi^l(x) = 0, \quad b_\lambda := a_l(\varphi^l(y) - \varphi^m(y))$$

y $b_l := a_l(\varphi^l(y) - \varphi^m(y)) \neq 0$ en contradicción a la minimalidad de m . \square

EJEMPLOS 12.3.

1. Encontrar F_4 : $X^4 - 1 = (X^2 + 1)(X - 1)(X + 1)$.

$\text{grad } F_4 = \phi(4) = 2$, F_4 irreducible en \mathbb{Q} y $F_4 \mid (X^4 - 1)$. Entonces $F_4 = X^2 + 1$.

2. F_8 : $X^8 - 1 = (X^4 + 1)(X^2 + 1)(X + 1)(X - 1)$, $\text{grad } F_4 = \phi(8) = 4$. Entonces $F_8 = X^4 + 1$.

3. F_{12} :

$$\begin{aligned} X^{12} - 1 &= (X^6 + 1)(X + 1)(X - 1)(X^2 + X + 1)(X^2 - X + 1) \\ &= (X^2 + 1)(X^4 - X^2 + 1)(X + 1)(X - 1)(X^2 + X + 1)(X^2 - X + 1). \end{aligned}$$

$\text{grad } F_{12} = \phi(12) = 4$. Entonces $F_{12} = X^4 - X^2 + 1$

4. Dar los factores irreducibles de F_{12} en \mathbb{Z}_{11} . El teorema 12.76, nos dice que si

$p \neq n$, entonces F_n se descompone en \mathbb{Z}_p en $\frac{\phi(n)}{e}$ factores irreducibles, donde

$e = \phi(\bar{p})$, ($\text{mód } n$). En nuestro caso $n = 12$, $p = 11$ y $e = \phi(\bar{11}) = 2$. Entonces F_{12} se descompone en \mathbb{Z}_{11} en dos factores de grado 2, es decir $F_{12} = X^4 - X^2 + 1 = (X^2 + aX + b)(X^2 + a'X + b')$, $a, b, a', b' \in \mathbb{Z}_{11}$. Esto nos lleva al sistema de ecuaciones ($\text{mód } 11$)

$$(12.45) \quad a + a' = 0$$

$$(12.46) \quad aa' + b + b' = -1$$

$$(12.47) \quad bb' = 1$$

$$(12.48) \quad ab' + a'b = 0$$

De la ecuación (12.46), resulta $a = -a'$. Substituyendo en (12.48):

$$a(b' - b) = 0 \Rightarrow \begin{cases} a = 0 & \text{o,} \\ b = b' & \end{cases}$$

Si $a = 0$, de las ecuaciones (12.47) y (12.48), resultaría

$$b' + b = -1 \quad y \quad b' = \frac{1}{b}$$

que nos lleva a la ecuación

$$(12.49) \quad b^2 + b + 1 = 0, \quad (\text{mód } 11).$$

Dejamos al lector, como ejercicio, comprobar que ningún elemento de \mathbb{Z}_{11} satisface la ecuación (12.49). Entonces $b = b'$ y de la ecuación (12.48) se obtiene $b^2 = 1$, es decir

$$b = \begin{cases} 1 & \text{o,} \\ -1 & \end{cases}$$

El caso $b = -1$ se descarta, ya que substituyendo en (12.47) obtendríamos

$$(12.50) \quad a^2 + 1 = 0, \quad (\text{mód } 11),$$

y el lector comprobará que la ecuación (12.50), tampoco tiene solución en \mathbb{Z}_{11} , por lo que $b = b' = 1$. Substituyendo nuevamente en (12.47) se obtiene la ecuación

$$a^2 - 3 = 0 \quad (\text{mód } 11)$$

la que nos da como resultado $a = 5$ y $a' = -5$. Entonces

$$F_{12} = (X^2 + 5X + 1)(X^2 - 5X + 1) = (X^2 + 5X + 1)(X^2 + 6X + 1) \in \mathbb{Z}_{11}.$$

5. Descomponer $X^{16} - 1$ en sus factores irreducibles en $\mathbb{Z}_3[X]$.

$$X^{16} - 1 = \underbrace{(X^8 + 1)}_{F_{16}} \underbrace{(X^4 + 1)}_{F_8} \underbrace{(X^2 + 1)}_{F_4} \underbrace{(X + 1)}_{F_2} \underbrace{(X - 1)}_{F_1}.$$

$$\circ(\bar{3}) \quad (\text{mód } 4) = 2 = \phi(4) \Rightarrow F_4 \text{ ya es irreducible en } \mathbb{Z}_3[X].$$

$$\circ(\bar{3}) \quad (\text{mód } 8) = 2, \phi(8) = 4 \Rightarrow F_8 \text{ se descompone en dos factores de grado 2 en } \mathbb{Z}_3[X].$$

$$\circ(\bar{3}) \quad (\text{mód } 16) = 4, \phi(16) = 8 \Rightarrow F_{16} \text{ se descompone en dos factores de grado 4 en } \mathbb{Z}_3[X].$$

Procediendo como en el ejemplo precedente se deben resolver, para cada caso, un sistema de ecuaciones en \mathbb{Z}_3 , tarea que dejamos al lector como ejercicio. El lector comprobará entonces que en $\mathbb{Z}_3[X]$

$$X^4 + 1 = (X^2 + X + 2)(X^2 + 2X + 2)$$

y

$$X^8 + 1 = (X^4 + X^3 + 2X^2 + X + 1)(X^4 + 2X^3 + 2X^2 + 2X + 1).$$

Entonces en $\mathbb{Z}_3[X]$:

$$X^{16} - 1 = (X^4 + X^3 + 2X^2 + X + 1)(X^4 + 2X^3 + 2X^2 + 2X + 1)(X^2 + X + 2)(X^2 + 2X + 2)(X^2 + 1)(X + 1)(X - 1).$$

12.2.6. Resolución de Ecuaciones Polinómicas por Radicación. Dado un polinomio $P \in \kappa[X]$ buscamos elementos x en una extensión

$$\begin{array}{c} E \\ | \\ \kappa \end{array}$$

tal que $P(x) = 0$ en E .

Por resolución de una ecuación de la forma

$$P(x) = 0,$$

donde $P \in \kappa[X]$ se entenderá el proceso de llegar a obtener las raíces de P por un proceso finito de extensiones radicales simples sucesivas del campo κ . En esta subsección, por facilidad, nos limitaremos al caso $\text{car } \kappa = 0$.

Decimos que la extensión

$$\begin{array}{c} E \\ | \\ \kappa \end{array}$$

es una *extensión radical*, si existe una cadena de campos intermedios

$$E_0 := \kappa \subseteq E_1 \subseteq \cdots \subseteq E_m := E,$$

tal que cada subextensión

$$\begin{array}{c} E_\mu \\ | \\ E_{\mu-1} \end{array}$$

es una extensión radical simple, $\forall \mu = 1, \dots, m$.

Decimos que la ecuación

$$P(x) = 0,$$

es *soluble por radicación*, Si el campo de descomposición E_P , está contenido en una extensión radical de κ .

Por ejemplo si

$$P := aX^2 + bX + c \in \mathbb{R}[X], \quad a \neq 0,$$

sus raíces vienen dadas por

$$x_{1,2} := -\frac{1}{2a}(b \pm \sqrt{b^2 - 4ac}).$$

Entonces podemos escribir

$$P = a\left(\left(X + \frac{b}{2a}\right)^2 + \frac{4ac - b^2}{4a^2}\right)$$

y su campo de descomposición está contenido en $\mathbb{R}(\sqrt{b^2 - 4ac})$ que es una extensión radical simple de \mathbb{R} .

TEOREMA 12.84. *Toda extensión radical E de κ está contenida en una extensión radical normal*

$$\begin{array}{c} K \\ | \\ \kappa \end{array}$$

DEMOSTRACIÓN. Por inducción sobre $n := [E : \kappa]$. Si $[E : \kappa] = 1$, entonces $E = \kappa$. Dado $a \in \kappa$, $E = \kappa \subseteq \kappa(\sqrt[n]{a})$, donde la extensión

$$\begin{array}{c} \kappa(\sqrt[n]{a}) \\ \downarrow \\ \kappa \end{array}$$

es de Galois y por consiguiente normal.

Supongamos, por hipótesis de inducción, que el teorema valga para $1 \leq m \leq n - 1$ y sea $n \geq 2$. Por definición de extensión radical, existe un campo intermedio E' tal que

- a) $E = E'(\alpha)$, con $\alpha^l \in \kappa$, para algún entero $2 \leq l$.
- b) $[E : E'] \geq 2$.

De b) resulta que $[E' : \kappa] \leq n - 1$ y, por hipótesis de inducción, existe una extensión radical normal K' , tal que $E' \subseteq K'$. Vamos a probar que si $K := E_P$, donde E_P es el campo de descomposición del polinomio

$$P := \prod_{\varphi \in \mathfrak{G}(K' : \kappa)} (X^l - \varphi(\alpha^l))$$

sobre K' , entonces la extensión

$$\begin{array}{c} K \\ \downarrow \\ \kappa \end{array}$$

posee las propiedades deseadas.

Como α es raíz del factor $X^l - \alpha^l$ de P , $\alpha \in E_P = K$, por lo que K es también una extensión de $E = E'(\alpha)$.

Vamos a mostrar que K es una extensión radical normal de κ . En efecto, $P \in \kappa[X]$, ya que dado $\psi \in \mathfrak{G}(E' : \kappa)$

$$\psi_*(P) = \prod_{\varphi \in \mathfrak{G}(K' : \kappa)} (X^l - (\psi \circ \varphi)(\alpha^l)) = P,$$

por lo que $P \in (\text{Fix } \mathfrak{G}(K' : \kappa))[X] = \kappa[X]$, ya que la extensión K' sobre κ es de Galois. Entonces K es normal sobre κ por ser campo de descomposición de un polinomio en $\kappa[X]$. Por otra parte, por definición de K

$$\begin{array}{c} K \\ \downarrow \\ K' \end{array}$$

es una extensión radical, pues se obtiene adjuntando sucesivamente las l -raíces de $X^l - \varphi(\alpha^l)$ y como, por hipótesis de inducción

$$\begin{array}{c} K' \\ \downarrow \\ \kappa \end{array}$$

también es radical, resulta que

$$\begin{array}{c} K \\ \downarrow \\ \kappa \end{array}$$

es normal y radical. \square

El siguiente teorema es considerado el teorema principal respecto de la solubilidad, por radicación, de una ecuación polinómica.

TEOREMA 12.85 (Teorema Principal de Solubilidad). *Sean κ un campo y $P \in \kappa[X]$. Entonces la ecuación $P(x) = 0$ es soluble por radicación, Ssi el grupo de Galois $\mathfrak{G}(E_P : \kappa)$, donde E_P es el campo de descomposición de P sobre κ , es un grupo soluble.*

DEMOSTRACIÓN. La demostración la desarrollaremos en una serie de lemas.

Supongamos que la ecuación $P(x) = 0$ es soluble por radicación. De la definición y por el teorema 12.84, el campo de descomposición E_P de P está contenido en una extensión radical normal

$$\begin{array}{c} K \\ \downarrow \\ \kappa \end{array}$$

que además es de Galois y finita y la extensión

$$\begin{array}{c} E_P \\ \downarrow \\ \kappa \end{array}$$

también es una extensión normal. Entonces, por teorema 12.60, existe un isomorfismo

$$\hat{\eta} : \mathfrak{G}(K : \kappa)/\mathfrak{G}(K : E_P) \rightarrow \mathfrak{G}(E_P : \kappa).$$

Entonces basta mostrar que $\mathfrak{G}(K : \kappa)$ es un grupo soluble.

LEMA 12.86. *Si*

$$\begin{array}{c} K \\ \downarrow \\ \kappa \end{array}$$

es una extensión normal y radical de κ , entonces el grupo $\mathfrak{G}(K : \kappa)$ es un grupo soluble.

DEMOSTRACIÓN. consideremos la cadena de campos

$$K_0 := \kappa \subseteq K_1 \subseteq \cdots \subseteq K_m := K,$$

donde para cada μ , $1 \leq \mu \leq m$, la extensión

$$\begin{array}{c} K_\mu \\ \downarrow \\ K_{\mu-1} \end{array}$$

es una extensión radical simple. $K_\mu = K_{\mu-1}(x_\mu)$, $x_\mu^{n_\mu} = a_\mu \in K_{\mu-1}$, para algún entero positivo n_μ . Sea $n := n_1 \cdots n_m$, $\kappa' := E_n(\kappa)$, $K'_\mu := E_n(K_\mu)$ y $K' := E_n(K)$. Entonces K'_μ es una extensión de $K'_{\mu-1}$ y se tiene la cadena

$$(12.51) \quad E_n(\kappa) := \kappa' = K'_0 \subseteq K'_1 \subseteq \cdots \subseteq K'_m := K',$$

K es campo de descomposición de un polinomio $G \in \kappa[X]$, sobre κ . Entonces K' es el campo de descomposición del polinomio $P := (X^n - 1)G$ sobre κ y la extensión

$$\begin{array}{c} K' \\ \downarrow \\ \kappa \end{array}$$

es de Galois.

Para $\mu = 1, \dots, m$, $K'_{\mu-1}$ contiene las n_μ raíces de la unidad y $K'_\mu = K'_{\mu-1}(x_\mu)$, donde

$x_\mu^{n_\mu} \in K'_{\mu-1}$ y, por teorema 12.82, $\mathfrak{G}(K'_\mu : K'_{\mu-1})$ es un grupo cíclico, en particular abeliano, y también el grupo $\mathfrak{G}(\kappa' : \kappa)$, como subgrupo de \mathbb{Z}_n^* , es abeliano. Además las extensiones

$$\begin{array}{c} K'_\mu \\ \downarrow \\ K'_{\mu-1} \end{array}$$

son normales. Tenemos, entonces, la siguiente configuración de extensiones:

$$\begin{array}{ccccc} & & K' & & \\ & \swarrow & & \searrow & \\ \kappa' & & & & K \\ & \swarrow & \searrow & & \\ & & K & & \end{array}$$

K es entonces un campo intermedio de la extensión de Galois

$$\begin{array}{c} K' \\ \downarrow \\ K \end{array}$$

y por teorema 12.60, la aplicación

$$\eta : \mathfrak{G}(K' : \kappa) \rightarrow \mathfrak{G}(K : \kappa),$$

tal que $\eta(\varphi) := \varphi|_K$, es sobreyectiva, por lo que $\mathfrak{G}(K : \kappa)$ es imagen homomorfa de $\mathfrak{G}(K' : \kappa)$. Si mostramos que $\mathfrak{G}(K' : \kappa)$ es soluble, entonces habremos mostrado también que $\mathfrak{G}(K : \kappa)$ es soluble.

La solubilidad de $\mathfrak{G}(K' : \kappa)$ resulta del siguiente lema:

LEMÁ 12.87. *Sea*

$$K_0 := \kappa \subseteq K_1 \subseteq \cdots \subseteq K_n := K,$$

una cadena de campos, donde la extensión

$$\begin{array}{c} K \\ \downarrow \\ \kappa \end{array}$$

es de Galois y para todo v , $1 \leq v \leq n$, las extensiones

$$\begin{array}{c} K_v \\ \downarrow \\ K_{v-1} \end{array}$$

son normales. Entonces, si $\mathfrak{G}(K_v : K_{v-1})$ es abeliano, para cada v , $\mathfrak{G}(K : \kappa)$ es un grupo soluble.

Aplicando lema 12.87 a la cadena 12.51, se obtiene la solubilidad del grupo $\mathfrak{G}(K' : \kappa)$. Con lo que queda demostrado el lema 12.86. \square

Mostremos ahora la validez del lema 12.87:

DEMOSTRACIÓN. Por inducción sobre n : Si $n = 0$ el lema es trivial. Sea entonces $n \geq 1$ y supongamos, por hipótesis de inducción, que para todo $m \leq n$ el lema vale. El campo intermedio K_1 de la extensión de Galois

$$\begin{array}{c} K \\ | \\ K_1 \end{array}$$

es normal sobre κ . En consecuencia $\mathfrak{G}(K : K_1)$ es un subgrupo normal de $\mathfrak{G}(K : \kappa)$ y, por teorema 12.60, se tiene un isomorfismo

$$\psi : \mathfrak{G}(K_1 : \kappa) \rightarrow \mathfrak{G}(K : \kappa) / \mathfrak{G}(K : K_1),$$

Como $\mathfrak{G}(K_1 : \kappa)$ es abeliano, entonces es soluble (ver ejemplo 6.3.1) y, por hipótesis de inducción, también $\mathfrak{G}(K : K_1)$ es soluble. Entonces, por teorema 6.26, $\mathfrak{G}(K : \kappa)$ es soluble. Con lo que queda demostrado el lema 12.87. \square

La solubilidad del grupo $\mathfrak{G}(E_p : \kappa)$ resulta entonces del teorema 6.24, aplicado al isomorfismo

$$\hat{\eta} : \mathfrak{G}(K : \kappa) / \mathfrak{G}(K : E_p) \rightarrow \mathfrak{G}(E_p : \kappa).$$

Con lo que queda demostrada la primera parte del teorema principal.

Sea E_P el campo de descomposición del polinomio P tal que el grupo $\mathfrak{G}(E_p : \kappa)$ es soluble. Si q_1, \dots, q_r son los divisores primos de $[E_p : \kappa]$, sean $n := q_1 \cdots q_r$, $\kappa' := E_n(\kappa)$, $E' := E_n(E_p)$, entonces se tiene el siguiente diagrama de extensiones

$$\begin{array}{ccccc} & & E' & & \\ & \swarrow & & \searrow & \\ \kappa' & & & & E_P \\ & \swarrow & & \searrow & \\ & & K & & \end{array}$$

Por lo que E' es una extensión de κ' . Como campo de descomposición del polinomio $G := (X^n - 1)P \in \kappa[X]$, la extensión

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

es normal sobre κ . Vamos a mostrar que E' es una extensión radical sobre κ , lo que mostraría que $P(x)$ es soluble por radicación.

Como $\kappa' = \kappa(\omega)$, donde ω es una n -raíz primitiva de la unidad, la extensión

$$\begin{array}{c} \kappa' \\ | \\ K \end{array}$$

es una extensión radical simple, por lo que es suficiente mostrar que la extensión

$$\begin{array}{c} E' \\ | \\ \kappa' \end{array}$$

es radical.

A tal efecto, recopilemos algunas propiedades de $\mathfrak{G}(E' : \kappa')$:

1. Dado $\varphi \in \mathfrak{G}(E' : \kappa')$, la restricción $\varphi|_{E_p}$ induce un homomorfismo inyectivo:

$$\eta : \mathfrak{G}(E' : \kappa') \rightarrow \mathfrak{G}(E_p : \kappa),$$

ya que $\mathfrak{G}(E' : \kappa') \subseteq \mathfrak{G}(E' : \kappa)$ y, por el teorema de normalidad finita 12.26, $\varphi[E_p] \subseteq E_p$, por lo que $\varphi|_{E_p} \in \mathfrak{G}(E_p : \kappa)$
 η es inyectivo: Si $\varphi \in \ker \eta$, entonces $\varphi(x) = x, \forall x \in E_p$ y también $\varphi(x) = x, \forall x \in \kappa'$. Como $E' = E_p(\kappa')$, resulta entonces que $\varphi = 1_{E'}$.

2. $\mathfrak{G}(E' : \kappa')$ es soluble, por ser isomorfo a un subgrupo de $\mathfrak{G}(E_p : \kappa)$, el cual, por hipótesis es soluble.

3. Dado $\varphi \in \mathfrak{G}(E' : E_p)$, la restricción $\varphi|_{\kappa}$ induce un homomorfismo inyectivo:

$$\theta : \mathfrak{G}(E' : E_p) \rightarrow \mathfrak{G}(\kappa' : \kappa),$$

ya que $E' = E_p(\omega)$ y $\kappa' = \kappa(\omega)$.

θ es inyectivo: Si $\varphi \in \ker \theta$, entonces $\varphi|_{\kappa'} = 1_{\kappa'}$ y como $E' = E_p(\kappa')$, resulta $\varphi = 1_{E'}$.

4. Si q es un factor primo de $[E' : \kappa']$, entonces κ' contiene todas las q -raíces de la unidad.

En efecto, como

$$\begin{array}{c} E' \\ | \\ E_P \end{array}$$

es de Galois,

$$[E' : E_P] = \circ(\mathfrak{G}(E' : E_P)) \mid \circ(\mathfrak{G}(\kappa' : \kappa)) = [\kappa' : \kappa]$$

y existe un entero positivo m , tal que $[\kappa' : \kappa] = m[E' : E_P]$. Como

$$\begin{array}{ccccc} & & E' & & \\ & \swarrow & & \searrow & \\ \kappa' & & & & E_P \\ & \searrow & & \swarrow & \\ & & K & & \end{array}$$

se tiene

$$[E' : \kappa] = [E' : \kappa'][\kappa' : \kappa] = [E' : E_P][E_P : \kappa],$$

o sea que

$$[E' : \kappa'][E' : E_P]m = [E' : E_P][E_P : \kappa],$$

de donde $[E' : \kappa']m = [E_P : \kappa]$, entonces q es un factor primo de $[E_P : \kappa]$ y por consiguiente de n . Entonces toda q -raíz de la unidad es también una n -raíz de la unidad y está en κ' .

El teorema principal queda demostrado, si mostramos el siguiente

LEMÁ 12.88. *Si la extensión normal y finita*

(12.52)

$$\begin{array}{c} K \\ | \\ \kappa \end{array}$$

es tal que $\mathfrak{G}(K : \kappa)$ es soluble y para cada factor primo q de $K : \kappa$, vale que κ contiene a todas las q -raíces de la unidad, entonces la extensión (12.52) es radical.

Entonces aplicando el lema 12.88 a la extensión

$$\begin{array}{c} E' \\ \downarrow \\ K' \end{array}$$

queda demostrado el teorema principal. \square

Mostremos ahora la validez del lema 12.88:

DEMOSTRACIÓN. Por inducción sobre $n := [K : \kappa]$: para $n = 1$ no hay nada que demostrar. Sea entonces $n \geq 2$ y supongamos, por hipótesis de inducción, que el lema sea válido para todo entero positivo $m \leq n - 1$.

Como $\mathfrak{G}(K : \kappa)$ es soluble, por teorema 6.30, posee una serie de composición, cuyos cocientes son grupos cíclicos de orden primo. En particular existe un subgrupo normal H tal que $\circ(\mathfrak{G}(K : \kappa)/H) = q$, donde q es un número primo.

Sea $E := \text{Fix } H$. Por el teorema principal de Galois, 12.53, vale $\mathfrak{G}(K : E) = H$ y

$$\mathfrak{G}(E : \kappa) \simeq \mathfrak{G}(K : \kappa)/\mathfrak{G}(K : E) = \mathfrak{G}(K : \kappa)/H,$$

por lo que $[E : \kappa] = q$ y la extensión

$$\begin{array}{c} E \\ \downarrow \\ K \end{array}$$

es, por teorema 12.60, de Galois, ya que $\mathfrak{G}(K : E) = H$ es normal. Como, por hipótesis K contiene a todas las raíces de la unidad, por teorema 12.83, la extensión

$$\begin{array}{c} E \\ \downarrow \\ K \end{array}$$

es una extensión radical simple. Por otra parte la extensión

$$\begin{array}{c} K \\ \downarrow \\ E \end{array}$$

es normal, ya que E es un campo intermedio de la extensión normal

$$\begin{array}{c} K \\ \downarrow \\ \kappa \end{array}$$

y $\mathfrak{G}(K : E) = H$ es también soluble, como subgrupo del grupo soluble $\mathfrak{G}(K : \kappa)$. Finalmente, todo factor primo \tilde{q} de $[K : E]$ es factor primo de $[E : \kappa]$ y E , como extensión de κ , contiene a todas las \tilde{q} -raíces de la unidad. Como

$$n = [K : \kappa] = [K : E][E : \kappa]$$

y

$$[K : E] = \frac{n}{[E : \kappa]} = \frac{n}{\tilde{q}} \leq n - 1,$$

por hipótesis de inducción,

$$\begin{array}{c} K \\ \downarrow \\ E \end{array}$$

es una extensión radical. Por lo tanto

$$\begin{array}{c} K \\ \downarrow \\ \kappa \end{array}$$

es una extensión radical. \square

Como corolario del teorema principal de solubilidad 12.85, se obtiene el siguiente resultado:

COROLARIO 12.89. *Toda ecuación $P(x) = 0$, donde P es un polinomio con coeficientes en un campo κ , de grado ≤ 4 , es soluble por radicación.*

DEMOSTRACIÓN. Por teorema 12.66, $\mathfrak{G}(E_P : \kappa)$, donde E_P es el campo de descomposición del polinomio P es isomorfo a un subgrupo del grupo de simetría \mathfrak{S}_m , donde $m := \text{grad } P$. Sabemos que para $m \leq 4$ el grupo \mathfrak{S}_m es soluble (ver ejemplo 6.3,3). Por consiguiente $\mathfrak{G}(E_P : \kappa)$, como subgrupo de un grupo soluble, es soluble. Por lo tanto la ecuación $P(x) = 0$ es soluble. \square

Para mostrar que, en general, una ecuación polinómica, $P(x) = 0$, donde P es un polinomio de grado $n \geq 5$, no es soluble por radicación, vamos a mostrar que el grupo de Galois $\mathfrak{G}(E_P : \kappa)$ es isomorfo a \mathfrak{S}_n , el cual, como se vió en el ejemplo 6.3, ej:solubgrupsim5, no es soluble.

Antes de demostrar el teorema general de Abel, vamos a analizar el siguiente ejemplo de una ecuación de grado $n := 5$.

EJEMPLO 12.4. Sea $P := X^5 - 2X^4 + 2 \in \mathbb{Q}[X]$. Vamos a mostrar que la ecuación $P(x) = 0$ no es soluble por radicación, mostrando que $\mathfrak{G}(E_P : \mathbb{Q})$ es isomorfo a \mathfrak{S}_5 que no es soluble.

Por el criterio de Eisenstein se tiene que P es irreducible en $\mathbb{Q}[X]$ y, como el lector comprobará fácilmente, no posee raíces en común con P' . Entonces P posee 5 raíces distintas en una extensión $E_P \subseteq \mathbb{C}$.

Sean $\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5 \in E_P$ las raíces de P . Evaluando P en el conjunto

$$\{-1, 0, \frac{3}{2}, 2\}$$

obtenemos lo siguiente:

$$\begin{aligned} P(-1) &= -1 < 0 \\ P(0) &= 2 > 0 \\ P(\frac{3}{2}) &= 2 - \frac{81}{32} < 0 \\ P(2) &= 2 > 0 \end{aligned}$$

Esto quiere decir, por el teorema del valor intermedio del cálculo diferencial, que P posee, al menos, 3 raíces reales.

Supongamos que P posea más de 3 raíces reales, entonces, por el teorema de Rolle, del cálculo diferencial, P' poseería, al menos, 3 raíces reales distintas, lo cual, como el lector comprobará fácilmente, no es cierto. Por consiguiente P posee exactamente 3 raíces reales y 2 raíces complejas conjugadas, no reales.

Sean $\alpha_1, \alpha_2, \alpha_3$ las tres raíces reales y α_4, α_5 las dos raíces complejas conjugadas. Si

$$\varphi : \mathbb{C} \rightarrow \mathbb{C}$$

es el \mathbb{Q} -automorfismo de la conjugación, entonces, como

$$\begin{array}{c} E_P \\ \downarrow \\ \mathbb{Q} \end{array}$$

es normal, se tiene que $\psi := \varphi|_{E_P} \in \mathfrak{G}(E_P : \mathbb{Q})$ y como $\text{Fix}\{1_{E_P}, \psi\} = \mathbb{R}$, tenemos que $\psi(\alpha_v) = \alpha_v$, para $1 \leq v \leq 3$ y $\psi(\alpha_4) = \alpha_5$. Entonces, si

$$\Phi : \mathfrak{G}(E_P : \mathbb{Q}) \rightarrow \mathfrak{S}_5$$

es el homomorfismo inyectivo, definido en la demostración del teorema 12.66, se obtiene que

$$\Phi(\psi) = \begin{pmatrix} 4 & 5 \end{pmatrix}.$$

Por otra parte, como P es irreducible sobre \mathbb{Q} , los elementos $\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5 \in E_P$, son conjugados sobre \mathbb{Q} y para cada par de raíces α_i, α_j , existe un $\varphi_{i,j} \in \mathfrak{G}(E_P : \mathbb{Q})$, tal que $\varphi_{i,j}(\alpha_i) = \alpha_j$. Entonces el grupo $\mathfrak{G} := \Phi[\mathfrak{G}(E_P : \mathbb{Q})]$ posee las siguientes propiedades:

- a) \mathfrak{G} es transitivo, pues para cada par de elementos $i, j \in S_5$, existe una permutación $\tau_{i,j} := \Phi(\varphi_{i,j})$, tal que $\tau_{i,j}(i) = j$.
- b) \mathfrak{G} contiene transposiciones.

Por lo tanto $\mathfrak{G} = \mathfrak{S}_5$.

Finalmente concluimos esta sección, con el famoso teorema de Abel:

TEOREMA 12.90 (Teorema de Abel). *Para $n \geq 5$, la ecuación polinómica general de grado n no es soluble por radicación.*

Previo a la demostración hacemos la siguiente observación sobre la notación utilizada: Si $K[X_1, \dots, X_n]$ es el anillo de polinomios en n indeterminadas, sobre el campo K , denotaremos por $K_n := K(X_1, \dots, X_n)$ su campo de fracciones correspondiente.

DEMOSTRACIÓN. Consideremos el polinomio

$$P_n := X^n + \sum_{v=1}^n (-1)^v U_v X^{n-v}, \quad U_v \in K_n = K(U_1, \dots, U_n).$$

Entonces la ecuación

$$P_n(x) = 0$$

se llama la *ecuación general* de grado n . Sean E_{P_n} el campo de descomposición de P_n sobre K_n y $\alpha_1, \dots, \alpha_n$ sus raíces en E_{P_n} . Entonces en E_{P_n}

$$P_n = \prod_{v=1}^n (X - \alpha_v) \quad \text{y} \quad U_v = \sum_{1 \leq \lambda_1 < \lambda_2 < \dots < \lambda_v \leq n} \alpha_{\lambda_1} \cdots \alpha_{\lambda_v} \quad 1 \leq v \leq n.$$

Vamos a calcular el grupo $\mathfrak{G}(E_{P_n} : K_n)$. Consideremos otras n indeterminadas X_1, \dots, X_n y los elementos

$$u_v = \sum_{1 \leq \lambda_1 < \lambda_2 < \dots < \lambda_v \leq n} X_{\lambda_1} \cdots X_{\lambda_v} \quad 1 \leq v \leq n, \quad u_v \in K[X_1, \dots, X_n],$$

Entonces X_1, \dots, X_n son las raíces del polinomio

$$G_n := X^n + \sum_{v=1}^n (-1)^v u_v X^{n-v} = \prod_{v=1}^n (X - X_v)$$

en la indeterminada X , sobre el campo $K'_n := K(u_1, \dots, u_n)$ y $E'_{G_n} := K(X_1, \dots, X_n)$ su campo de descomposición sobre K'_n . Sea

$$\rho : K[U_1, \dots, U_n] \rightarrow K[u_1, \dots, u_n]$$

el homomorfismo inducido por $U_n \mapsto u_n$, o sea $\rho(P(U_1, \dots, U_n)) := P(u_1, \dots, u_n)$. De forma análoga sea

$$\sigma : K[X_1, \dots, X_n] \rightarrow K[\alpha_1, \dots, \alpha_n]$$

el homomorfismo $\sigma(P(X_1, \dots, X_n)) := P(\alpha_1, \dots, \alpha_n)$. ρ es inyectiva: Sea $P \in \ker \rho$, entonces $P(u_1, \dots, u_n) = 0 \in K[X_1, \dots, X_n]$, ya que $K[u_1, \dots, u_n] \subseteq K[X_1, \dots, X_n]$. Aplicando σ , obtenemos $0 = \sigma(P(u_1, \dots, u_n)) = P(U_1, \dots, U_n) = P$. Como ρ es sobreyectiva, es ρ un isomorfismo y posee una extensión natural a un K -isomorfismo

$$\hat{\rho} : K_n \rightarrow K'_n.$$

La extensión canónica

$$\hat{\rho}_* : K_n[X] \rightarrow L'_n[X]$$

mapea P_n en G_n . Por teorema 12.18, existe un isomorfismo

$$\psi : E_{P_n} \rightarrow E'_{G_n},$$

tal que $\psi|_{K_n} = \hat{\rho}$ y $\psi[\{\alpha_1, \dots, \alpha_n\}] = \{X_1, \dots, X_n\}$. Entonces vale que

$$\mathfrak{G}(E_{P_n} : K_n) \simeq \mathfrak{G}(E'_{G_n} : K'_n)$$

y basta calcular $\mathfrak{G}(E'_{G_n} : K'_n)$. Vamos a mostrar que el homomorfismo inyectivo

$$\Phi : \mathfrak{G}(E'_{G_n} : K'_n) \rightarrow \mathfrak{S}_n$$

es sobreyectivo. En efecto, sea $\tau \in \mathfrak{S}_n$, entonces τ induce un elemento $\varphi_\tau \in \mathfrak{G}(E'_{G_n} : K'_n)$, por medio de $\varphi_\tau(X_v) := X_{\tau(v)}$, ya que G_n es irreducible en $K'_{G_n} = K[U_1, \dots, U_n]$ y todas sus raíces X_1, \dots, X_n son conjugadas y

$$\varphi_\tau(u_v) = \sum_{1 \leqslant \lambda_1 < \lambda_2 < \dots < \lambda_v \leqslant n} X_{\tau(\lambda_1)} \cdots X_{\tau(\lambda_v)} = u_v,$$

ya que la sumatoria abarca a todas las combinaciones posibles de v elementos del conjunto de n elementos S_n y entonces $\Phi(\varphi_\tau) = \tau$. Por lo tanto

$$\mathfrak{G}(E'_{G_n} : K'_n) \simeq \mathfrak{S}_n.$$

Como $n \geq 5$, \mathfrak{S}_n no es soluble. Por lo tanto $P_n(x) = 0$ no es soluble por radicación. \square

12.3. Construcción con Regla y Compás

Finalmente terminamos este capítulo con una aplicación de la teoría de extensión de campos y teoría de Galois al problema de construcción con regla y compás en la geometría elemental. Ya desde la antigüedad son conocidos los siguientes problemas clásicos:

1. Problema de la cuadratura del círculo: Dado un círculo de radio r , ¿Es posible construir un cuadrado, con la ayuda de regla y compás, que tenga la misma área del círculo?
2. Problema de Deli: Dado un cubo de arista de longitud l , ¿Es posible, con regla y compás, construir un cubo de arista l' cuyo volumen sea el cuadrado del volumen del cubo de arista l ?
3. Construcción del polígono regular de n lados. ¿Para cuáles valores de n es posible, con regla y compás, construir un polígono de n lados?
4. Problema de la trisección de un ángulo α . ¿Para cuáles valores de α es posible, con regla y compás dividir el ángulo en tres partes iguales?

Empezaremos definiendo lo que entenderemos por el concepto de *constructibilidad*. Sea \mathbb{R}^2 el plano euclídeo real y M un subconjunto del \mathbb{R}^2 que contenga por, lo menos, dos puntos. Decimos que una recta g es *construible* a partir del conjunto M , si g contiene dos puntos de M . Diremos que un círculo C es *construible* a partir del conjunto M , si su centro está en M y si su radio coincide con la distancia entre dos puntos de M . Por $G(M)$ denotaremos al conjunto de todas las rectas y círculos construibles a partir de M . Diremos que un punto $P \in \mathbb{R}^2$ es *construible* a partir de M , si existen elementos $A, B \in G(M)$, $A \neq B$, tales que $P \in A \cap B$. Denotaremos por $M^{(1)}$ al conjunto de todos los puntos del \mathbb{R}^2 construibles a partir de M . Definimos el conjunto $M^{(n)} := (M^{(n-1)})^{(1)}$, para $n \geq 2$ y

$$\Omega(M) := \bigcup_{n=1}^{\infty} M^{(n)}.$$

$\Omega(M)$ es entonces el conjunto de todos los puntos de \mathbb{R}^2 que pueden ser construidos a partir de M en un número finito de pasos, consistentes en intersecciones sucesivas de rectas y círculos en $G(M)$. Decimos entonces que un punto $P \in \mathbb{R}^2$ es *construible con regla y compás*, a partir de M , Ssi $P \in \Omega(M)$.

El siguiente teorema nos resume las propiedades básicas de $\Omega(M)$:

TEOREMA 12.91. *Sean M, N dos subconjuntos del \mathbb{R}^2 , contenido cada uno, al menos, dos puntos. Entonces vale:*

- a) $M \subseteq M^{(1)}$.
- b) $M^{(m)} \subseteq M^{(n)}$, si $m \leq n$.
- c) $\Omega(\Omega(M)) = \Omega(M)$.
- d) $M \subseteq N \Rightarrow M^{(n)} \subseteq N^{(n)}$, $\forall n$ y $\Omega(M) \subseteq \Omega(N)$.
- e) Si $M \subseteq N \subseteq \Omega(M)$, entonces $\Omega(M) = \Omega(N)$.

DEMOSTRACIÓN.

- a) Sea $P \in M$, como M contiene, al menos, dos puntos, existe un punto $Q \in M$, $P \neq Q$ y podemos construir la recta $g := (P, Q)$ y el círculo C con centro en Q y radio $r := d(P, Q)$, entonces $P \in g \cap C$. Por lo tanto $P \in M^{(1)}$.
- b) Inmediato de a).
- c) Basta mostrar que $(\Omega(M))^{(1)} \subseteq \Omega(M)$, ya que entonces, por a), $(\Omega(M))^{(1)} = \Omega(M)$, de donde resulta que $(\Omega(M))^{(n)} = \Omega(M)$, $\forall n$ y $\Omega(\Omega(M)) = \Omega(M)$. Sea, pues, $P \in (\Omega(M))^{(1)}$, entonces existen elementos $A, B \in G(\Omega(M))$, tales que $P \in A \cap B$. Los objetos A, B que son rectas o círculos en $G(\Omega(M))$, son construidos a partir de un número finito de puntos $P_1, \dots, P_n \in \Omega(M)$, por lo que existe un entero positivo n , tal que $P_\mu \in M^{(n)}$, $\forall \mu = 1, \dots, m$, Entonces $P \in (M^{(n)})^{(1)} = M^{(n+1)} \subseteq \Omega(M)$.
- d) $M^{(1)} \subseteq N^{(1)}$ es obvio. El caso general se obtiene de forma sencilla procediendo por inducción sobre n . De $M^{(n)} \subseteq N^{(n)}$, $\forall n$ resulta $\Omega(M) \subseteq \Omega(N)$.
- e) De c) y d) se obtiene $\Omega(M) \subseteq \Omega(N) \subseteq \Omega(\Omega(M)) = \Omega(M)$. Por lo tanto $\Omega(M) = \Omega(N)$.

□

Otra propiedad sencilla de $\Omega(M)$ nos la da el siguiente

TEOREMA 12.92. *Sea M un subconjunto del \mathbb{R}^2 , que contiene, al menos, dos puntos. Dada la recta $g := (AB) \in G(\Omega(M))$. Entonces vale:*

- a) Si $C \in \Omega(M)$, $C \notin g$, entonces la paralela g' a g por C es construible a partir de $\Omega(M)$.

- b) Dado $C \in \Omega(M)$, entonces la perpendicular a g por el punto C es construible a partir de $\Omega(M)$.

DEMOSTRACIÓN.

- a)) La recta g se obtiene a partir de dos puntos $A, B \in \Omega(M)$. La configuración de los puntos A, B, C la completamos con un punto E , de forma tal que A, B, C, E formen un paralelogramo. El punto E se obtiene como intersección de los círculos C_1 , con centro en C y radio $r_1 = d(A, B)$, y el círculo C_2 , con centro en B y radio $r_2 := d(A, C)$. (Ver figura 12.2).

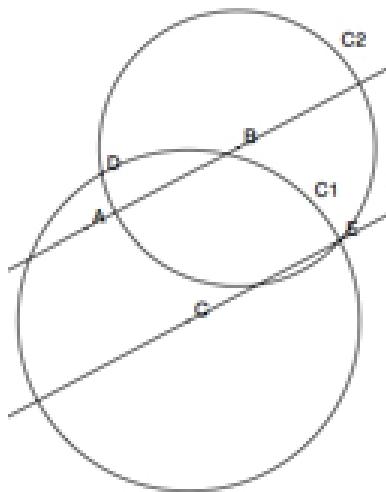


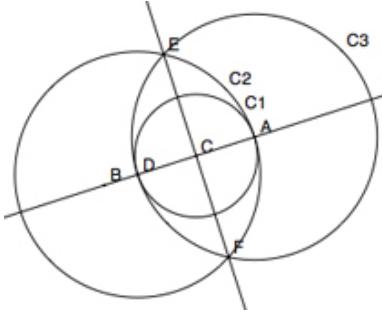
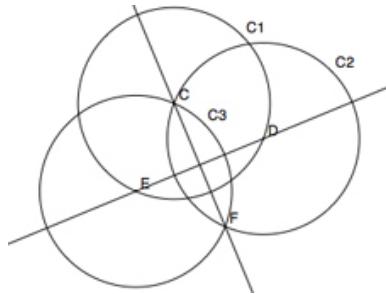
FIGURA 12.2. Paralela a recta (AB)

- b) Existen dos casos:

1. $C \in g$: El objetivo es construir un rombo cuyas diagonales pasen por C . A tal efecto, seleccionamos un punto $A \in g$ y trazamos un círculo C_1 con centro en C que pase por A , e intersecte a g en el punto D , luego trazamos un círculo C_2 con centro en D que pase por A y un círculo C_3 con centro en A que pase por D . $C_2 \cap C_3 = \{E, F\}$, los puntos A, D, E, F forman un rombo. Entonces la recta (EF) es perpendicular a la recta (AB) . (Ver figura 12.3)
2. $C \notin g$: El objetivo nuevamente es construir un rombo que tenga como esquinas al punto C y dos puntos sobre la recta g . A tal efecto escogemos un punto D sobre la recta g que no quede al pie de C y trazamos el círculo C_1 con centro en C y que pase por D , el cual intersecta a g en el punto E . Seguidamente trazamos un círculo C_2 con centro en E que pase por C y un círculo C_3 con centro en D y radio $r_3 := d(C, D)$, entonces $C_2 \cap C_3 = \{C, F\}$ entonces la recta (CF) es la perpendicular buscada. (Ver figura 12.4)

□

Para aplicar la teoría de Galois a los problemas de constructibilidad tenemos que aclararnos de qué manera interviene el álgebra en dicho problema. Empecemos por identificando \mathbb{R}^2 con el plano complejo \mathbb{C} . Como el conjunto M posee, al menos, dos elementos,

FIGURA 12.3. Perpendicular por punto C sobre g FIGURA 12.4. Perpendicular por punto $C \notin g$

entonces podemos escoger dos puntos $A, B \in M$, $A \neq B$, y darnos un sistema de referencia, tales que la recta $g := (AB)$ coincida con el eje x que identificaremos con \mathbb{R} , A posea la coordenada $(0, 0)$ y B la coordenada $(1, 0)$ y $d(A, B) = 1$. Entonces la recta $g := (AB)$ y el círculo de radio $r := 1$ y centro en A están en $G(M)$ y también la perpendicular g' a la recta g por el punto A está en $G(M)$, la cual la podemos identificar con el eje imaginario iy .

Se tiene el siguiente teorema que involucra a números complejos:

TEOREMA 12.93.

1. $i \in \Omega(M)$.
2. $z \in \Omega(M) \Rightarrow \bar{z} \in \Omega(M)$.
3. Un número complejo $z := re^{i\psi} \in \Omega(M)$, Ssi $r, e^{i\psi} \in \Omega(M)$.

DEMOSTRACIÓN.

1. Ya vimos que el eje imaginario iy y el círculo $C1$ de radio $r_1 := 1$ con centro en el origen están en $G(\Omega(M))$. Por consiguiente $i \in iy \cap C1$, lo que implica que $i \in \Omega(M)$.
2. Si $z \in \mathbb{R}$ no hay nada que demostrar. Supongamos, pues, que $z \notin \mathbb{R}$. Entonces por el teorema 12.92, la perpendicular al eje real, por el punto z , g , está en $G(\Omega(M))$, al igual que el círculo $C1$ de radio $r_1 := |z|$ y $w := \bar{z} \in g \cap C1$. Por lo tanto $\bar{z} \in \Omega(M)$. (Ver figura 12.5)
3. Como el eje real y el círculo $C1$ de radio $r_1 := 1$ están en $G(\Omega(M))$, tenemos que con $z := re^{i\psi}$ también r y $w := e^{i\psi}$ están en $\Omega(M)$. r se obtiene como uno

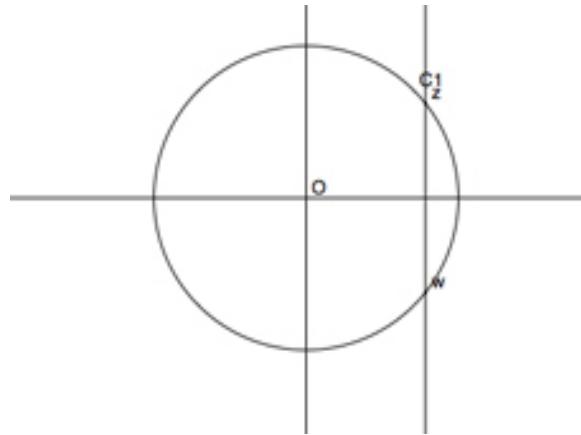
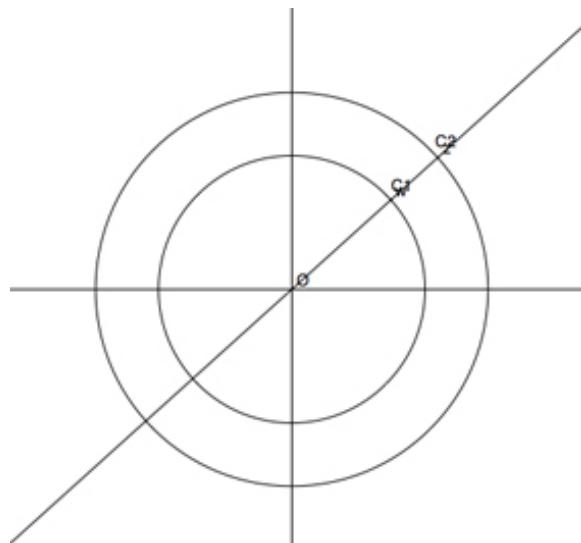


FIGURA 12.5. Conjugado

de los puntos de la intersección del círculo C_2 de radio r , que también está en $G(\Omega(M))$, con el eje real y w como uno de los puntos de la intersección de la recta $g := \lambda z$, que también está en $G(\Omega(M))$, con el círculo C_1 . (Ver figura 12.6). Por otra parte, si r y $w := e^{i\psi}$ están en $\Omega(M)$, entonces la recta $g := \lambda w$ y el círculo C_2 de radio r están en $G(\Omega(M))$ y $z := re^{i\psi}$ se obtiene como uno de los puntos de $g \cap C_2$.

FIGURA 12.6. $z := re^{i\psi}$

□

TEOREMA 12.94. $\Omega(M)$ es un campo.

DEMOSTRACIÓN. Basta mostrar lo siguiente:

- a) $z, w \in \Omega(M) \Rightarrow z - w \in \Omega(M)$.
b) $z, w \in \Omega(M), w \neq 0 \Rightarrow \frac{z}{w} \in \Omega(M)$.

- a) Con $z, w \in \Omega(M)$, la recta $g := \lambda w$, su paralela g' por z , el círculo C_1 con centro en z y radio $r_1 := |w|$, así como el círculo C_2 de radio $r := |w|$ con centro en el origen, están en $G(\Omega(M))$. Entonces $v := -w$ está en $\Omega(M)$ pues resulta de la intersección de g con C_2 . El punto $A := z + v = z - w$ resulta de la intersección de g' con el círculo C_1 . (Ver figura 12.7)

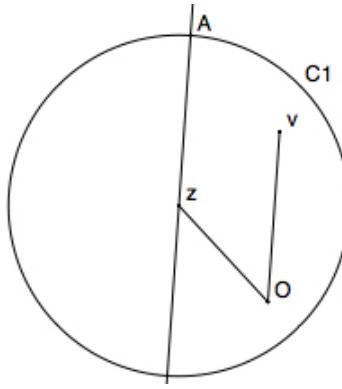


FIGURA 12.7. $A := z - w$

- b) Sean $z := re^{i\phi}, w := se^{i\psi} \in \Omega(M), w \neq 0, \frac{z}{w} = \frac{r}{s}e^{i(\phi-\psi)}$. Debemos mostrar que $\frac{r}{s}$ y $e^{i(\phi-\psi)}$ están en $\Omega(M)$. En efecto, como $1, i \in \Omega(M)$, también $v := 1 + i = 1 - (-i) \in \Omega(M)$ y la recta $g := \lambda v \in G(\Omega(M))$. También los círculos C_1 y C_2 de radios $r_1 := s$ y $r_2 := r$ respectivamente, están en $G(\Omega(M))$. Sea a el punto de intersección de la recta g con el círculo C_1 y b el punto de intersección de la recta g con el círculo C_2 , entonces $a, b \in \Omega(M)$. Sean g_1 la recta $(1a) \in G(\Omega(M))$, g_2 la recta paralela a g_1 por b y c el punto de intersección de g_2 con el eje x . Entonces $c \in \Omega(M)$ y utilizando el teorema de las proporciones

$$c = \frac{c}{1} = \frac{|b|}{|a|} = \frac{r}{s} \in \Omega(M).$$

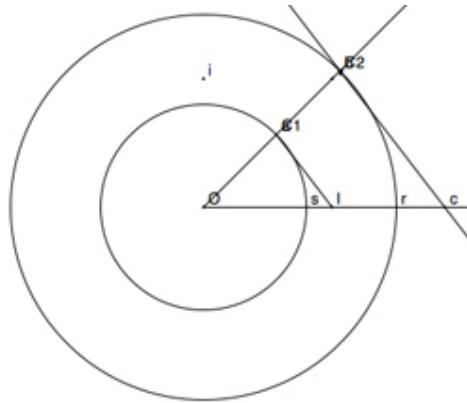
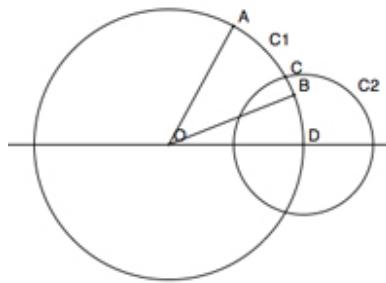
Falta mostrar que $\omega := e^{i(\phi-\psi)} \in \Omega(M)$. Como $A := e^{i\phi}$ y $B := e^{i\psi}$ están en $\Omega(M)$, y el punto D que es intersección del eje x con el círculo C_1 de radio $r_1 := 1$ y centro en el origen O , también está en $\Omega(M)$, entonces el círculo C_2 con centro en D y radio $r_2 := d(A, B)$ está en $G(\Omega(M))$. Entonces obtenemos $C := e^{i(\phi-\psi)}$ como punto de intersección de C_1 y C_2 . (Ver figura 12.9)

□

Como un corolario del teorema 12.94, cuya demostración dejamos al lector, se tiene el siguiente resultado:

COROLARIO 12.95. *El campo \mathbb{Q} de los números racionales está contenido en $\Omega(M)$.*

TEOREMA 12.96. *Si $z \in \Omega(M)$, entonces también $\sqrt{z} \in \Omega(M)$.*

FIGURA 12.8. Cociente $\frac{z}{w}$ FIGURA 12.9. $C := e^{i(\phi - \psi)}$

DEMOSTRACIÓN. Basta mostrar que $\sqrt{r} \in \Omega(M)$, para cualquier número positivo $r \in \Omega(M)$ y $e^{i\frac{\phi}{2}} \in \Omega(M)$.

En efecto, sea $r \in \Omega(M)$, $r > 0$ y supongamos de primero que $r > 1$. Sea la recta g una paralela al eje imaginario, que pasa por 1. Con r también $A := r + 1$, $B := \frac{r+1}{2}$ están en $\Omega(M)$ y por consiguiente el círculo $C1$ con centro en B y radio $r_1 := \frac{r+1}{2}$ está en $G(\Omega(M))$. Entonces el punto de intersección a de la recta g con $C1$ está en $\Omega(M)$. Consideremos el triángulo rectángulo formado por los puntos $a, 1, B$, entonces por pitágoras tenemos:

$$(d(1, a))^2 = (d(B, a))^2 - (d(1, B))^2 = \left(\frac{1+r}{2}\right)^2 - \left(\frac{1+r}{2} - 1\right)^2 = r.$$

Entonces $d(1, a) = \sqrt{r}$. (Ver figura 12.10). Si $0 < r < 1$, aplicamos el procedimiento a $\frac{1}{r}$.

El caso $r = 1$ es trivial. Si $A := e^{i\phi} \in \Omega(M)$, entonces la recta $g := \lambda e^{i\phi}$ y su paralela g' por el punto 1 están en $G(\Omega(M))$, así como también el círculo $C2$ con centro en 1 y radio $r_2 := 1$. Si B es el punto de intersección del círculo $C2$ con la recta g' , entonces los puntos $O, 1, A, B$ forman un rombo y obtenemos el punto $C := e^{i\frac{\phi}{2}}$ como intersección de $C1$ y el segmento $[OB]$. (Ver figura 12.11) \square

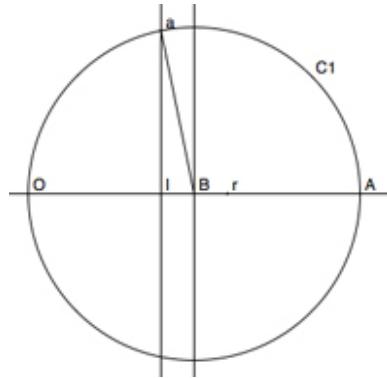
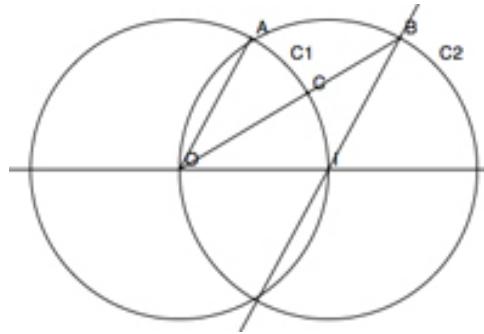


FIGURA 12.10. Raíz cuadrada

FIGURA 12.11. $C := e^{i\frac{\phi}{2}}$

Ahora que hemos visto las principales propiedades de $\Omega(M)$, estamos en condiciones de estudiar sus propiedades algebraicas, que nos permitirán relacionar el problema de construcción con la teoría de Galois y extensión de campos. Bajo las condiciones que planteamos arriba sobre M y los teoremas demostrados, el lector comprobará que $\mathbb{Q} \subseteq \Omega(M)$. Si $\kappa := \mathbb{Q}(M, \bar{M})$, donde

$$\bar{M} := \{\bar{z} \mid z \in M\}.$$

Obviamente $\bar{\kappa} = \kappa$ y $\Omega(M)$ es una extensión de κ .

El siguiente teorema nos caracteriza a los puntos de $\Omega(M)$:

TEOREMA 12.97. *Sea $z \in \mathbb{C}$. Entonces las siguientes condiciones son equivalentes:*

- a) $z \in \Omega(M)$.
- b) Existe una cadena de campos

$$K_0 := \kappa \subseteq K_1 \subseteq \cdots \subseteq K_m := K \subseteq \mathbb{C}.$$

tal que $z \in K$ y $[K_\mu : K_{\mu-1}] \leq 2$, para $1 \leq \mu \leq m$.

- c) El grado del polinomio de descomposición del polinomio minimal de z sobre κ es una potencia de 2.

- d) z está en una extensión finita de Galois de κ cuyo grado sobre κ es una potencia de 2.

DEMOSTRACIÓN.

- b) \Rightarrow c) Supongamos que para un determinado μ , $1 \leq \mu \leq m$, $[K_\mu : K_{\mu-1}] = 2$. entonces existe un $b_\mu \in K_\mu$, cuyo polinomio minimal P_μ es de grado 2 sobre $K_{\mu-1}$ y $K_\mu = K_{\mu-1}(b_\mu)$. Sea, entonces

$$P_\mu := X^2 + cX + d = (X + \frac{c}{2})^2 + d - \frac{c^2}{4}.$$

Entonces

$$\beta_\mu := \sqrt{c^2 - 4d}$$

es un elemento primitivo de la extensión

$$\begin{array}{ccc} & K_\mu & \\ & | & \\ & K_{\mu-1} & \end{array}$$

Entonces, para cada μ , $1 \leq \mu \leq m$ podemos encontrar un elemento $a_{\mu-1} \in K_{\mu-1}$, tal que $K_\mu = K_{\mu-1}(\sqrt{a_{\mu-1}})$. Vamos a mostrar la siguiente proposición:

(A) Si

$$K_0 := \kappa \subseteq K_1 \subseteq \cdots \subseteq K_m := K \subseteq \mathbb{C}$$

es una cadena de campos, tal que $K_\mu := K_{\mu-1}(\sqrt{a_{\mu-1}})$, para $1 \leq \mu \leq m$, entonces existe una extensión de Galois $E \subseteq \mathbb{C}$ sobre K_0 que contiene a K y para la cual existe una cadena de campos

$$K_0 := \kappa \subseteq E_1 \subseteq \cdots \subseteq E_l := E \subseteq \mathbb{C},$$

tal que $[E_\lambda : E_{\lambda-1}] \leq 2$, para $1 \leq \lambda \leq l$.

De (A) resulta c): La extensión E es normal sobre κ , por ser de Galois y E contiene al campo de descomposición del polinomio minimal P de z sobre κ . Por consiguiente $\text{grad } P \mid [E : \kappa]$. Como $[E : \kappa]$ es una potencia de 2, resulta que $\text{grad } P$ debe ser también una potencia de 2.

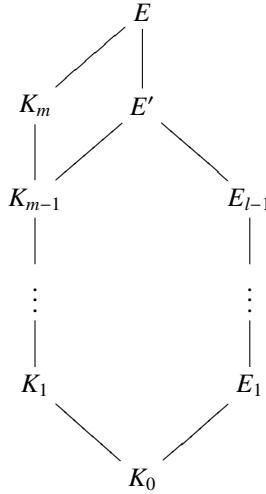
Mostremos ahora que (A) vale: Por inducción sobre m . Para $m = 1$ no hay nada que mostrar. Sea entonces $m > 1$ y supongamos, por hipótesis de inducción que (A) es cierto para todo entero $n \leq m - 1$. Entonces para la cadena

$$K_0 := \kappa \subseteq K_1 \subseteq \cdots \subseteq K_{m-1},$$

existe un campo E' que cumple con las propiedades especificadas en (A). Sea

$$G := \prod_{\varphi \in \mathfrak{G}(E' : K_0)} (X^2 - \varphi(a_{m-1}))$$

Entonces $G \in K_0[X]$, ya que $\psi(G) = G$, $\forall \psi \in \mathfrak{G}(E' : K_0)$. Sea E el campo de descomposición de G sobre E' . Como E' es de Galois sobre K_0 , E' es normal y es campo de descomposición de un polinomio $Q \in K_0[X]$. Entonces E es campo de descomposición del polinomio $GQ \in K_0[X]$ y como tal es de Galois sobre K_0 . Obviamente E es una extensión de $L_m = K$, ya que $(X^2 - a_{m-1}) \mid G$. La última aserción de (A) resulta del siguiente diagrama de extensiones sucesivas:



c) \Rightarrow d) Resulta de la demostración de (A).

d) \Rightarrow a) Vamos a mostrar que si K es una extensión de Galois sobre κ , tal que $[K : \kappa] = 2^m$, para algún $n \in \mathbb{N}$, entonces $K \subseteq \Omega(M)$. Por inducción sobre m . Si $m = 0$, no hay nada que demostrar. Sea entonces $m > 0$ y supongamos, por hipótesis de inducción, que la aserción es válida para todo entero $n \leq m$ y mostremos que vale para m . En efecto, si $[K : \kappa] = 2^m$, entonces $\mathcal{G}(K : \kappa) = 2^m$. Entonces, por teorema 4.28, el centro $Z(\mathcal{G}(K : \kappa)) \neq \{e\}$, por lo que existe un subgrupo normal $H \subseteq Z(\mathcal{G}(K : \kappa))$ de orden 2. Para $E := \text{Fix } H$, vale entonces $[K : E] = 2$, $[E : \kappa] = 2^{m-1}$ y, por el teorema 12.60, E es de Galois sobre κ . Por la hipótesis de inducción $E \subseteq \Omega(M)$. Como $[K : E] = 2$, vimos arriba que entonces existe $a \in E$, tal que $K := E(\sqrt{a})$. Como $a \in \Omega(M)$, por teorema 12.96, también $\sqrt{a} \in \Omega(M)$. Por lo tanto $K := E(\sqrt{a}) \subseteq \Omega(M)$.

a) \Rightarrow b) Vamos a mostrar primero lo siguiente:

(B) Si $N \subseteq \mathbb{C}$ es un subconjunto que posee, al menos, dos puntos, entonces todo elemento $z \in N^{(1)}$, al igual que $\bar{z} \in N^{(1)}$ son de grado ≤ 2 , sobre $K := \mathbb{Q}(N, \bar{N})$.

$z \in N^{(1)}$ implica que existen dos elementos $A, B \in G(N)$, $A \neq B$, tales que $z \in A \cap B$. Aquí vamos a diferenciar tres casos posibles:

i) A, B son dos rectas en \mathbb{C} , Es decir que los puntos de cada una satisfacen una ecuación paramétrica de la forma

$$w(t) = a + ct, \quad a, c \in \mathbb{C}, \quad c \neq 0, \quad t \in \mathbb{R}.$$

Como $t \in \mathbb{R}$, $t = \bar{t}$ y se obtiene la ecuación

$$\bar{c}(w - a) = c(\bar{w} - \bar{a})$$

Esto quiere decir que si z está sobre una determinada recta en \mathbb{C} , su conjugado \bar{z} está en la recta conjugada. Entonces si $z \in A \cap B$ debe existir un $t_0 \in \mathbb{R}$, tal que

$$z = a + ct_0 = b + dt_0, \quad a, b, d, c \in N.$$

Es decir que z y \bar{z} deben ser solución del sistema de ecuaciones

$$(12.53) \quad \bar{c}(w - a) - c(\bar{w} - \bar{a}) = 0$$

$$(12.54) \quad \bar{d}(w - b) - d(\bar{w} - \bar{b}) = 0$$

Como los coeficientes del sistema de ecuaciones están todos en K , resulta que también $z, \bar{z} \in K$, y son de grado $1 < 2$.

- ii) A es una recta y B es un círculo. Entonces los puntos sobre la recta A satisfacen una ecuación de la forma:

$$\bar{c}(w - a) = c(\bar{w} - \bar{a}), \quad a, c \in K, c \neq 0,$$

y los puntos sobre el círculo B una ecuación de la forma

$$(w - d)(\bar{w} - \bar{d}) = s, \quad d \in N$$

y s es el cuadrado de la distancia entre dos puntos de N . Nuevamente, si z satisface el sistema de estas dos ecuaciones, también lo hace \bar{z} , de la primera ecuación se obtiene

$$\bar{z} = \frac{\bar{c}(z - a)}{c} + \bar{a}.$$

Substituyendo en la segunda ecuación se obtiene una ecuación polinómica de segundo grado en z con coeficientes en K y lo mismo para \bar{z} . Por lo tanto $\text{grad } z = \text{grad } \bar{z} \leq 2$.

- iii) A, B son círculos. Entonces si $z \in A \cap B$, z debe satisfacer el sistema de ecuaciones

$$(12.55) \quad (z - a)(\bar{z} - \bar{a}) = r,$$

$$(12.56) \quad (z - b)(\bar{z} - \bar{b}) = s,$$

donde $a, b, r, s \in K$ y $a \neq b$. Substrayendo la segunda ecuación de la primera, se obtiene, poniendo

$$c := r - s + b\bar{b} - a\bar{a},$$

el sistema de ecuaciones

$$(12.57) \quad (\bar{b} - \bar{a})w + (b - a)\bar{w} = c$$

$$(12.58) \quad (w - b)(\bar{w} - \bar{b}) = s.$$

Como $a - b \neq 0$, el problema se reduce al caso ii). La primera ecuación corresponde a la ecuación del llamado *eje radical*, que es una recta que pasa por los puntos de intersección de los dos círculos.

Sea entonces $z \in \Omega(M)$, entonces existe un número natural n , tal que $z \in M^{(n)}$. Por consiguiente existe un número finito de puntos en $M^{(n-1)}$ a partir de los cuales fue construido z y lo mismo podemos decir de los puntos de $M^{(n-1)}$. Por consiguiente existe una sucesión finita de puntos z_1, \dots, z_m tales que:

1. $z_m := z$
2. para $\mu = 2, \dots, m$, z_μ es construible a partir de $M \cup \{z_1, \dots, z_{\mu-1}\}$
3. z_1 es construible a partir de M .

Sea $N_1 := M$ y $N_\mu := M \cup \{z_1, \dots, z_{\mu-1}\}$, para $2 \leq \mu \leq m$. Por (B) son, entonces z_μ, \bar{z}_μ elementos de grado ≤ 2 sobre $K := \mathbb{Q}(N, \bar{N}) = \kappa(z_1, \dots, z_m, \bar{z}_1, \dots, \bar{z}_m)$. Por lo tanto vale b).

□

Finalmente con base a la teoría desarrollada hasta aquí, entremos a analizar algunos de los problemas de construcción que fueron quebraderos de cabeza para los matemáticos griegos de la antigüedad y que mencionáramos al inicio de esta sección.

1. Problema de la cuadratura del círculo: Construir con regla y compás un cuadrado de lado l , tal que su área coincida con el área de un círculo de radio $r := 1$. Es decir que $l^2 = \pi$, de donde $l = \sqrt{\pi}$. Dandonos un círculo de radio $r := 1$, tenemos entonces que $M := \{0, 1\}$. Si $\alpha := \sqrt{\pi} \in \Omega(M)$, entonces también $\alpha^2 = \pi \in \Omega(M)$ y π sería algebraico sobre $\kappa := \mathbb{Q}(M, \bar{M}) = \mathbb{Q}$, es decir π sería un número algebraico, lo cual no es cierto.

Los matemáticos griegos y de la antigüedad nunca pudieron dar respuesta a este problema, pues la trascendencia del número π no fue demostrada hasta en el año 1882, por el matemático alemán Karl Ferdinand Lindemann, en su artículo “Über die Zahl π ”, ver [16].

2. El problema de Deli: Dado un cubo K de arista $l = 1$, construir con regla y compás la arista l' de un cubo K' , cuyo volumen sea el doble del volumen de K . Es decir que $l^3 = s$, o sea $l' = \sqrt[3]{2}$. Nuevamente nuestro conjunto $M \setminus \{0, 1\}$ y $\kappa := \mathbb{Q}(M, \bar{M}) = \mathbb{Q}$. La pregunta es entonces si $\alpha := \sqrt[3]{2} \in \Omega(M)$. Como $\text{grad } \alpha = \text{grad } \sqrt[3]{2} = 3$ sobre \mathbb{Q} y 3 no es potencia de 2, entonces $\alpha \notin \Omega(M)$, por lo que dicho cubo no puede ser construido con regla y compás.
3. Construcción del polígono regular de n lados: La respuesta nos la da el siguiente teorema de Gauss:

TEOREMA 12.98 (Teorema de Gauss). *El n -polígono regular es construible con regla y compás, Ssi $\phi(n)$ es una potencia de 2. Donde ϕ es la función de Euler.*

DEMOSTRACIÓN. Sabemos que las n -raíces de la unidad forman sobre el círculo de radio $r := 1$ un n -polígono regular, por lo que nuestro problema se traduce en términos algebraicos de la siguiente forma: Dado $M = \{0, 1\}$, ¿Para qué valores de n está una n -raíz primitiva de la unidad en $\Omega(M)$? Como sabemos las n -raíces primativas de la unidad son las raíces del polinomio ciclotómico F_n , el cual, por teorema 12.75, es irreducible en $\mathbb{Q}[X]$, por consiguiente F_n es su polinomio minimal y $\text{grad } F_n = \phi(n)$. Por lo tanto un n -polígono regular es construible con regla y compás, Ssi $\phi(n)$ es una potencia de 2. \square

Cabe ahora preguntarnos ¿Cuándo es $\phi(n)$ una potencia de 2? Si $n = p_1^{r_1} \cdots p_m^{r_m}$, entonces, por lema 7.8, se tiene

$$\phi(n) = \phi(p_1) \cdots \phi(p_m) = \prod_{\mu=1}^m p_1^{r_\mu} \left(1 - \frac{1}{p_\mu}\right) = \prod_{\mu=1}^m (p_\mu - 1) p_\mu^{r_\mu - 1} = p_1^{r_1 - 1} \cdots p_m^{r_m - 1} (p_1 - 1) \cdots (p_m - 1).$$

Entonces $\phi(n)$ es una potencia de 2, Ssi para todos los primos $p_\mu \neq 2$, $r_\mu = 1$ y $p_\mu - 1$ es una potencia de 2.

Decimos que un número primo impar p es un *número primo de Fermat*, si $p - 1$ es una potencia de 2.

Entonces podemos concluir lo siguiente:

TEOREMA 12.99. *El n -polígono regular es construible con regla y compás, Ssi n posee la representación*

$$n = 2^r p_1 \cdots p_m,$$

donde los p_μ son primos de Fermat.

El siguiente teorema nos caracteriza a los primos de Fermat:

TEOREMA 12.100. *Si p es un primo de Fermat, entonces p posee la representación*

$$p = 2^{2^t} + 1,$$

donde t es un número natural.

DEMOSTRACIÓN. Si s es un número impar, entonces -1 es una raíz del polinomio $X^s + 1$ y

$$X^s + 1 = G(X + 1),$$

donde $G \in \mathbb{Z}[X]$. Si r es cualquier entero positivo, Substituyendo X por 2^r obtenemos

$$(12.59) \quad 2^{rs} + 1 = (2^r)^s + 1 = (2^r + 1)G(2^4).$$

Si m no fuera una potencia de 2, entonces existiría un s impar y un entero positivo r , tal que $m = sr$ y por la ecuación (12.59), $2^m + 1$ no podría ser primo. Por consiguiente $m = 2^t$, para algún número natural t . \square

No todos los números de la forma $n = 2^{2^t} + 1$ resultan ser primos. Un caso conocido, pero difícil de probar, por su gran magnitud, es el número $n = 2^{2^5} + 1 = 4294967297$. Sin embargo podemos afirmar que para los siguientes valores de n , el n -polígono es construible con regla y compás:

$$n = 3, 4, 5, 6, 8, 10, 12, 15, 16, 17, 20.$$

Mientras que para los siguientes valores de n no es posible construir el n -polígono:

$$n = 7, 9, 11, 13, 14, 18, 19.$$

4. La trisección de un ángulo: Dado un ángulo cualquiera ¿Es posible, con regla y compás, dividir dicho ángulo en tres partes iguales? La respuesta es que no, pues si fuera posible, entonces del triángulo equilátero podríamos construir el polígono de 9 lados, el cual no es construible, por no tener la descomposición en números primos requerida.

Bibliografía

1. Anton, Howard, *Elementary Linear Algebra*, Second Edition, John Wiley & Sons, 1977.
2. Atiyah, M.F. and I. MacDonald, *Introduction to Commutative Algebra*, Addison-Wesley Publishing Company, inc., 1969.
3. Atiyah, M.F, *K-Theory*, Editorial Benjamin 1988
4. Ayres, Frank, Jr., *Modern Algebra*, Schaum Publishing co., 1965
5. Cohn, P.M., *Universal Algebra*, Harper and Row, 1965.
6. Cohen, P.J., *Set Theory and Continuum Hypothesis*, Benjamin. 1963.
7. Dieudonné, J., *Cours de Géometrie Algébrique*, Presses Univ. France, 1974.
8. Escamilla, Juan F., *Introducción a la Topología*, Editorial Lulu, 2007.
9. Fulton, W. *Algebraic Curves*, New York: W.A. Benjamin, Inc., 1969.
10. Gramain, André, *Topologie des Surfaces*, Presses Universitaires de France, 1971.
11. Halmos, Paul, *Naive Set Theory*, Princeton/New York/Toronto/London 1960.
12. Herstein, I.N., *Topics in Algebra*, Second Edition, John Wiley & Sons, 1975.
13. Kendig, Keith, *Elementary Algebraic Geometry*, Springer Verlag, Ney York Berlin Heidelberg Tokyo, segunda edición, 1984.
14. Kunz, Ernst, *Introduction to Commutative Algebra and Algebraic Geometry*, Birkhäuser Verlag, Second Edition, 1991.
15. Lang, Serge, *Algebra*, Second Edition, Addison-Wesley Publishing Company, Inc., 1984.
16. Lindemann, F., Über die Zahl π , *Mathematische Annalen* 20, (1882), 213-225.
17. Matsumura, H., *Commutative Algebra*, Second Edition, Benjamin, New York, 1980.
18. MacDonald, I., *Algebraic Geometry, An Introduction to Schemas*, Editorial Benjamin 1968.
19. Neugebauer, O., *Vorlesungen über Geschichte der Antiken Mathematischen Wissenschaften*, Erster Band, *Vorgriechische Mathematik*, Springer-verlag, 1969.
20. Reiffen, Hans-Jörg, Günter Scheja, Udo Vetter, *Algebra*, BI Hochschultaschenbücher, Band 110, Manheim 1969.
21. Sarges, Heidrun, *Ein Beweis des Hilbertschen Basis Satzes*, J. Reine Angew. Math., 283/284, 1976, 436-437.
22. Scholz, Erhard, *Geschichte der Algebra*, Wissenschaftsverlag, 1990.
23. Struik, Kirk J., *Abriss der Geschichte der Mathematik*, Vieweg, 1967.
24. Suppes, P., *Axiomatic Set Theory*, Princeton/New York/Toronto/London, 1960.
25. tom Dieck, Tammo., *Topologie*, de Gruyter Lehrbuch, NY 1991.
26. Wikipedia en inglés, www.wikipedia.org

Índice alfabético

- Ω_v^μ -estructura algebraica, 26
n-radical, 277
- A*-álgebra, 23, 187
libre sobre un monoide, 189
- Abel, 5
- Abu Al-Hasan, 4
- Abu Bakr, 3
- acción de grupo, 79
- Al Fajri, 3
- Al-Jwarizmi, 1, 3
- Al-Mahani, 3
- álgebra
- abstracta, 6
 - afín, 229
 - comutativa, 6
 - de Boole, 15
 - de Lie, 6
 - de Rees, 189
 - graduada, 189
 - graduada asociada, 189
 - homológica, 6
- algoritmo
- euclídeo, 32, 38
 - algoritmo euclídeo, 39
- anillo, 21, 145
- booleano, 148
 - cociente, 152, 153
 - con unidad, 22, 145
 - comutativo, 22, 145
 - de Dedekind, 177
 - de fracciones, 165
 - de polinomios, 191
 - euclídeo, 175
 - factorial o factorización única, 172
 - local, 168
 - noetheriano, 171
 - principal, 169
 - semilocal, 168
- anulador
- de un elemento, 186
 - de un ideal, 151
 - de un módulo, 186
- Apastamba, 2
- aplicación, 8
- lineal, 23, 179
- Arithmetica, 2
- Ars Magna, 4
- Aryabhata, 2
- Aryabhatiya, 2
- automorfismo, 19
- interno, 66
- axioma
- de aditividad, 24
 - de homogeneidad, 24
 - de positividad, 24
 - de selección, 11
 - de simetría, 24
- Bernoulli, 5
- Bhaskara, 3
- Bijaganita, 3
- biyección, 8
- Bombelli, 4
- boreleano, 8
- Brahmagupta, 1, 2
- cadena estacionaria
- ascendente, 171
- campo, 22, 146
- algebraicamente cerrado, 244
 - algebraicamente cerrado en, 244
 - de descomposición, 219
 - perfecto, 225
- campo de fracciones, 164
- campo primo, 216
- característica
- de un campo, 215
 - de un dominio entero, 161
- Cardano, 4
- cardinalidad
- del continuo, 10
- Cauchy, Augustin, 49
- Cayley, Arthur, 49
- centralizador, 62
- de un subgrupo, 64
- centro
- de un anillo, 148

- de un grupo, 61
- Chakravala, 2
- ciclo, 80
- clase
 - de equivalencia, 11
 - de isomorfía, 67
- clase lateral
 - derecha, 55
 - izquierda, 55
- clases
 - de congruencia, 12
- cociente, 33
- coeficiente
 - principal, 196
- complemento, 8
- complemento relativo, 8
- composición de aplicaciones, 8
- condición
 - del mínimo, 16
- conjunto, 7
 - potencia, 8
 - algebraico, 162, 227
 - bien ordenado, 13
 - cociente, 11
 - contable, 10
 - de generadores, 54
 - de primos seleccionados, 174
 - denumerable, 10
 - finito, 10
 - inductivamente ordenado, 13
 - infinito, 10
 - multiplicativo, 164
 - numeral, 15
 - parcialmente ordenado, 13
 - totalmente ordenado, 13
 - universal, 15
- comutador, 63
- construible, 292
 - con regla y compás, 292
- continuo
 - hipótesis del, 10
- contradominio, 8
- contraimagen, 8
- coproducto
 - de grupos, 137
- cota
 - inferior, 13
 - superior, 13
- cuaterniones, 25
- cuerpo, 22, 146
 - de Morgan, 8
 - leyes de, 9
 - leyes de , 8
- denominador, 44
- derivación, 221
- derivada, 221
- diagonal, 11
- diagrama
 - comutativo, 12
- diferencia de conjuntos, 8
- diferencia simétrica, 8
- Diophanto, 1, 2
- directamente irreducible, 120
- directamente reducible, 120
- discriminante, 218
- divisor, 33, 170
 - propio, 33
- divisor común, 40, 170
- divisor de cero, 145
 - propio, 145
- divisor normal, 60
- dominio, 8
 - de acción, 83
- dominio entero, 145
- ecuación
 - de clase, 62
- Eisenstein
 - criterio de, 204
- eje radical, 301
- elemento
 - algebraico, 236
 - de torsión, 122
 - inseparable, 251
 - inseparable puro, 252
 - inverso, 51
 - irreducible, 169
 - más grande, 13
 - más pequeño, 13
 - maximal, 13
 - minimal, 13
 - neutro, 17, 51
 - primitivo, 245
 - primo, 170
 - reducible, 169
 - separable, 251
 - simétrico, 17, 51
 - trascendente, 236
- elementos
 - asociados, 169
 - conjugados, 62, 247
- endomorfismo, 19
- entero
 - gaussiano, 149
 - gaussianos, 146
- envolvente
 - algebraica cerrada, 244
 - separable, 256
- epimorfismo, 19
- escalares, 23
 - campo de, 23
- espacio vectorial, 22
- espectro, 157
 - maximal, 158
 - primo, 157

- estructura algebraica, 17
- Euclides, 2
- Euler
 - función de, 42
- Euler, Leonhard, 50
- extensión
 - algebraica, 236
 - de campos, 233
 - de Galois, 261
 - inseparable pura, 251
 - normal, 247
 - radical, 282
 - radical simple, 277
 - separable, 251
 - simple, 245
 - trascendente, 236
- factorización
 - teorema de, 12
- familia de conjuntos, 8
- familia indizada, 9
- Fermat, 2, 57
 - congruencia de, 57
 - número primo de, 302
- Fibonacci, 3
- función
 - algebraica, 210
 - grado, 175
 - monomial, 210
 - polinomial o polinómica, 210
- Galois
 - grupo de, 50, 243, 259
 - teoría de, 5, 258
- Galois, Évariste, 5, 49, 258
- Gauss
 - lema de, 201
 - lema original de, 202
 - teorema de, 202
 - teorema original de, 202
- Gauss, Friedrich, 50
- grado
 - de inseparabilidad, 256
 - de separabilidad, 256
 - de un álgebra graduada, 189
 - de un monomio, 191
 - de un polinomio, 191
 - de una extensión, 234
 - reducido, 225
- Grothendieck, 134
- grupo, 18
 - abeliano, 18
 - cíclico, 54
 - cociente, 60
 - comutativo, 18
 - de automorfismos, 66, 157
 - de comutadores, 64
 - de Grothendieck, 134
 - de Lie, 50
- de los 4 de Klein, 93, 94
- de permutaciones, 77
- de simetría, 77
- de torsión, 122
- de unidades, 148
- díédrico, 94
- finitamente generado, 54
- fundamental, 142
- libre abeliano, 132
- libre de torsión, 122
- lineal, 18
- producto directo, 127
- simple, 60
- sóluble, 112
- suma directa, 130
- transitivo, 89
- grupoide, 17
- Hölder
 - teorema de, 116
- Harriot, 4
- Hilbert
 - teorema abstracto de los ceros, 167
 - teorema de la base, 203
- hipersuperficie, 227
- homomorfismo, 19
 - canónico, 68, 153
 - de A-álgebras, 24
 - de anillos, 22, 151
 - de valuación, 181
 - identidad, 65
 - interno, 65
- ideal, 149
 - bilátero, 149
 - cero, 149
 - cociente, 151
 - de álgebras, 187
 - de anulación, 228
 - derecho, 149
 - intersección, 150
 - izquierdo, 149
 - maximal, 157
 - primario, 161
 - primo, 157
 - principal, 149
 - producto, 150
 - propio, 150
 - radical, 161
 - suma, 150
- imagen, 8
- inducción
 - Noetheriana, 16
 - principio de, 15, 27
 - transfinita, 16
- ínfimo, 13
- intersección, 8
- introducción, 1
- inyección, 8

- isomorfía
 - teoremas de, 68, 180, 188
- isomorfismo, 19
- Jia Xian, 3
- Jiuzhang Suanshu, 2
- Jordan, Camille, 49
- kernel, 20, 151
- Klein, Felix, 50
- Kowa Seki, 5
- Kronecker, Leopold, 50
- Kummer, Ernst, 50
- Lagrange, Joseph, 49
- Leibniz, 4
- Leonardo de Pisa, 3
- Liber Abaci, 3
- Lie, Sophus, 50
- localización, 168
- máximo común divisor, 40, 170
- mínimo común múltiplo, 43
- módulo, 22, 179
 - de fracciones, 186
 - dual, 181
 - libre, 181
 - localizado, 186
 - producto directo, 183
 - reflexivo, 181
 - suma directa, 185
- Madhava de Sangamagramma, 4
- magma, 17
 - abeliano, 17
- Mahavira, 3
- monoide, 18
 - abeliano, 18
 - libre abeliano, 143
- monomio
 - simple, 191
- monomorfismo, 19
- morfismo, 6
- multiplicidad
 - de una raíz, 212
- núcleo
 - de homomorfismo de anillos, 151
 - de un homomorfismo, 20
- número
 - entero, 34
 - natural, 15
 - racional, 44
- números naturales, 27
- nilradical, 161
- nomenclatura, 6
- normalizador, 62
- numerador, 44
- objeto, 6
- Omar Khayyam, 3
- operación
 - n*-aria, 26
 - binaria, 17
 - cerrada, 17
 - interna, 17
- operador deslizamiento, 148
- órbita, 79
- orden
 - de un elemento, 54
 - de un grupo, 54
 - de una raíz, 212
- p*-grupo, 104
- paridad
 - de una permutación, 86
 - función de, 87
- partición, 11
 - de un entero, 90
- Pauli
 - matrices de, 19
- peano
 - axiomas de, 15, 27
- permutación, 53
 - cíclica, 81
 - circular, 81
- permutaciones, 49
 - grupo de, 49
 - semejantes, 85
- polinomio
 - ciclotómico, 273
 - de división del círculo, 273
 - homogéneo, 191
 - inseparable, 225
 - mónico, 198
 - minimal, 238
 - primitivo, 200
 - separable, 225
- predecesor, 38
- primo
 - número, 33
- primos
 - relativos, 41, 175
- producto
 - amalgulado, 141
 - con escalares, 23
 - cruz o vectorial, 26
 - de subgrupos, 117
 - directo, 117
 - escalar o interno, 24
 - fibrado, 128
- producto cartesianano
 - sobre familias indizadas, 10
- producto cartesiano, 8
- producto libre, 139, 140
- proyección
 - canónica, 12, 68
- pull-back, 129
- push-out, 132

- raíz
 - de la unidad, 271
 - de un polinomio, 210
 - múltiple, 212
 - simple, 212
- radical, 161
 - de Jacobson, 168
 - de un ideal, 161
 - irreducible, 277
- rango, 8
 - de un grupo abeliano, 125
- red, 14
 - complementada, 15
- relación, 8
 - antisimétrica, 11
 - de congruencia, 55
 - de equivalencia, 11
 - de orden parcial, 13
 - de orden total, 13
 - reflexiva, 11
 - simétrica, 11
 - transitiva, 11
- relación inversa, 8
- resolvente
 - de Lagrange, 279
- resta, 36
- resto, 33
- resto chino
 - teorema del, 159
- Ruffini, Paolo, 49
- semigrupo, 18
 - abeliano, 18
 - comutativo, 18
- serie
 - de composición, 115
 - sobreyectiva, 8
 - soluble
 - por radicación, 282
- soporte
 - de un módulo, 186
- subanillo, 148
- subconjunto, 7
- subgrupo, 53
 - alternante, 87
 - característico, 65
 - de Borel, 54
 - de Borel especial, 54
 - lineal especial, 54
 - normal, 60
 - propio, 53
- subgrupos
 - conjugados, 104
- submódulo, 180
- substracción, 36
- sucesión
 - exacta, 71
 - normal, 115
- sucesor, 15
 - de un número entero, 37
- suma
 - amalgamada, 141
 - fibrada, 131
- supremo, 13
- Sylow, Ludwig Mejell, 51
- Sylow, Ludwig Mejell, 101
- Tartaglia, 4
- teorema
 - de factorización única, 174, 198
- tipo
 - de una estructura, 26
- torsión
 - elemento de, 186
 - submódulo de, 186
- transposición, 77
- unión, 7
- universo, 7
- valor absoluto, 38
- variedad
 - algebraica, 229
 - algebraica abstracta, 162
- vectores, 23
- Viète, 4
- von Dyck, Walther, 50
- Zariski
 - topología de, 157, 163
- Zermelo, 11
- Zhu Shijie, 3
- Zorn
 - lema de, 13