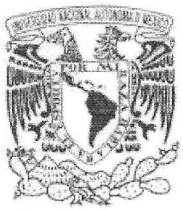

UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE CIENCIAS

DE LA TEORÍA DE GRUPOS AL TEOREMA FUNDAMENTAL DE LA TEORÍA DE GALOIS

T E S I S

QUE PARA OBTENER EL TÍTULO DE:

MATEMÁTICO

PRESENTA:

ROGELIO ALBERTO SERRANO RAMOS

DIRECTOR DE TESIS:
DRA. EUGENIA O'REILLY REGUEIRO
2014

NIVERSIDAD NACIONAL
AVPNOMA DE
MEXICO

FACULTAD DE CIENCIAS
Secretaría General
División de Estudios Profesionales

Votos Aprobatorios

DR. ISIDRO ÁVILA MARTÍNEZ
Director General
Dirección General de Administración Escolar
P r e s e n t e

Por este medio hacemos de su conocimiento que hemos revisado el trabajo escrito titulado:

"De la teoría de grupos al Teorema Fundamental de la Teoría de Galois"

realizado por **SERRANO RAMOS ROGELIO ALBERTO** con número de cuenta **4-0508049-6** quien ha decidido titularse mediante la opción de **tesis** en la licenciatura en **Matemáticas**. Dicho trabajo cuenta con nuestro voto aprobatorio.

Propietario	Dr. Hugo Alberto Rincón Mejía	Hugo A. Rincón M.
Propietario	Dra. Bertha María Tomé Arreola	Bertha Tomé
Propietario Tutora	Dra. Eugenia O'Reilly Regueiro	
Suplente	Dr. Emilio Lluis Puebla	Emilio Lluis Puebla
Suplente	Dra. Diana Avella Alaminos	Diana Avella Alaminos

Atentamente
"POR MI RAZA HABLARÁ EL ESPÍRITU "
Ciudad Universitaria, D. F., a 19 de mayo de 2014
EL JEFE DE LA DIVISIÓN DE ESTUDIOS PROFESIONALES

ACT. MAURICIO AGUILAR GONZÁLEZ

Señor sinodal: antes de firmar este documento, solicite al estudiante que le muestre la versión digital de su trabajo y verifique que la misma incluya todas las observaciones y correcciones que usted hizo sobre el mismo.
MAG/mdm

De la teoría de grupos al Teorema Fundamental de la Teoría de Galois

Rogelio Alberto Serrano Ramos

Ciudad Universitaria a 14 de Agosto de 2014

Índice

Introducción

Una de las cualidades más significativas y útiles de la Matemática es la capacidad de transformar un problema complicado en uno más simple o en varios más simples y así poder darle solución a problemas que, de otra forma, hubiera sido mucho más complicado resolver. Ejemplo de esto son las preguntas que la Teoría de Galois responde aun cuando los problemas presentados no parecen tener relación alguna entre sí; preguntas en diversos temas, desde la solubilidad por radicales a ecuaciones de grado superior a cuatro hasta la posibilidad de construir ciertas figuras geométricas con sólo regla y compás, son resueltas gracias al desarrollo de esta teoría. La transformación de estos problemas es posible al estudiarlos en relación a su estructura algebraica en vez de asociarlos directamente a su área de estudio.

En este trabajo partimos de la definición de grupo y llegamos a la demostración del teorema del elemento primitivo de la Teoría de Galois; dando las definiciones, lemas y teoremas con sus respectivas demostraciones para ver claramente cómo se desarrolla esta teoría, particularmente la estructura algebraica. Empezando con un conjunto y una operación binaria, dadas ciertas propiedades, se obtiene un grupo. Partiendo de la teoría de grupos y añadiendo otra operación con propiedades adicionales se obtiene un anillo, y a partir de los anillos obtenemos los anillos de polinomios y las extensiones de campos, culminando con la materia de estudio de la Teoría de Galois.

En un panorama más general, cabe mencionar que, aunque en este trabajo vayamos construyendo la Teoría de Galois paso a paso, en los hechos históricos la construcción no sucedió de esa manera. La Teoría de Galois logra combinar dos ramas de la Matemática que en un principio parecen no tener mucho en común, entrelaza el Álgebra lineal con la Teoría de grupos, esto lo vemos claramente cuando, por un lado, las extensiones de campos se ven como espacios vectoriales sobre un campo y, por el otro, cuando al conjunto de automorfismos se les dota de una operación para formar grupos.

Como se ha mencionado, el alcance de este trabajo está enfocado en la construcción de la teoría y cómo, con la estructura algebraica, podemos dar solución a ciertos problemas incluso olvidando el caso particular estudiado.

1. Grupos: definiciones y propiedades elementales

1.1. Orden, potencia de un elemento, grupo cíclico y ley de cancelación

Definición 1. Un grupo $(G, \cdot)$ es una pareja que consta de un conjunto $G \neq \emptyset$ y de una operación binaria $\cdot$ que cumple con las siguientes propiedades:

i) Cerradura: $\forall\ a, b \in G, a \cdot b \in G$

ii) Asociatividad: $\forall\ a, b, c \in G$, se cumple: $a \cdot (b \cdot c) = (a \cdot b) \cdot c$

iii) Existencia del neutro: $\exists\ e \in G$ tal que $\forall\ g \in G$, se cumple: $e \cdot g = g \cdot e = g$

iv) Existencia de inversos: $\forall\ g \in G$, $\exists\ g^{-1} \in G$ tal que $g \cdot g^{-1} = g^{-1} \cdot g = e$

Conmutatividad: si además, $\forall\ f, g \in G, f \cdot g = g \cdot f$, diremos que se trata de un grupo conmutativo o un *grupo abeliano*.

Semigrupo: Si $(G, \cdot)$ cumple únicamente con *i)* y *ii)* se le denomina *semigrupo*.

Monoide: Si $(G, \cdot)$ cumple con *i), ii)* y *iii)* le llamaremos *monoide*.

Ejemplo 1. Sea $\mathbb{N}^* = \{1, 2, \ldots\}$, entonces, $(\mathbb{N}^*, +)$ es un semigrupo con $+$ la operación usual.

- $\forall\ a, b \in \mathbb{N}^*, a + b \in \mathbb{N}^*$, por lo que $+$ es cerrada en $\mathbb{N}^*$.
- $\forall\ a, b, c \in \mathbb{N}^*, a + (b + c) = (a + b) + c$, por lo que $+$ es asociativa en $\mathbb{N}^*$.
- $\forall\ a, b \in \mathbb{N}^*, a < a + b$, esto es, no existe un elemento neutro.

Ejemplo 2. $(\mathbb{N}^*, \cdot)$ es un monoide con $\cdot$ la operación usual.

- $\forall\ a, b \in \mathbb{N}^*, a \cdot b \in \mathbb{N}^*$, por lo que $\cdot$ es cerrada en $\mathbb{N}^*$.

- $\forall\ a, b, c \in \mathbb{N}^*, a \cdot (b \cdot c) = (a \cdot b) \cdot c$, por lo que $\cdot$ es asociativa en $\mathbb{N}^*$.

- $1 \cdot n = n \cdot 1 = n\ \forall\ n \in \mathbb{N}^*$, existe un elemento neutro.

- Si $a \in \mathbb{N}^*$ con $1 < a$, entonces, $1 < a \cdot b\ \forall\ b \in \mathbb{N}^*$, por lo tanto, $\forall\ a > 1, a$ no tiene elemento inverso. El 1 es *autoinverso*, ya que $1 \cdot 1 = 1$.

Ejemplo 3. Sea $\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$, entonces, $(\mathbb{Z}, +)$ es un grupo abeliano con $+$ la operación usual.

- $\forall\ x, y \in \mathbb{Z}, x + y \in \mathbb{Z}$ por lo que $+$ es cerrada en $\mathbb{Z}$.

- $\forall\ x, y, z \in \mathbb{Z}, x + (y + z) = (x + y) + z$ por lo que $+$ es asociativa en $\mathbb{Z}$.

- Existe el elemento neutro, $\forall\ z \in \mathbb{Z}, z + 0 = 0 + z = z$.

- Existen los inversos, $\forall\ z \in \mathbb{Z}, z + (-z) = 0$.

- $\forall\ x, y \in \mathbb{Z}, x + y = y + x$, por lo tanto, $+$ es conmutativa en $\mathbb{Z}$.

Nota: En adelante se omitirá la operación del grupo al escribir la operación de sus elementos con el fin de facilitar la notación, así, en lugar de escribir $a \cdot b$ escribiremos ab.

Lema 1. Sea $(G, \cdot)$ un grupo, entonces, se cumplen las siguientes propiedades:

i) El elemento neutro es único.

ii) El inverso de cada elemento es único.

iii) $\forall\ g \in G, (g^{-1})^{-1} = g$.

iv) $\forall\ g, h \in G, (gh)^{-1} = h^{-1}g^{-1}$.

Demostración. Como $(G, \cdot)$ es un grupo, $\exists\ e \in G$ tal que $\forall\ g \in G, eg = ge = g$ y $\forall\ g \in G\ \exists\ g^{-1} \in G$ tal que $gg^{-1} = e$, entonces:

i) Supongamos que $\exists\ f \in G$ tal que $\forall\ g \in G$, $fg = gf = g$. En particular, $ef = e$, por otro lado, $ef = f$ y así, $f = e$. Por lo tanto, el neutro es único.

ii) Sea $a \in G$, supongamos que existe otro inverso b tal que $ab = ba = e$. Sabemos que $a^{-1} = ea^{-1} = baa^{-1} = be = b$, así, $a^{-1} = b$ por lo que el inverso es único.

iii) Como $g^{-1} \in G$, entonces, $(g^{-1})^{-1} \in G$. Sabemos que $g^{-1}(g^{-1})^{-1} = e$, por lo que $gg^{-1}(g^{-1})^{-1} = ge$ y $e(g^{-1})^{-1} = g$. Así, $(g^{-1})^{-1} = g\ \forall\ g \in G$.

iv) $(gh)(h^{-1}g^{-1}) = g(hh^{-1})g^{-1} = geg^{-1} = gg^{-1} = e$. Por lo que $h^{-1}g^{-1} = (gh)^{-1}\ \forall\ g, h \in G$.

□

Definición 2. El *orden* de un grupo $(G, +)$ es la cardinalidad de G y se denota como $o(G)$ o como $|G|$. Si G es infinito, decimos que tiene orden infinito.

Definición 3. Sean $(G, \cdot)$ un grupo y $x \in G$, definimos la *potencia n-ésima* del elemento x como sigue:

i) $x^0 = e$.

ii) $x^1 = x$.

iii) $x^n = \underbrace{x \cdot x \cdot \ldots \cdot x}_{n \text{ veces}}$, $n \in \mathbb{N}$.

iv) $x^{-n} = (x^{-1})^n = \underbrace{x^{-1} \cdot x^{-1} \cdot \ldots \cdot x^{-1}}_{n \text{ veces}}$, $n \in \mathbb{N}$.

Nota: x^n indica que el elemento x será operado (con la operación del grupo) n veces y no necesariamente *multiplicarlo* n veces como estamos acostumbrados al hablar de potencia.

La potencia en la operación $+$ está dada por nx, lo que indica que el elemento x será operado n veces con la operación $+$. Así, en $(\mathbb{Z}, +)$ tenemos el siguiente ejemplo:

$$3(2) = 3 \cdot 2 = \underbrace{2 + 2 + 2}_{3 \text{ veces}} = 6 \neq 8 = 2 \cdot 2 \cdot 2 = 2^3 \text{ con la potencia usual.}$$

Propiedades de la potencia de x:

- $x^{m+n} = x^m \cdot x^n$, en donde $+$ es la operación usual.
- $(x^m)^n = x^{m \cdot n}$, en donde $\cdot$ es la operación multiplicación usual.

Así, en $(G, +)$, si $x \in G$, $nx = \underbrace{x + x + \cdots + x}_{n \text{ veces}}$ $\forall\, n \in \mathbb{N}$, de la misma manera, $-nx = \underbrace{(-x) + (-x) + \cdots + (-x)}_{n \text{ veces}}$ $\forall\, n \in \mathbb{N}$, así, $(-1)x = -x$, lo cual coincide con el inverso aditivo del elemento x.

Definición 4. El *orden de un elemento* de un grupo lo definimos de la siguiente manera: si G es un grupo y $x \in G$, entonces:

- el orden de x es $n \in \mathbb{N}$ si se cumple:

  i) $x^n = e$.

  ii) Si $x^r = e$, entonces, $r \geq n$ y $r > 0$.

- el orden de x es *infinito* si $\forall\, n \in \mathbb{N}$, $n \neq 0$, $x^n \neq e$.

Sea $x \in G$, el orden de x lo denotamos como $\mathrm{o}(x)$.

Observación 1. Si $\mathrm{o}(x) = n$ y $x^r = e$, entonces, $n|r$.

Demostración. Supongamos que $n \nmid r$, entonces, $r = nk+m$ para algún $k \in \mathbb{N}$ y $0 < m < n$. Así, $x^r = x^{nk+m} = x^{nk}x^m = (x^n)^k x^m = e^k x^m = ex^m = x^m$, por lo que $x^m = e$, lo cual contradice la hipótesis de que $\mathrm{o}(x) = n$, por lo tanto, $n|r$.

□

Definición 5. Sean G un grupo y $x \in G$, definimos $\langle x \rangle = \{x^z \mid z \in \mathbb{Z}\}$ y lo llamamos *subgrupo cíclico* generado por x.

Si $G = \langle x \rangle$, decimos que G es un *grupo cíclico*.

Observación 2. Si G es un grupo cíclico, entonces, G es abeliano.

Demostración. Sean G un grupo cíclico, $x \in G$ tal que $G = \langle x \rangle$ y $y, z \in G$. Así, $y = x^m$ y $z = x^n$ para algunos $m, n \in \mathbb{Z}$. De esta manera, $yz = x^m x^n = x^{m+n} = x^{n+m} = x^n x^m = zy$, por lo que $yz = zy \ \forall \ y, z \in G$ y por lo tanto G es abeliano.

□

Teorema 1. Sean G un grupo y $x \in G$, $\mathrm{o}(x) = n$ si y sólo si $|\langle x \rangle| = n$.

Demostración. Si $n = 1$, entonces, $x = e$ y $|\langle e \rangle| = 1$.

Sea $n > 1$. Supongamos que $\mathrm{o}(x) = n$ y sea $R = \{e, x, x^2, \ldots, x^{n-1}\}$ por lo que $|R| = n$. Sea $x^m \in G$ con $n < m$, así, $m = nq + r$ para algunos $q, r \in \mathbb{Z}^+$ y $0 < r < n$. De tal manera, $x^m = x^{nq+r} = x^{nq} x^r = (x^n)^q x^r = e^q x^r = e x^r = x^r$ y así $x^m = x^r \in R$. Por lo tanto, $\langle x \rangle = R$ y $|\langle x \rangle| = |R| = n$.

Ahora, supongamos que $|\langle x \rangle| = n$. con $1 < i \leq n$. Si $\mathrm{o}(x) = i$ con $1 < i < n$, de la implicación previamente demostrada tenemos que $|\langle x \rangle| = i < n$, lo cual contradice nuestra hipótesis. Por lo tanto, $\mathrm{o}(x) = n$.

□

Ejemplo 4. $(\mathbb{Z}, +)$ es un grupo cíclico.

- $(\mathbb{Z}, +)$ es un grupo con $+$ la operación usual.
- Como se vio en la definición 3 la potencia n-ésima con la operación $+$ está dada por $nx \ \forall \ x \in \mathbb{Z}$. Sea $x = 1 \in \mathbb{Z}$, $\langle 1 \rangle = \{z1 \mid z \in \mathbb{Z}\}$ y $\forall \ z \in \mathbb{Z}$, $z = z1$, por lo tanto, $\langle 1 \rangle = \mathbb{Z}$ y $(\mathbb{Z}, +)$ es cíclico.
- Como $\forall \ n \in \mathbb{N}$, $n1 = n \neq 0$, entonces, $\mathrm{o}(1)$ es infinito.
- $\mathrm{o}(\mathbb{Z}) = \mathrm{o}(1)$ que es infinito.

Nota: En adelante, al hablar de un grupo lo haremos mencionando únicamente al conjunto para simplificar la notación. Así, al referirnos al grupo $(G, \cdot)$ lo haremos mencionando únicamente a G.

Proposición 1. Sea G un grupo, si $xy = xz$ entonces $y = z$. De igual manera, si $yx = zx$, entonces, $y = z$.

Demostración. Supongamos que $xy = xz$, entonces, $x^{-1}(xy) = x^{-1}(xz)$, así, $(x^{-1}x)y = (x^{-1}x)z$, $ey = ez$ y $y = z$.

Ahora supongamos que $yx = zx$, entonces, $(yx)x^{-1} = (zx)x^{-1}$, de manera que $y(xx^{-1}) = z(xx^{-1})$, $ye = ze$ y $y = z$.

□

Esta propiedad es conocida como *ley de cancelación* (por la izquierda y por la derecha respectivamente).

Proposición 2. Sean G un grupo y $x, y \in G$. Las ecuaciones $xa = y$ y $bx = y$ tienen soluciones únicas para a y b en G.

Demostración. Sea $xa = y$. Como $x(x^{-1}y) = (xx^{-1})y = ey = y$, entonces, $a = x^{-1}y$ es una solución para $xa = y$. Supongamos que existe otra solución a' a la ecuación, entonces, $xa' = y$. De tal manera que $xa = xa'$ y por la ley de cancelación, $a = a'$ y la solución es única.

Ahora, sea $bx = y$. Como $(yx^{-1})x = y(x^{-1}x) = ye = y$, entonces, $b = yx^{-1}$ es una solución para $bx = y$. Supongamos que existe otra solución b' a la escuación, entonces, $b'x = y$. De tal manera que $bx = b'x$ y por la ley de cancelación, $b = b'$ y la solución es única.

□

1.2. Subgrupos, clases laterales, grupo cociente y grupo normal

Definición 6. Sean $(G, \cdot)$ un grupo y $\emptyset \neq H \subset G$; $(H, \cdot)$ es la restricción de la operación $\cdot$ del grupo G en el subconjunto H. Decimos que H es *subgrupo* de G si $(H, \cdot)$ es un grupo y lo denotamos como $H < G$.

Teorema 2. Sean G un grupo y $\emptyset \neq H \subset G$, entonces, $H < G$ si y sólo si $\forall\ x, y \in H, xy^{-1} \in H$.

Demostración. Sean $H < G$ y $x, y \in H$. Como H es un grupo y $y \in H$, entonces, $y^{-1} \in H$ y $xy^{-1} \in H \ \forall \ x, y \in H$.

Observación: El elemento y^{-1} es el inverso del elemento y respecto al grupo H el cual coincide con el inverso de y con respecto al grupo G ya que $H \subset G$.

Ahora supongamos que $H \subset G$ y $\forall \ x, y \in H, xy^{-1} \in H$.

i) $H \neq \emptyset$ por lo que $\exists \ x \in H$, entonces, $xx^{-1} \in H$ y así $e \in H$.

ii) $e, x \in H$, entonces, $ex^{-1} \in H$ y así $x^{-1} \in H \ \forall \ x \in H$.

iii) Sean $x, y \in H$. Por *ii)*, $y^{-1} \in H$ por lo que $x(y^{-1})^{-1} \in H$ y así, $xy \in H \ \forall \ x, y \in H$.

iv) H es asociativo por ser $H \subset G$.

Por *i), ii), iii)* y *iv)*, $H < G$.

□

Definición 7. Dado $n \in \mathbb{N}$, definimos el conjunto $n\mathbb{Z}$ como sigue:

$$n\mathbb{Z} = \{nz \mid z \in \mathbb{Z}\}$$

Este es el conjunto de los *múltiplos* de n.

Proposición 3. Sea $(\mathbb{Z}, +)$ con $+$ la operación usual, veamos que $n\mathbb{Z} < \mathbb{Z}$ $\forall \ n \in \mathbb{N}$.

Demostración. Sean $x, y \in n\mathbb{Z}$, entonces, $x = nz_1$ y $y = nz_2$ con $z_1, z_2 \in \mathbb{Z}$. De manera que, $x + (-y) = nz_1 + (-nz_2) = nz_1 + n(-z_2) = n(z_1 - z_2) = nz$ con $z_1 - z_2 = z$ para algún $z \in \mathbb{Z}$. Por lo tanto, $n\mathbb{Z}$ es grupo y $n\mathbb{Z} < \mathbb{Z}$ $\forall \ n \in \mathbb{N}$.

□

Teorema 3. Sean G un grupo y $F = \{H_\alpha \mid \alpha \in I\}$ una familia no vacía de subgrupos de G, entonces, $\bigcap_{\alpha \in I} H_\alpha < G$.

Demostración. Sean $a, b \in \bigcap_{\alpha \in I} H_\alpha$, entonces, $a, b \in H_\alpha \ \forall \ \alpha \in I$ y como $H_\alpha < G \ \forall \ \alpha \in I$, entonces, $ab^{-1} \in H_\alpha \ \forall \ \alpha \in I$, por lo que $ab^{-1} \in \bigcap_{\alpha \in I} H_\alpha$ y así, $\bigcap_{\alpha \in I} H_\alpha < G$.

□

Definición 8. Sean $M < G$ y $N < G$, definimos el *producto* de M y N por $MN = \{mn \mid m \in M \text{ y } n \in N\}$.

Teorema 4. Sean G un grupo, $x \in G$ y $H = \langle x \rangle$, entonces, $H < G$.

Demostración. Por la definicion 5, $H = \{x^z \mid z \in \mathbb{Z}\}$. Sean $h_1, h_2 \in H$, entonces, $h_1 = x^{z_1}$ y $h_2 = x^{z_2}$ para algunos $z_1, z_2 \in \mathbb{Z}$. De tal manera que $h_1 h_2^{-1} = x^{z_1}(x^{z_2})^{-1} = x^{z_1} x^{-z_2} = x^{z_1 - z_2} = x^z$, con $z = z_1 - z_2 \in \mathbb{Z}$. Por lo que $h_1 h_2^{-1} \in H$ y así $H < G$.

□

Definición 9. Sean G un grupo y $H < G$. Si $a, b \in G$, definimos la relación $\equiv_H$ como: $a \equiv b \pmod{H}$ si y sólo si $ab^{-1} \in H$ y decimos que a es *congruente* con b *módulo* H.

Observación 3. La relación $\equiv_H$ es una relación de equivalencia.

Demostración. Veamos que $\equiv_H$ es:

i) reflexiva. Sea $a \in H, aa^{-1} = e \in H$ puesto que $H < G$. Así, $\forall \ a \in H$, $a \equiv a \pmod{H}$ y $\equiv_H$ es reflexiva.

ii) simétrica. Supongamos que $a \equiv b \pmod{H}$, entonces, $ab^{-1} \in H$, como $H < G$, $(ab^{-1})^{-1} = (b^{-1})^{-1}a^{-1} = ba^{-1} \in H$ por lo que $b \equiv a \pmod{H}$ y $\equiv_H$ es simétrica.

iii) transitiva. Supongamos que $a \equiv b \pmod{H}$ y $b \equiv c \pmod{H}$, esto es, $ab^{-1}, bc^{-1} \in H$. Como $H < G, (ab^{-1})(bc^{-1}) = a(b^{-1}b)c^{-1} = ac^{-1} \in H$ y $a \equiv c \pmod{H}$, por lo que $\equiv_H$ es transitiva.

Por *i), ii)* y *iii)*, $\equiv_H$ es una relación de equivalencia.

Nota: Recordemos que una relación de equivalencia induce una *partición en clases de equivalencia*, los conjuntos de esta partición son disjuntos dos a dos y su unión es igual al conjunto entero.

□

Definición 10. Sean G un grupo, $H < G$ y $x \in G$. Definimos el conjunto $xH = \{xh \mid h \in H\}$ y lo llamamos *clase lateral izquierda* de H en G.

De igual manera, $Hx = \{hx \mid h \in H\}$ y lo llamamos *clase lateral derecha* de H en G.

Ejemplo 5. Tomemos $3\mathbb{Z} < \mathbb{Z}$ y las clases laterales de $0, 1, 2 \in \mathbb{Z}$.

- $0 + 3\mathbb{Z} = \{\ldots, 0 + (-3), 0 + 0, 0 + 3, 0 + 6, \ldots\} = \{\ldots, -3, 0, 3, 6, \ldots\} = 3\mathbb{Z}$.
- $1 + 3\mathbb{Z} = \{\ldots, 1 + (-3), 1 + 0, 1 + 3, 1 + 6, \ldots\} = \{\ldots, -2, 1, 4, 7, \ldots\}$.
- $2 + 3\mathbb{Z} = \{\ldots, 2 + (-3), 2 + 0, 2 + 3, 2 + 6, \ldots\} = \{\ldots, -1, 2, 5, 8, \ldots\}$.

Teorema 5. Sean G un grupo y $H < G$, entonces, $\forall\ a \in G$, $|aH| = |H|$.

Demostración. Definimos una función $f : aH \to H$ dada por: $f(ah) = h$ $\forall\ h \in H$. Veamos que f es biyectiva:

i) Supongamos que $f(ah_1) = f(ah_2)$, entonces, $h_1 = h_2$ y $ah_1 = ah_2$, por lo que f es inyectiva.

ii) Sean $h \in H$ y $a \in G$. Sabemos que $f(ah) = h$, por lo que f es suprayectiva.

Por *i)* y *ii)*, f es biyectiva y así, $|aH| = |H|$.

□

Lema 2. Sean G un grupo y $H < G$, entonces, $\forall\ a \in G, aH = \{x \in G \mid x \equiv a \pmod{H}\}$.

Demostración. Sean $a \in G$ y los conjuntos $A = aH = \{ah \mid h \in H\}$ y $B = \{g \in G \mid g \equiv a \pmod{H}\}$.

i) sea $x \in A$, entonces, $x = ah$ con $h \in H$, de manera que $a^{-1}x = a^{-1}ah = h \in H$, por lo que $x \equiv a \pmod{H}$ y $x \in B$. Así $A \subset B$.

ii) ahora sea $x \in B$, entonces, $x \equiv a \pmod{H}$, esto es, $a^{-1}x \in H$ por lo que $a^{-1}x = h$ para algún $h \in H$. Así, $aa^{-1}x = ah$ y $x = ah$, con $h \in H$ de manera que $x \in A$. Por lo tanto $B \subset A$.

Por *i)* y *ii)* $A = B$, por lo tanto $aH = \{x \in G \mid x \equiv a \pmod{H}\}$.

□

Definición 11. Si G es un grupo y $N < G$, decimos que N es *subgrupo normal* de G si $\forall\ g \in G$ y $\forall\ n \in N$ se cumple que $gng^{-1} \in N$ (gng^{-1} es la conjugación de n por g). Lo denotamos como $N \lhd G$.

Lema 3. Si G es un grupo abeliano, todo subgrupo de G es normal.

Demostración. Sea G un grupo abeliano, $H < G$, $g \in G$ y $h \in H$. Entonces, $ghg^{-1} = gg^{-1}h = eh = h \in H$, por lo que $\forall\ g \in G$ y $\forall\ h \in H, ghg^{-1} \in H$ y por lo tanto, $H \lhd G$.

□

Ejemplo 6. Tomemos $(\mathbb{Z}, +)$. Veamos que $n\mathbb{Z}$ es un subgrupo normal de $\mathbb{Z}$.

- $\forall\ z_1, z_2 \in \mathbb{Z}, z_1 + z_2 = z_2 + z_1$, por lo que $(\mathbb{Z}, +)$ es un grupo abeliano.
- $n\mathbb{Z} < \mathbb{Z}$.

Por el lema 3, $n\mathbb{Z} \lhd \mathbb{Z}$.

Teorema 6. Sean G un grupo y $H < G$, entonces, son equivalentes:

1) $xHx^{-1} \subset H\ \forall\ x \in G$.

2) $xHx^{-1} = H\ \forall\ x \in G$.

3) $xH = Hx\ \forall\ x \in G$.

Demostración. Sea $H < G$ y $x \in G$, entonces:

1) $\Rightarrow$ 2). Supongamos que $xHx^{-1} \subset H \ \forall \ x \in G$ y sea $h \in H$. Como $x \in G$, $x^{-1} \in G$, entonces, $x^{-1}h(x^{-1})^{-1} = x^{-1}hx \in H$ por lo que $x^{-1}hx = h_1$ para algún $h_1 \in H$, de donde $h = xh_1x^{-1} \in xHx^{-1}$ y así, $H \subset xHx^{-1}$, por lo tanto, $xHx^{-1} = H \ \forall \ x \in G$.

2) $\Rightarrow$ 3). Supongamos que $xHx^{-1} = H \ \forall \ x \in G$. Operamos con x por la derecha en ambos lados de la igualdad, $xHx^{-1}x = Hx$ por lo que $xH = Hx \ \forall \ x \in G$.

3) $\Rightarrow$ 1). Supongamos que $xH = Hx \ \forall \ x \in G$. Operamos con x^{-1} por la derecha en ambos lados de la igualdad, $xHx^{-1} = Hxx^{-1}$ por lo que $xHx^{-1} = H$ y en particular, $xHx^{-1} \subset H \ \forall \ x \in G$.

□

Observación: Dadas estas equivalencias, podemos decir que si $N < G$, entonces, $N \lhd G$ si y sólo si toda clase lateral derecha de N es clase lateral izquierda.

Definición 12. Sean G un grupo, $H \subset G$ y $x, y \in G$, definimos el conjunto $xHyH = \{xh_1yh_2 \mid h_1, h_2 \in H\} \subset G$.

Teorema 7. Sea $H < G$, $H \lhd G$ si y sólo si $\forall \ x, y \in G, xHyH = xyH$.

Demostración. Supongamos que $H \lhd G$ y sean $x, y \in G$, entonces, $yH = Hy$, así, $xHyH = xyHH = xyH$, por lo tanto, $\forall \ x, y \in G, xHyH = xyH$.

Ahora, supongamos que $\forall \ x, y \in G, xHyH = xyH$. Como $H < G, e \in H$. Sean $x \in G$ y $h \in H$, entonces, $xhx^{-1} = xhx^{-1}e \in xHx^{-1}H = xx^{-1}H = eH = H$, así, $\forall \ x \in G$ y $\forall \ h \in H, xhx^{-1} \in H$. Por lo tanto $H \lhd G$.

□

Definición 13. Sean G un grupo y $N \lhd G$, definimos $G/N = \{Ng \mid g \in G\} = \{gN \mid g \in G\}$.

Proposición 4. Sean G un grupo y $N \lhd G$, entonces, $(G/N, \cdot)$ es un grupo con la operación $\cdot$ dada por $xNyN = xyN$.

Demostración. Veamos que se cumple la cerradura en G/N y las 3 propiedades de grupo, sean $x, y, z \in G$:

i) Cerradura: Sean $xN, yN \in G/N$, entonces, $xNyN = xyN$ y como $xy \in G$, entonces, $xyN \in G/N$.

ii) Asociatividad: Sean $xN, yN, zN \in G/N$, entonces, $xN(yNzN) = xN(yzN) = x(yz)N = (xy)zN = xyNzN = (xNyN)zN$.

iii) Existe el neutro: Sea $N = eN$, entonces, $\forall\ x \in G$, $NxN = eNxN = exN = xN$.

iv) Existen los inversos: $xNx^{-1}N = xx^{-1}N = eN = N$, de manera que, $\forall\ x \in G, (xN)^{-1} = x^{-1}N$.

Por *i), ii), iii)* y *iv)*, G/N es un grupo.

A G/N se le conoce como *grupo cociente* de G *módulo* N.

□

Ejemplo 7. Como $n\mathbb{Z} \lhd \mathbb{Z}$, entonces, en particular podemos tomar $n = 2$ y formar $\mathbb{Z}/2\mathbb{Z} = \{z + 2\mathbb{Z} \mid z \in \mathbb{Z}\ \}$.

Veamos algunas clases laterales de $2\mathbb{Z}$. Tomemos $0, 1, 2, 3 \in \mathbb{Z}$:

- $0 + 2\mathbb{Z} = \{\ldots, -4, -2, 0, 2, 4, \ldots\} = 2\mathbb{Z}$.
- $1 + 2\mathbb{Z} = \{\ldots, -3, -1, 1, 3, 5, \ldots\}$.
- $2 + 2\mathbb{Z} = \{\ldots, -4, -2, 0, 2, 4, \ldots\} = 0 + 2\mathbb{Z} = 2\mathbb{Z}$.
- $3 + 2\mathbb{Z} = \{\ldots, -3, -1, 1, 3, 5, \ldots\} = 1 + 2\mathbb{Z}$.

Observemos que sólo hay dos clases laterales y que $\mathbb{Z}/2\mathbb{Z} = \{2\mathbb{Z}, 1 + 2\mathbb{Z}\}$. De modo más general, $\mathbb{Z}/n\mathbb{Z} = \{n\mathbb{Z}, 1 + n\mathbb{Z}, \ldots, (n-1) + n\mathbb{Z}\}$.

Definición 14. Suma y producto *módulo n*.

Por el algoritmo de la división, si $z \in \mathbb{Z}$, entonces, $\forall\ n \in \mathbb{N}\ \exists!\ x \in \mathbb{Z}$ y $r \in \mathbb{N}, r < n$, tales que $z = nx + r$.

Sean $a, b \in \mathbb{Z}$, por lo anterior, $a + b = nx_1 + r_1$ y $a \cdot b = nx_2 + r_2$ Así, podemos definir:

i) $a + b \pmod{n} = r_1$.

ii) $a \cdot b \pmod{n} = r_2$.

Observemos que como $r \in \mathbb{N}$ y $r < n$, entonces, $r \in \{0, 1, \ldots, n-1\}$.

Definición 15. Dado $n \in \mathbb{N}$, definimos el conjunto $\mathbb{Z}_n$ como sigue:

$$\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z} = \{0 + n\mathbb{Z} = n\mathbb{Z}, 1 + n\mathbb{Z}, \ldots, (n-1) + n\mathbb{Z}\}$$

Observación: Sea $0 \leq i < n$, entonces:

$$\begin{aligned} i + n\mathbb{Z} &= \{\ldots, i - 2n, i - n, i, i + n, i + 2n, \ldots\} \\ &= \{z \in \mathbb{Z} \mid z = i + nx, x \in \mathbb{Z}\} \\ &= \{z \in \mathbb{Z} \mid z \equiv i \pmod{n}\} \\ &= \bar{i}. \end{aligned}$$

En donde $\bar{i}$ es la *clase de equivalencia* de i, entonces, podemos decir que:

$$\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$$

A este conjunto se le conoce como el conjunto de *residuos módulo n*.

Teorema 8. (Teorema de Lagrange). Sean G un grupo finito, $\mathrm{o}(G) = n$, con $n \in \mathbb{N}$ y $H < G$, entonces, $\mathrm{o}(H)$ divide a $\mathrm{o}(G)$ y lo denotamos como $\mathrm{o}(H)|\mathrm{o}(G)$.

Demostración. $\mathrm{o}(G) = n$. Sean $G = \{g_1, \ldots, g_n\}$ y $\mathrm{o}(H) = m \leq n$. Supongamos que $e = g_1$ y que las distintas clases laterales de H son: $eH, g_2H, \ldots, g_kH$, con $k \leq n$. Como las clases laterales forman una partición, entonces:

i) $g_iH \bigcap g_jH = \emptyset, i \neq j$

ii) $\bigcup_{i=1}^{k} g_iH = G$, entonces, $|G| = |\bigcup_{i=1}^{k} g_iH| = \sum_{i=1}^{k} |g_iH| = \sum_{i=1}^{k} |H| = k|H|$

Por lo que $n = km$ y así, $\mathrm{o}(H)|\mathrm{o}(G)$.

□

Corolario 1. Si G es un grupo finito y $x \in G$, entonces, $\mathrm{o}(x)|\mathrm{o}(G)$.

Demostración. Sea $H = \langle x \rangle$ y $m = \mathrm{o}(H)$. Por el teorema 4, sabemos que $H < G$ y como $\mathrm{o}(x) = m = \mathrm{o}(H)$, entonces, por el teorema 8, $\mathrm{o}(H)|\mathrm{o}(G)$ por lo que $\mathrm{o}(x)|\mathrm{o}(G)$.

□

Corolario 2. Si G es un grupo finito de orden n y $x \in G$, entonces, $x^n = e$.

Demostración. Por el corolario 1, sabemos que $\mathrm{o}(x)|\mathrm{o}(G) = n$, entonces, $n = \mathrm{o}(x) \cdot k$, con $k \in \mathbb{Z}$. Así, $x^n = x^{\mathrm{o}(x)\cdot k} = (x^{\mathrm{o}(x)})^k = e^k = e$. De tal manera que $x^n = e$.

□

Corolario 3. Todo grupo finito de orden p, con p primo, es cíclico.

Demostración. Sea G un grupo tal que $|G| = p$ y $x \in G, x \neq e$. Sabemos que $\mathrm{o}(x)|\mathrm{o}(G) = p$ por lo que $\mathrm{o}(x) = p$ por ser p primo. De manera que, $|\langle x \rangle| = p$ y $\langle x \rangle = G$, por lo que G es cíclico.

□

Observación: Un grupo G de orden primo únicamente tiene los subgrupos G y $\{e\}$, los cuales son normales. De manera que podemos hacer los cocientes G/G y $G/\{e\}$.

Definición 16. Diremos que un grupo G es *simple* si tiene exactamente dos subgrupos normales (G y $\{e\}$).

Definición 17. Si $H < G$, al número de clases laterales de H en G lo llamamos *índice* de H en G y lo denotamos como $[G : H]$.

Observación: Si G es un grupo finito y $H < G$, entonces, por el teorema 8 (de Lagrange), se tiene que $|G| = [G : H] \cdot |H|$ por lo que $[G : H] = |G|/|H|$.

2. Relaciones entre grupos

2.1. Homomorfismos e isomorfismos

Definición 18. Sean $(G, \cdot)$ y $(G', \cdot')$ dos grupos, llamamos *homomorfismo* (de grupos) a una función φ que cumple la siguiente propiedad:

$$\forall\ f, g \in G,\ \varphi(f \cdot g) = \varphi(f) \cdot' \varphi(g)$$

y escribimos $\varphi : G \to G'$.

Proposición 5. La composición de homomorfismos de grupos es un homomorfismo de grupos.

Demostración. Sean $\varphi : G \to G'$ y $\omega : G' \to G''$ dos homomorfismos de grupos. Por composición de funciones sabemos que $\omega \circ \varphi : G \to G''$, y que $\forall\ f, g \in G$:

$$\begin{aligned}(\omega \circ \varphi)(f \cdot g) &= \omega(\varphi(f \cdot g)) \\ &= \omega(\varphi(f) \cdot' \varphi(g)) \\ &= \omega(\varphi(f)) \cdot'' \omega(\varphi(g)) \\ &= (\omega \circ \varphi)(f) \cdot'' (\omega \circ \varphi)(g).\end{aligned}$$

Por lo tanto, $(\omega \circ \varphi)(f \cdot g) = (\omega \circ \varphi)(f) \cdot'' (\omega \circ \varphi)(g)$ y así, $\omega \circ \varphi$ es un homomorfismo de grupos de G en G''.

□

Lema 4. Si $\varphi : G \to G'$ es un homomorfismo, entonces:

i) $\varphi(e) = e'$.

ii) $\forall\ g \in G,\ \varphi(g^{-1}) = \varphi(g)^{-1}$.

Demostración. Sea φ un homomorfismo, entonces:

i) $\forall\ g \in G,\ \varphi(e)\varphi(g) = \varphi(eg) = \varphi(g) = e'\varphi(g)$ por lo que $\varphi(e)\varphi(g) = e'\varphi(g)$ y así, $\varphi(e) = e'$.

ii) $\forall\ g \in G,\ \varphi(g)\varphi(g^{-1}) = \varphi(gg^{-1}) = \varphi(e) = e' = \varphi(g)\varphi(g)^{-1}$ por lo que $\varphi(g)\varphi(g^{-1}) = \varphi(g)\varphi(g)^{-1}$ y así, $\varphi(g) = \varphi(g)^{-1}$.

□

Definición 19. Sea $\varphi : G \to G'$ un homomorfismo, entonces:

Llamamos *núcleo* de φ al conjunto de todos los elementos $g \in G$ tales que $\varphi(g) = e'$ (elemento neutro en el grupo G'). Al núcleo también se le conoce como *kernel* y se denota como $\ker\varphi$.

$$\ker\varphi = \{\ g \in G \mid \varphi(g) = e'\ \}$$

Observación: La palabra *kernel* no existe en el idioma español, es una palabra en inglés que se utiliza para nombrar al núcleo.

Llamamos *imagen* de φ al conjunto de todos los elementos $\varphi(g)$ tales que $g \in G$ y se denota como $\text{Img}\varphi$.

$$\text{Img}\varphi = \{\ \varphi(g) \mid g \in G\ \}$$

- Si φ es suprayectiva decimos que es *epimorfismo*.
- Si φ es inyectiva decimos que es *monomorfismo*.
- Si φ es biyectiva decimos que es *isomorfismo* y lo denotamos como $G \cong G'$.
- Si φ es un isomorfismo de G en G, decimos que es un *automorfismo*.
- Si $\varphi(g) = e'\ \forall\ g \in G$, esto es, $\text{Img}\varphi = \{e'\}$ o $\ker\varphi = G$, diremos que se trata de un *homomorfismo de grupos trivial*.

Proposición 6. Sea φ un homomorfismo, entonces, φ es monomorfismo si y sólo si $\ker\varphi = \{e\}$.

Demostración. Supongamos que φ es monomorfismo, esto es, es inyectiva. Sea $g \in \ker\varphi$, entonces, $\varphi(g) = e' = \varphi(e)$ por lo que $\varphi(g) = \varphi(e)$, lo que implica que $g = e$ y así, $\ker\varphi = \{e\}$.

Ahora supongamos que $\ker\varphi = \{e\}$. Sean $f, g \in G$ tales que $\varphi(f) = \varphi(g)$. Así, $\varphi(f)\varphi(g)^{-1} = \varphi(g)\varphi(g)^{-1} = e'$, de manera que $\varphi(f)\varphi(g)^{-1} = \varphi(f)\varphi(g^{-1}) = \varphi(fg^{-1}) = e'$ lo que implica que $fg^{-1} \in \ker\varphi = \{e\}$. Entonces, $fg^{-1} = e$, $fg^{-1}g = eg$ y $f = g$. Por lo tanto, φ es inyectiva, es decir, φ es monomorfismo.

□

Proposición 7. Si φ es un isomorfismo de grupos, entonces, φ^{-1} es un isomorfismo de grupos.

Demostración. Supongamos que $\varphi : G \to G'$ es un isomorfismo, entonces, φ es biyectiva, por lo tanto, $\varphi^{-1} : G' \to G$ es también biyectiva.

Sean $g', h' \in G'$, como φ es biyectiva, entonces, $\exists!\ g, h \in G$ tales que $\varphi(g) = g'$ y $\varphi(h) = h'$. Así, $\varphi^{-1}(\varphi(g)) = \varphi^{-1}(g')$ y $\varphi^{-1}(\varphi(h)) = \varphi^{-1}(h')$, por lo que $g = \varphi^{-1}(g')$ y $h = \varphi^{-1}(h')$, entonces:

$$\begin{aligned} \varphi^{-1}(g' \cdot' h') &= \varphi^{-1}(\varphi(g) \cdot' \varphi(h)) \\ &= \varphi^{-1}(\varphi(g \cdot h)) \\ &= \varphi^{-1}\varphi(g \cdot h) \\ &= g \cdot h \\ &= \varphi^{-1}(g') \cdot \varphi^{-1}(h'). \end{aligned}$$

Por lo tanto, φ^{-1} es homomorfismo y como φ^{-1} es biyectiva, entonces, φ^{-1} es un isomorfismo.

□

Proposición 8. Sean $\varphi : G \to G'$, $\omega : G' \to G''$ dos homomorfismos de grupos y $\Phi = \omega \circ \varphi$, entonces:

i) si Φ es monomorfismo, φ es monomorfismo.

ii) si Φ es epimorfismo, ω es epimorfismo.

Demostración. Sean φ y ω homomorfismos y $\Phi = \omega \circ \varphi$:

i) Supongamos que $\varphi(f) = \varphi(g)$, entonces, $\omega(\varphi(f)) = \omega(\varphi(g))$, esto es, $\Phi(f) = \Phi(g)$ y como Φ es monomorfismo, $f = g$. Por lo tanto, φ es monomorfismo.

ii) Φ es epimorfismo, entonces: $\forall\ h \in G''\ \exists\ f \in G$ tal que $\Phi(f) = h$. $\Phi(f) = \omega(\varphi(f)) = h$. Así, $\forall\ h \in G''\ \exists\ g \in G'$, a saber, $g = \varphi(f)$ tal que $\omega(g) = \omega(\varphi(f)) = h$ y por lo tanto, ω es epimorfismo.

□

Definición 20. Sean $\varphi : G \to G'$ un homomorfismo, $g' \in G'$ y $H' \subset G'$. Definimos la *preimagen* de g' como $\varphi^{-1}(g') = \{g \in G \mid \varphi(g) = g'\}$ y la *preimagen* de H' como $\varphi^{-1}(H') = \{h \in G \mid \varphi(h) \in H'\}$.

Teorema 9. Sea $\varphi : G \to G'$ un homomorfismo de grupos, se cumplen:

i) Si $H < G$, entonces, $\varphi(H) < G'$.

ii) Si $H' < G'$, entonces, $\varphi^{-1}(H') < G$.

Demostración. Supongamos que φ es un homomorfismo de grupos:

i) Sea $H' = \varphi(H) = \{\varphi(h) \mid h \in H\}$ y sean $f', g' \in H'$, entonces, existen $f, g \in H$ tales que $\varphi(f) = f'$ y $\varphi(g) = g'$. De manera que $f'(g')^{-1} = \varphi(f)\varphi(g)^{-1} = \varphi(f)\varphi(g^{-1}) = \varphi(fg^{-1})$ y así, $f'(g')^{-1} = \varphi(fg^{-1})$. Como $H < G$, entonces, $fg^{-1} \in H$ y $\varphi(fg^{-1}) \in H'$, por lo que $f'(g')^{-1} \in H'$. De manera que $H' < G'$.

ii) Sea $H = \varphi^{-1}(H') = \{h \in G \mid \varphi(h) \in H'\}$. Supongamos que $f, g \in H$, entonces, $\varphi(f), \varphi(g) \in H'$. $\varphi(fg^{-1}) = \varphi(f)\varphi(g^{-1}) = \varphi(f)\varphi(g)^{-1} \in H'$ puesto que $H' < G'$. Así, $\varphi(fg^{-1}) \in H'$, por lo tanto, $fg^{-1} \in H$ y $H < G$.

□

Corolario 4. Sea $\varphi : G \to G'$ un homomorfismo, entonces, Img$\varphi < G'$ y ker$\varphi \lhd G$.

Demostración. Img$\varphi = \{\varphi(g) \mid g \in G\} = \{\varphi(G)\}$ y como $G < G$, entonces, Img$\varphi < G'$ por *i)* del teorema 9.

ker$\varphi = \{g \in G \mid \varphi(g) = e'\} = \varphi^{-1}(e')$ y como $\{e'\} < G'$, entonces, por *ii)* del teorema 9, ker$\varphi < G$. Ahora, sean $g \in$ kerφ y $x \in G$, entonces, $\varphi(xgx^{-1}) = \varphi(x)\varphi(g)\varphi(x^{-1}) = \varphi(x)e'\varphi(x^{-1}) = \varphi(x)\varphi(x)^{-1} = e'$, por lo que $xgx^{-1} \in$ kerφ $\forall$ $x \in G$ y por lo tanto, ker$\varphi \lhd G$.

□

Teorema 10. Sean $\langle x \rangle$ un grupo cíclico generado por x y $\eta : \langle x \rangle \to H$ un homomorfismo, entonces, Imgη es un subgrupo cíclico de H.

Demostración. Sea $|\langle x \rangle| = n$, entonces, $\langle x \rangle = \{x, x^2, \ldots, x^n = e\}$.

Como η es homomorfismo, entonces, $\eta(x^m) = (\eta(x))^m$ $\forall$ $m \in \{1, 2, \ldots, n\}$ y $\eta(x)^n = \eta(x^n) = \eta(e) = e'$, de manera que Img$\eta = \{\eta(y) \mid y \in \langle x \rangle\} = \{\eta(x^m) \mid m \in \{1, 2, \ldots, n\}\} = \{\eta(x^1), \eta(x^2), \ldots, \eta(x^n)\}$. De esta manera, Img$\eta = \{\eta(x)^1, \eta(x)^2, \ldots, \eta(x)^n = e'\}$. Por lo tanto, Img$\eta = \langle \eta(x) \rangle$ y así, Imgη es cíclico.

□

2.2. Teoremas de isomorfismos

Definición 21. Sea $H \lhd G$, definimos la función $\pi : G \to G/H$ dada por $\pi(x) = xH \ \forall \ x \in G$. A π se le llama *proyección canónica*.

Proposición 9. π es un epimorfismo y $\ker\pi = H$.

Demostración. Sabemos que en el grupo $G/H, eH = H$ es el elemento neutro ($eHxH = exH = xH \ \forall \ xH \in G/H$) y que $x^{-1}H$ es el elemento inverso de $xH \ \forall \ xH \in G/H$ ($xHx^{-1}H = xx^{-1}H = eH = H$).

i) Sean $x, y \in G, \pi(xy) = xyH = xHyH = \pi(x)\pi(y)$ por lo que π es homomorfismo.

ii) Sea $xH \in G/H$, $\pi(x) = xH \ \forall \ x \in G$, por lo tanto, π es suprayectiva.

Por *i)* y *ii)*, π es un epimorfismo

Ahora, $\ker\pi = \{x \in G \mid \pi(x) = eH = H\} = \{x \in G \mid xH = H\} = \{x \in G \mid x \in H\} = H$. De esta manera, $\ker\pi = H$.

□

Corolario 5. Si $H \lhd G$, entonces, $H = \ker\varphi$ con φ un homomorfismo de G en G'.

Demostración. Como $H \lhd G$, podemos tomar $G' = G/H$ y $\varphi = \pi$. Por la proposición 9, $H = \ker\varphi$.

□

Proposición 10. Sean $H \lhd G$, $H' \lhd G'$ y $\pi : G \to G/H$, $\pi' : G' \to G'/H'$ las proyecciones canónicas. Si $\varphi : G \to G'$ es un homomorfismo tal que $\varphi(H) \subset H'$, entonces:

i) $\varphi^* : G/H \to G'/H'$, con $\varphi^*(xH) = \varphi(x)H'$ está bien definido y es un homomorfismo (inducido por φ).

ii) $\pi' \circ \varphi = \varphi^* \circ \pi$, es decir, el siguiente cuadro conmuta:

$$\begin{array}{ccc} G & \xrightarrow{\varphi} & G' \\ \downarrow^{\pi} & & \downarrow^{\pi'} \\ G/H & \xrightarrow{\varphi^*} & G'/H' \end{array}$$

iii) $\ker\varphi^* = \pi(\varphi^{-1}(H'))$ e $\mathrm{Img}\varphi^* = \pi'(\mathrm{Img}\varphi)$.

Demostración. Sea $\varphi : G \to G'$ un homomorfismo tal que $\varphi(H) \subset H'$, entonces:

i) Sean $a, b \in G/H$ tales que $a = b$. Como $a, b \in G/H$, entonces, $a = x_1H$ y $b = x_2H$ para algunos $x_1, x_2 \in G$. De esta manera:

$$\begin{aligned} x_1H = x_2H &\Leftrightarrow x_1(x_2)^{-1} \in H \\ &\Rightarrow \varphi(x_1(x_2)^{-1}) \in H'; \quad \text{(por hipótesis, } \varphi(H) \subset H') \\ &\Leftrightarrow \varphi(x_1(x_2)^{-1})H' = H' \\ &\Leftrightarrow \varphi(x_1)\varphi(x_2)^{-1}H' = H' \\ &\Leftrightarrow \varphi(x_1)H' = \varphi(x_2)H' \\ &\Leftrightarrow \varphi^*(x_1H) = \varphi^*(x_2H) \end{aligned}$$

Por lo tanto, φ^* está bien definido.

Ahora, sean $a, b \in G/H$, entonces, $a = x_1H$ y $b = x_2H$ con $x_1, x_2 \in G$ y así:

$$\begin{aligned} \varphi^*(ab) &= \varphi^*(x_1Hx_2H) \\ &= \varphi^*(x_1x_2H) \\ &= \varphi(x_1x_2)H' \\ &= \varphi(x_1)\varphi(x_2)H' \\ &= \varphi(x_1)H'\varphi(x_2)H' \\ &= \varphi^*(x_1H)\varphi^*(x_2H) \\ &= \varphi^*(a)\varphi^*(b). \end{aligned}$$

De tal manera, tenemos que $\varphi^*(ab) = \varphi^*(a)\varphi^*(b)$ por lo que φ^* es homomorfismo.

ii) Sean $\pi' \circ \varphi$ la composición de las funciones y $x \in G$, entonces:

$$\begin{aligned} (\pi' \circ \varphi)(x) &= \pi'(\varphi(x)) \\ &= \varphi(x)H' \\ &= \varphi^*(xH) \\ &= \varphi^*(\pi(x)) \\ &= (\varphi^* \circ \pi)(x). \end{aligned}$$

Por lo que $\pi' \circ \varphi = \varphi^* \circ \pi$ y el cuadro conmuta.

iii) Ahora, veamos que $\ker\varphi^* = \pi(\varphi^{-1}(H'))$ e $\mathrm{Img}\varphi^* = \pi'(\mathrm{Img}\varphi)$:

$$\begin{aligned}
\ker\varphi^* &= \{y \in G/H \mid \varphi^*(y) = H'\} \\
&= \{xH \mid x \in G \text{ y } \varphi^*(xH) = H'\} \\
&= \{xH \mid x \in G \text{ y } \varphi(x)H' = H'\} \\
&= \{xH \mid x \in \varphi^{-1}(H')\} \\
&= \pi(\varphi^{-1}(H')).
\end{aligned}$$

$$\begin{aligned}
\mathrm{Img}\varphi^* &= \{\varphi^*(y) \mid y \in G/H\} \\
&= \{\varphi^*(xH) \mid x \in G\} \\
&= \{\varphi(x)H' \mid x \in G\} \\
&= \pi'(\mathrm{Img}\varphi).
\end{aligned}$$

□

Teorema 11. (Primer teorema de isomorfismos). Sea $\varphi : G \to G'$ un homomorfismo, entonces, $G/\ker\varphi \cong \mathrm{Img}\varphi$.

Demostración. Por el corolario 4 del teorema 9, $\mathrm{Img}\varphi < G'$ y $\ker\varphi \lhd G$, por lo tanto, $\varphi : G \to \mathrm{Img}\varphi$ es un epimorfismo y $G/\ker\varphi$ está bien definido.

Por la proposición 10, tenemos que $\varphi^* : G/\ker\varphi \longrightarrow \mathrm{Img}\varphi$ es un homomorfismo y es único puesto que $\varphi^*(xH) = \varphi(x)H'$, esto es, φ^* está determinado únicamente por φ. Sin pérdida de generalidad, tomamos $H' = \{0'\}$ por lo que $\varphi^*(xH) = \varphi(x)H' = \varphi(x)0' = \varphi(x)$ y tenemos:

i) $\ker\varphi^* = \pi(\varphi^{-1}(H')) = \pi(\varphi^{-1}(\{0'\})) = \pi(\ker\varphi) = 0_{G/\ker\varphi}$ por lo que φ^* es monomorfismo.

ii) $\mathrm{Img}\varphi^* = \pi'(\mathrm{Img}\varphi) = \mathrm{Img}\varphi$ y como $\mathrm{Img}\varphi \cong \mathrm{Img}\varphi/\{0'\}$, entonces, φ^* es epimorfismo.

Por *i)* y *ii)*, φ^* es un isomorfismo.

Por lo tanto, $G/\ker\varphi \cong \mathrm{Img}\varphi$ y el siguiente diagrama conmuta:

$$\begin{array}{ccc}
G & \xrightarrow{\varphi} & G' = \mathrm{Img}\varphi \\
\downarrow{\scriptstyle \pi} & \cong\nearrow_{\varphi^*} & \\
G/\ker\varphi & &
\end{array}$$

□

Teorema 12. (Segundo teorema de isomorfismos). Sea $H < G$ y $N \lhd G$, entonces, $(HN)/N \cong H/(H \cap N)$.

Demostración. Veamos que $H/(H \cap N)$ está bien definido:

i) $H \cap N \subset H$ y por el teorema 3, $H \cap N < H$.

ii) Sean $h \in H$ y $x \in H \cap N$, entonces:

- Como $x \in H \cap N$, $x \in H$ y $hxh^{-1} \in H$.
- Como $x \in H \cap N$, $x \in N$. $N \lhd G$, así, $hxh^{-1} \in N$.

Así, $\forall\ h \in H$ y $\forall\ x \in H \cap N$, $hxh^{-1} \in H \cap N$, por lo que $H \cap N \lhd H$.

Por *i)* y *ii)*, $H/(H \cap N)$ está bien definido.

Recordemos que $HN = \{hn \mid h \in H \text{ y } n \in N\}$ y sea $\eta : HN \to H/(H \cap N)$ dada por $\eta(hn) = h(H \cap N)$, veamos que η está bien definida y es un homomorfismo:

i) Sea $h_1n_1 = hn$, entonces, $h^{-1}h_1 = nn_1^{-1}$, de manera que $h^{-1}h_1 \in H$ y $h^{-1}h_1 \in N$, por lo que $h^{-1}h_1 \in H \cap N$. Así, en $H/(H \cap N), h(H \cap N) = h_1(H \cap N)$ y $\eta(hn) = \eta(h_1n_1)$, por lo que η está bien definida.

ii) Como $N \lhd G$, entonces, $hN = Nh\ \forall\ h \in H$, de manera que $n_1h_2 = h_2n$ para algún $n \in N$. Sean $h_1n_1, h_2n_2 \in HN$, entonces:

$$\begin{aligned}
\eta((h_1n_1)(h_2n_2)) &= \eta(h_1(n_1h_2)n_2) \\
&= \eta(h_1(h_2n)n_2) \\
&= \eta((h_1h_2)(nn_2)) \\
&= h_1h_2(H \cap N) \\
&= h_1(H \cap N)h_2(H \cap N) \\
&= \eta(h_1n_1)\eta(h_2n_2).
\end{aligned}$$

Por lo tanto, η es un homomorfismo.

Veamos que $\ker\eta = \{hn \in HN \mid h \in H \cap N\} = \{hn \mid h \in N\} = N$ y como $\eta(he) = h(H \cap N)\ \forall\ h \in H$, por el teorema 11 (primer teorema de isomorfismos), $HN/N \cong H/(H \cap N)$.

□

Teorema 13. (Tercer teorema de isomorfismos). Sean $H \lhd G, N \lhd G$ y $N < H$, entonces, $G/H \cong (G/N)/(H/N)$.

Demostración. Sea $\eta : G \to (G/N)/(H/N)$ dada por $\eta(g) = (gN)(H/N)$. Sean $g_1, g_2 \in G$, entonces, $\eta(g_1 g_2) = (g_1 g_2 N)(H/N) = ((g_1 N)(g_2 N))(H/N) = [(g_1 N)(H/N)][(g_2 N)(H/N)] = \eta(g_1)\eta(g_2)$, por lo que η es homomorfismo.

$\ker\eta = \{g \in G \mid \eta(g) = H/N\} = H$. Por el teorema 11 (primer teorema de isomorfismos), $G/H \cong (G/N)/(H/N)$.

□

3. Anillos: definiciones y propiedades elementales

3.1. Divisores de cero, dominio entero, anillo con división, campo y anillo euclidiano

Definición 22. Un anillo $(A, +, \cdot)$ es una terna que consta de un conjunto $A \neq \emptyset$ y de dos operaciones binarias, $+$ y $\cdot$ las cuales cumplen las siguientes propiedades:

i) $(A, +)$ es un grupo abeliano.

ii) $(A, \cdot)$ es un semigrupo.

iii) $\cdot$ es distributivo respecto a $+$, esto es, $\forall\ a, b, c \in A$ se cumple:

$$(a + b) \cdot c = (a \cdot c) + (b \cdot c) \qquad \text{y} \qquad a \cdot (b + c) = (a \cdot b) + (a \cdot c)$$

A esta propiedad se le conoce como la *ley distributiva* del producto sobre la suma.

Si además $(A, \cdot)$ es un *semigrupo conmutativo*, diremos que $(A, +, \cdot)$ es un *anillo conmutativo*.

Ejemplo 8. $(\mathbb{Z}, +, \cdot)$ es un anillo con $+$ y $\cdot$ las operaciones usuales de suma y producto.

- $(\mathbb{Z}, +)$ es un un *grupo abeliano* (ver ejemplo 3).
- $(\mathbb{Z}, \cdot)$ es un *semigrupo*. $\forall\ x, y, z \in \mathbb{Z}, x \cdot (y \cdot z) = (x \cdot y) \cdot z$.
- $\cdot$ distribuye a $+$ en $\mathbb{Z}$.

Por lo tanto se cumplen las 3 propiedades necesarias para tener un anillo.

- $(\mathbb{Z}, \cdot)$ es además abeliano por lo que $(\mathbb{Z}, +, \cdot)$ es un anillo conmutativo.

Definición 23. Si $(A, \cdot)$ es un *monoide*, diremos que $(A, +, \cdot)$ es un *anillo con uno*.

Nota: En algunos textos a un anillo con uno se le denomina también *anillo con unidad*. Nosotros sí haremos una diferencia entre 1 y *unidad* para no confundirnos con definiciones y términos que posteriormente se darán.

Ejemplo 9. Anillo con uno. Tomamos nuevamente el anillo $(\mathbb{Z}, +, \cdot)$.

- $(\mathbb{Z}, \cdot)$ es un monoide y por lo tanto tiene elemento neutro. En $(\mathbb{Z}, \cdot)$ el elemento neutro es 1, ya que se cumple que $\forall\ z \in \mathbb{Z}, z \cdot 1 = 1 \cdot z = z$.

Por convención, al elemento neutro de $(A, +)$ le llamaremos 0 (cero) y al elemento neutro de $(A, \cdot)$ le llamaremos 1 (uno).

Ejemplo 10. Anillo *sin* uno. Tomemos el anillo $(2\mathbb{Z}, +, \cdot)$ con las operaciones usuales.

- $(2\mathbb{Z}, +)$ es un grupo y además $2\mathbb{Z} < \mathbb{Z}$ (ver proposición 3), por lo tanto hereda las propiedades de $(\mathbb{Z}, +)$.
- $1 \notin 2\mathbb{Z}$, por lo tanto $(2\mathbb{Z}, \cdot)$ no es monoide.

Así, $(2\mathbb{Z}, +, \cdot)$ es un anillo sin uno.

Proposición 11. Sea A un anillo con uno. Si $|A| > 1$, entonces, $0 \neq 1$.

Demostración. Suponemos que $1 = 0$ y lo denotaremos como e. Como además, $|A| > 1$, entonces, $\exists\, a \in A$ tal que $a \neq e$. Por otro lado, sabemos que $a+e = a$ y $a \cdot e = a \;\forall\; a \in A$.

Observación: $[(e + e) = e]$ y $[(e \cdot e) = e]$, así:

$$\begin{aligned} a &= a \cdot e \\ &= a \cdot (e \cdot e) \\ &= a \cdot (e + e) \\ &= (a \cdot e) + (a \cdot e) \\ &= a + a. \end{aligned}$$

De tal forma que $a = a + a$. Aplicando el inverso aditivo de a tenemos que:

$$\begin{aligned} a - a &= (a + a) - a \\ e &= a + (a - a) \\ &= a + e \\ &= a \end{aligned}$$

Por lo tanto, $e = a$ lo cual es una contradicción con nuestra hipótesis. Así, $0 \neq 1$.

□

Definición 24. Sea $a \in A, a \neq 0$. Diremos que a es divisor propio de cero si $\exists\, b \in A, b \neq 0$ tal que $a \cdot b = 0$.

A partir de este momento, cuando hablemos de un anillo con uno, estaremos suponiendo que $|A| > 1$, esto es, $0 \neq 1$.

Ejemplo 11. Divisores propios de cero. Tomemos el anillo $(\mathbb{Z}_6, +, \cdot)$, en este caso, $+$ y $\cdot$ son la suma y el producto *módulo* n.

- $\mathbb{Z}_6 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}\}$ (ver definición 15).
  - El neutro aditivo es $\overline{0}$.
  - $\overline{2} \cdot \overline{3} = \overline{0}$, por lo tanto $\overline{2}$ y $\overline{3}$ son divisores propios de cero.

Definición 25. Si A es un anillo conmutativo con uno y no tiene divisores propios de 0, diremos que es un *dominio entero*.

Ejemplo 12. Dominio entero. Tomemos el anillo $(\mathbb{Z}_5, +, \cdot)$.

- $\mathbb{Z}_5 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\}$.
  - El neutro aditivo es $\overline{0}$ y al ser el módulo 5 primo, no se tienen divisores propios de cero.
  - El uno es $\overline{1}$, por lo tanto tenemos un anillo con uno.

Definición 26. Sea A un anillo con uno, llamamos *inverso izquierdo* de $a \in A$, a un elemento $x \in A$ tal que $xa = 1$. Si dicho elemento existe, decimos que a es *invertible* por la izquierda.

De manera análoga, llamamos *inverso derecho* de $a \in A$, a un elemento $y \in A$ tal que $ay = 1$ y si dicho elemento existe, decimos que a es *invertible* por la derecha.

Lema 5. Sea A un anillo con uno, si $a \in A$ es tal que es invertible por la izquierda y por la derecha, entonces, los inversos coinciden.

Demostración. Sea $a \in A$ un elemento invertible por la izquierda y derecha, esto es, $\exists\ x, y \in A$ tal que $xa = 1$ y $ay = 1$.

Así, $xay = 1y$, por lo que $x(ay) = y$. Como $ay = 1$, entonces, $x1 = y$ y finalmente $x = y$.

□

Definición 27. Sea A un anillo con uno. Decimos que un elemento $a \in A$ es una *unidad* si $\exists\ b \in A$ tal que $a \cdot b = b \cdot a = 1$. Al conjunto de unidades de A se denota $\mathrm{U}(A)$.

Teorema 14. El conjunto $\mathrm{U}(A)$ es un grupo bajo la multiplicación.

Demostración. Sean $a, b \in \mathrm{U}(A)$, esto es, $\exists\ x, y \in A$ tal que $xa = ax = 1$ y $yb = by = 1$.

Observación: Supongamos que $\exists\ x' \in A$ tal que $x'a = ax' = 1$ por lo que $xa = x'a$. Operamos x en ambos lados de la igualdad y tenemos $xax = x'ax$, como $ax = 1$, entonces, $x = x'$.

Por esta observación podemos decir que $x = a^{-1}$ y $y = b^{-1}$, de manera que $ab^{-1} = ay \in A$. Sea $z = bx \in A$, entonces:

i) $zab^{-1} = bxay = b(xa)y = b(1)y = by = 1$. Por lo que z es inverso izquierdo de ab^{-1}.

ii) $ab^{-1}z = aybx = a(yb)x = a(1)x = ax = 1$. Por lo que z es inverso derecho de ab^{-1}.

Por *i)* y *ii)*, $\forall\ a, b \in \mathrm{U}(A), ab^{-1} \in \mathrm{U}(A)$, por lo tanto, $\mathrm{U}(A)$ es un grupo bajo la multiplicación.

□

Observación 4. El cero no tiene inverso multiplicativo y por lo tanto no es unidad.

Demostración. Sea $(A, +, \cdot)$ un anillo. $\forall\ a \in A$ se tiene:

$$\begin{aligned} a \cdot 0 &= a \cdot (0 + 0) \\ a \cdot 0 &= (a \cdot 0) + (a \cdot 0) \\ (a \cdot 0) - (a \cdot 0) &= (a \cdot 0) + (a \cdot 0) - (a \cdot 0) \\ 0 &= (a \cdot 0) \end{aligned}$$

Así, $\nexists\ a \in A$ tal que $a \cdot 0 = 1$, esto es, 0 no tiene inverso multiplicativo y por lo tanto, 0 no es unidad.

□

Definición 28. Sea A un anillo con uno, si existe un inverso multiplicativo para todo elemento distinto de 0, diremos que A es un *anillo con división.*

Observación: Un anillo con división no necesariamente es un dominio entero ya que puede no ser conmutativo.

Ejemplo 13. Anillo con división no conmutativo. Tomemos el anillo de los cuaternios $(\mathbb{H}, +, \cdot)$.

- $\mathbb{H} = \{a + bi + cj + dk \mid a, b, c, d \in \mathbb{R} \text{ e } i^2 = j^2 = k^2 = ijk = -1\}$.
- Sean $a, b \in \mathbb{H}, a = a_1 + a_2 i + a_3 j + a_4 k$ y $b = b_1 + b_2 i + b_3 j + b_4 k$, la suma y el producto están definidos como:
  - $a + b = (a_1 + b_1) + (a_2 + b_2)i + (a_3 + b_3)j + (a_4 + b_4)k$.
  - $ab = (a_1b_1 - a_2b_2 - a_3b_3 - a_4b_4) + (a_1b_2 + a_2b_1 + a_3b_4 - a_4b_3)i + (a_1b_3 - a_2b_4 + a_3b_1 + a_4b_2)j + (a_1b_4 + a_2b_3 - a_3b_2 + a_4b_1)k$.

  El producto no es conmutativo.

Este es un ejemplo de un anillo con división que no es dominio entero.

Definición 29. Definimos como *campo* a un anillo conmutativo con división.

Ejemplo 14. Anillo con división y campo. Tomemos el anillo $(\mathbb{R}, +, \cdot)$ con las operaciones usuales.

- El neutro aditivo es 0 y el neutro multiplicativo es 1.
- En $\mathbb{R}$, $ab = 0$ si y sólo si $a = 0$ o $b = 0$.
- $\forall\ a \in \mathbb{R} \setminus \{0\}$, $\exists\ a^{-1}$ tal que $aa^{-1} = 1$.

$\mathbb{R}$ es un anillo con uno, sin divisores propios de cero y con inverso multiplicativo para todo elemento distinto de cero, $\mathbb{R}$ es un anillo con división.

- $\mathbb{R}$ es un anillo conmutativo.

$\mathbb{R}$ es un anillo conmutativo con división, $\mathbb{R}$ es un campo.

Proposición 12. Sea A un anillo, entonces:

i) $0x = 0 = x0\ \forall\ x \in A$.

ii) $\forall\ x \in A, x \neq 0$ vale la ley de cancelación si y sólo si A no tiene divisores de 0.

iii) $-(xy) = (-x)y = x(-y)\ \forall\ x \in A$.

iv) $(-x)(-y) = xy\ \forall\ x, y \in A$.

Demostración. Sea A un anillo:

i) $0 = 0 + 0$, entonces, $0x = (0 + 0)x = 0x + 0x$, por lo tanto, $0 = 0x$ $\forall\ x \in A$, análogamente, $x0 = x(0 + 0) = x0 + x0$, así, $0 = x0\ \forall\ x \in A$, de manera que $0x = 0 = x0\ \forall\ x \in A$.

ii) Suponemos que $\forall\ x \in A, x \neq 0$ vale la ley de cancelación y que A tiene divisores de cero, esto es, $\exists\ x, y \in A$, con $x, y \neq 0$ tales que $xy = 0$. Por *i)* sabemos que $x0 = 0$, por lo tanto, $xy = x0$, cancelamos x y obtenemos $y = 0$ lo cual contradice el hecho de que $y \neq 0$. De tal manera que A no tiene divisores de 0.

Ahora suponemos que A no tiene divisores de 0. Sean $x, y, a \neq 0$ tales que $xa = ya$. Sabemos que $(x - y)a = xa - ya = 0$, así, $(x - y)a = 0$ y como $a \neq 0$, entonces, $x - y = 0$ por lo que $x = y$. De tal manera que $\forall\ x \in A, x \neq 0$ vale la ley de cancelación.

iii) $0 = 0y = (x + (-x))y = xy + (-x)y$, así, $0 = xy + (-x)y$ por lo que $-(xy) = (-x)y$.

Por otro lado, $0 = x0 = x(y + (-y)) = xy + x(-y)$, así, $0 = xy + x(-y)$ por lo que $-(xy) = x(-y)$. Entonces, $(-x)y = x(-y) = -(xy)$.

iv) Por *iii)* $(-x)(-y) = -(x(-y)) = -(-xy)$, entonces, $(-x)(-y) + (-xy) = 0$ y así, $(-x)(-y) = xy$.

□

Definición 30. Sea A un anillo conmutativo y $a, b \in A, a \neq 0$, decimos que a *divide* a b si $\exists\ c \in A$ tal que $b = ac$ y lo denotamos como $a|b$.

Proposición 13. Sea A un anillo conmutativo y sean $a, b \in A$ tales que $a|b$, se cumplen:

i) Si $b|c$, entonces, $a|c$.

ii) Si $a|c$, entonces, $a|(b \pm c)$.

iii) $a|bz \ \forall \ z \in A$.

Demostración. Sean $a, b \in A$ tales que $a|b$. Como caso particular, tomemos $b = 0$, entonces, por la proposición 12, $b = a0 \ \forall \ a \in A$ de manera que $a|0 \ \forall \ a \in A, a \neq 0$.

i) Sean $b, c \in A$ tales que $b|c$, entonces, $c = by$ para algún $y \in A$ y como $a|b, b = ax$ para algún $x \in A$. De esta manera, $c = by = (ax)y = a(xy)$ con $xy \in A$ y $a|c$.

ii) Como $a|c, c = ay$ para algún $y \in A$, de manera que $b \pm c = ax \pm ay = a(x \pm y)$ con $x \pm y \in A$ y así, $a|(b \pm c)$.

iii) $bz = (ax)z = a(xz)$ con $xz \in A$, por lo tanto, $a|bz \ \forall \ z \in A$.

□

Definición 31. Sea A un anillo conmutativo y sean $a, b \in A$. Decimos que $d \in A$ es *máximo común divisor* de a y b si se cumplen:

i) $d|a$ y $d|b$.

ii) $\forall \ c \in A$ tal que $c|a$ y $c|b$, entonces, $c|d$.

Si d es máximo común divisor de a y b lo denotamos como $d = (a, b)$.

Proposición 14. Sean A un dominio entero y $a, b \in A$ con $a, b \neq 0$ tales que $a|b$ y $b|a$, entonces, $a = ub$ en donde u es una unidad de A.

Demostración. Como $a|b$ y $b|a$, entonces, $b = xa$ y $a = yb$ para algunos $x, y \in A$ por lo que $b = xa = xyb$. Cancelamos b y tenemos que $xy = 1$ de manera que x y y son unidades en A.

□

Definición 32. Sea A un anillo conmutativo con uno y sean $a, b \in A$. Decimos que a y b son dos elementos *asociados* en A si $b = ua$, con u una unidad en A.

Nota: La relación de ser elementos asociados es una relación de equivalencia.

Lema 6. Sea A un dominio entero *finito*, entonces, A es un campo.

Demostración. Como A es finito, entonces, $A = \{a_1, a_2, \ldots, a_n\}$ para algún $n \in \mathbb{N}$. Sea $x \in A$, $x \neq 0$ y tomemos los elementos $xa_1, xa_2, \ldots, xa_n$.

Veamos que $xa_i \neq xa_j$ para $i \neq j$. Supongamos que $xa_i = xa_j$, entonces, $xa_i - xa_j = 0$ y $x(a_i - a_j) = 0$. Como A es dominio entero, entonces, $a_i - a_j = 0$ con lo que $a_i = a_j$ lo no puede ocurrir puesto que $i \neq j$. Así, sea $y \in A$, $y = xa_k$ para un único $k \in \{1, 2, \ldots, n\}$. Como A es un dominio entero, tiene uno y, sin pérdida de generalidad, podemos suponer que a_1 es el uno de A.

Demostremos ahora que A tiene inversos multiplicativos. Puesto que a_1 es el neutro multiplicatvo de A decimos que $1 = a_1 \in A$, así, $1 = xa_k$ para un único $k \in \{1, 2, \ldots, n\}$ y $a_k = x^{-1}$. Como x se tomó arbitrariamente, entonces, $\forall\ x \in A, x \neq 0$, $\exists!\ a_k \in A$ tal que $xa_k = 1$, por lo que todo elemento distinto de cero tiene inverso multiplicativo.

Puesto que A es un dominio entero y para todo elemento distinto de cero existe un inverso multiplicativo, entonces, A es un anillo con división; por hipótesis, A es conmutativo, así, A es un campo. Por lo tanto, si A un dominio entero finito, entonces, A es un campo.

□

Definición 33. Sea A un anillo, decimos que A es un *anillo euclidiano* si cumple con las siguientes condiciones:

1. A es un dominio entero.
2. $\forall\ a \in A, a \neq 0$ está definida una función $d : A \setminus \{0\} \to \mathbb{Z}^+$ tal que $\forall\ a, b \in A, a, b \neq 0$ se cumplen:

   i) $d(a) \leq d(ab)$.

   ii) $\exists\ q, r \in A$ tales que $a = qb + r$, en donde $r = 0$ o $d(r) < d(b)$.

Observación: Un anillo euclidiano tiene uno al ser un dominio entero.

Definición 34. Sea A un anillo euclidiano y sea $p \in A$, un elemento no nulo que no es unidad. Decimos que p es un *elemento irreducible* de A si siempre que $p = ab$, con $a, b \in A$ se tiene que a o b es unidad en A.

Podemos decir que un elemento irreducible de un anillo es aquel elemento que únicamente puede ser factorizado en forma trivial. A un elemento irreducible se le conoce también como elemento *primo*.

Definición 35. Sea A un anillo euclidiano y sean $a, b \in A$. Decimos que a y b son *primos relativos* si $(a, b) = u$, con u una unidad en A.

3.2. Subanillos, ideales y factorización única

Definición 36. Sean $(A, +, \cdot)$ y $\emptyset \neq B \subset A$; $(B, +, \cdot)$ es la restricción de las operaciones $+$ y $\cdot$ del anillo A en el subconjunto B. Decimos que B es un *subanillo* de A si $(B, +, \cdot)$ es a su vez un anillo y lo denotaremos como $B < A$.

Si el anillo A es además un dominio entero y el subanillo B es a su vez un dominio entero, diremos que B es un *subdominio* de A.

De igual manera, si el anillo A es un campo y el subanillo B es un campo, diremos que B es un *subcampo* de A.

Ejemplo 15. Tomemos los anillos $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ y $(\mathbb{C}, +, \cdot)$ con $+$ y $\cdot$ las operaciones usuales.

- $\mathbb{Z} \subset \mathbb{Q}$, así, $\mathbb{Z}$ es subanillo de $\mathbb{Q}, \mathbb{Z} < \mathbb{Q}$.
- $\mathbb{Q} \subset \mathbb{R}$, $\mathbb{Q} < \mathbb{R}$. $\mathbb{Q}$ y $\mathbb{R}$ son dominios enteros, así, $\mathbb{Q}$ es un subdominio de $\mathbb{R}$.
- $\mathbb{R} \subset \mathbb{C}$, $\mathbb{R} < \mathbb{C}$. $\mathbb{R}$ y $\mathbb{C}$ son campos, así, $\mathbb{R}$ es un subcampo de $\mathbb{C}$.

Proposición 15. Un subconjunto B del anillo $(A, +, \cdot)$ es un subanillo de A si y sólo si $(B, +, \cdot)$ es cerrado bajo las dos operaciones y $\forall\ x \in B$, $-x \in B$, esto es, si $x - y \in B$ y $xy \in B\ \forall\ x, y \in B$.

Demostración. Sea B un subanillo del anillo $(A, +, \cdot)$. Por definición, $(B, +, \cdot)$ es un anillo, entonces:

i) $(B, +)$ es un grupo, por lo tanto:

- $+$ es cerrada en B, esto es, $\forall\ x, y \in B$, $x + y \in B$
- $\forall\ x \in B, \exists\ -x \in B$ tal que $x + (-x) = 0$

De tal forma, obtenemos que $\forall\ x, y \in B$, $x - y \in B$.

ii) $(B, \cdot)$ es un semigrupo, por lo tanto:

- $\cdot$ es cerrada en B, esto es, $\forall\ x, y \in B$, $x \cdot y \in B$.

De *i)* y *ii)* tenemos que $(B, +, \cdot)$ es cerrado bajo las operaciones $+$ y $\cdot$.

Ahora supongamos que B es un subconjunto del anillo $(A, +, \cdot)$ y se cumple que $x - y \in B$ y $xy \in B\ \forall\ x, y \in B$. Así:

i) Existe el neutro aditivo en B. $0 \in B$ ya que, en particular, $0 = x - x \in B$.

ii) Existen inversos aditivos en B. $0 \in B$, entonces, $\forall\ x \in B$, $0 - x \in B$, así, $-x \in B\ \forall\ x \in B$.

iii) $+$ es cerrada en B. $x - (-y) \in B\ \forall\ x, y \in B$, esto es, $x + y \in B$ $\forall\ x, y \in B$.

Nota: Las operaciones son asociativas y distributivas en B al ser $B \subset A$.

De *i), ii)* y *iii)* se tiene que $(B, +)$ es grupo y por hipótesis, $(B, \cdot)$ es cerrada en B, así, $(B, +, \cdot)$ es un subanillo de A.

□

Definición 37. Sean A y B subconjuntos de un anillo $(R, +, \cdot)$, definimos el producto entre A y B como: $AB = \{a \cdot b \mid a \in A \text{ y } b \in B\}$

Proposición 16. El subconjunto $\{0\}$ de un anillo es un subanillo.

Demostración. Utilizando la proposición 15, basta ver que $0 - 0 = 0 \in \{0\}$ y que $0 \cdot 0 = 0 \in \{0\}$. Por lo tanto $\{0\}$ es un subanillo.

□

Definición 38. Llamamos *ideal izquierdo* a un subanillo B de un anillo A si $\forall\ a \in A$ y $\forall\ b \in B$ se cumple que $ab \in B$, esto es, $AB \subset B$.

Análogamente definimos el *ideal derecho* si $\forall\ a \in A$ y $\forall\ b \in B$ se cumple que $ba \in B$, esto es, $BA \subset B$.

B es subanillo *ideal* de A si es ideal izquierdo e ideal derecho.

Observación: Sea A un anillo e I un ideal de A. Por definición $(A, +)$ tiene estructura de grupo abeliano y, por lo tanto, $(I, +)$ es un subgrupo normal de $(A, +)$.

Ejemplo 16. Es fácil notar que en un anillo A, los subanillos A y $\{0\}$ son ideales ya que:

- $AA = A \subset A$
- $\{0\}A = A\{0\} = \{0\} \subset \{0\}$

Estos dos subconjuntos son llamados *ideales triviales*. Los ideales distintos de estos son llamados *ideales propios* o *no triviales*.

Proposición 17. Sea A un anillo con uno e I un subanillo ideal también con uno, entonces, $I = A$.

Demostración. Como I es ideal de A, entonces, $AI \subset I$ y por nuestra hipótesis, $1 \in I$. De manera que $\forall\ a \in A, a = a1 \in aI \subset AI \subset I$, de manera que $A \subset I$ y así, $I = A$.

□

Proposición 18. Sea A un anillo con división, entonces, A únicamente tiene ideales triviales.

Demostración. Sea F un ideal no trivial de A, entonces, $\{0\} \neq F \neq A$.

Así, $\exists\ f \in F$ tal que $f \neq 0$. Como A es anillo con división, $\exists\ f^{-1} \in A$ tal que $f^{-1}f = 1$ de tal manera que $1 \in F$. Sabemos que $A = 1A \subset FA \subset F$, entonces, $F = A$ lo cual contradice nuestra hipótesis original. Por lo tanto, A tiene sólo ideales triviales.

□

Ejemplo 17. $(2\mathbb{Z}, +, \cdot)$ es subanillo ideal de $(\mathbb{Z}, +, \cdot)$.

Demostración. Sabemos que $2\mathbb{Z}$ es subgrupo de $\mathbb{Z}$, entonces:

i) $2\mathbb{Z}$ es subanillo de $\mathbb{Z}$. $(2\mathbb{Z}, +)$ es un grupo y $(2\mathbb{Z}, \cdot)$ es un semigrupo, así $(2\mathbb{Z}, +, \cdot) < (\mathbb{Z}, +, \cdot)$.

ii) $2\mathbb{Z}$ es ideal izquierdo de $\mathbb{Z}$. Sea $x \in \mathbb{Z}, y \in 2\mathbb{Z}, x = z_1$ y $y = 2z_2$ con $z_1, z_2 \in \mathbb{Z}$. Entonces, $xy = z_1 2z_2 = 2z_1 z_2 = 2z$, con $z = z_1 z_2 \in \mathbb{Z}$, de tal manera que $xy \in 2\mathbb{Z}$ y $\mathbb{Z}2\mathbb{Z} \subset 2\mathbb{Z}$.

iii) $2\mathbb{Z}$ es ideal derecho de $\mathbb{Z}$. Sea $x \in \mathbb{Z}, y \in 2\mathbb{Z}, x = z_1$ y $y = 2z_2$ con $z_1, z_2 \in \mathbb{Z}$. Entonces, $yx = 2z_2 z_1 = 2z$, con $z = z_2 z_1 \in \mathbb{Z}$, de tal manera que $yx \in 2\mathbb{Z}$ y $2\mathbb{Z}\mathbb{Z} \subset 2\mathbb{Z}$.

Por *i), ii)* y *iii)*, $(2\mathbb{Z}, +, \cdot)$ es subanillo ideal de $(\mathbb{Z}, +, \cdot)$.

□

Definición 39. Sean A un anillo e I un ideal de A tal que $I \neq A$. Decimos que I es un *ideal máximo* de A si para todo B ideal de A tal que $I \subset B \subset A$ se tiene que $B = A$ o $B = I$.

Proposición 19. Sea A un anillo conmutativo con uno con exactamente dos ideales (A y $\{0\}$), entonces, A es campo.

Demostración. Tenemos que demostrar que A es un anillo con división, esto es, $\forall\ x \in A, x \neq 0, x$ tiene inverso multiplicativo, por lo que basta mostrar que $A \setminus \{0\}$ forma un grupo bajo la multiplicación.

Sea $x \in A, x \neq 0$ y tomemos el conjunto $xA = \{xa \mid a \in A\}$. Veamos que xA es ideal de A. Sean $y, z \in xA$, entonces, $y = xa_1$ y $z = xa_2$ para algunos $a_1, a_2 \in A$, así:

i) $y+z = xa_1 + xa_2 = x(a_1 + a_2)$ con $a_1 + a_2 \in A$ por lo que $y+z \in xA$. Asimismo, $-y = -xa_1 = x(-a_1)$ con $-a_1 \in A$ por lo que $-y \in xA$ y, entonces, $\forall\ y, z \in xA, y - z \in xA$.

ii) $yz = xa_1xa_2 = x(a_1xa_2)$ con $a_1xa_2 \in A$ y así, $yz \in xA$.

iii) Sea $a \in A$, entonces, $ya = xa_1a = x(a_1a)$ con $a_1a \in A$, de manera que $\forall\ y \in xA$ y $a \in A$ se tiene que $ya \in xA$.

Por *i)* y *ii)*, xA es un subanillo de A y por *iii)*, xA es ideal de A.

Por hipótesis, $xA = \{0\}$ o $xA = A$. Como $0 \neq x = x1 \in xA$, entonces, $xA = A$. Por lo tanto, $\forall\ x \in A$, $\exists\ b \in A$ tal que $xb = 1$, esto es, $b = x^{-1}$. De manera que todo elemento de A distinto de 0 tiene inverso multiplicativo, por lo tanto, $A \setminus \{0\}$ es un grupo bajo la multiplicación.

Así, A es un anillo conmutativo con división y por lo tanto A es campo.

□

Definición 40. Sea A un anillo e I un ideal de A, decimos que I es un *ideal principal* de A si $\exists\ i \in A$ tal que $I = \{ia \mid a \in A\}$.

El subanillo ideal $I = \{ia \mid a \in A\}$ representa al *ideal de los múltiplos de* i y lo denotamos por $\langle i \rangle$. De manera que $\langle i \rangle = \{ia \mid a \in A\}$.

Teorema 15. Sea A un anillo euclidiano e I un ideal de A, entonces, $\exists\ i_0 \in I$ tal que $I = \{i_0a \mid a \in A\}$.

Demostración. Supongamos que $I = \{0\}$, entonces, $i_0 = 0$. De esta manera, $I = \{0\} = \{i_0a\ \forall\ a \in A\} = \{i_0a \mid a \in A\}$.

Ahora supongamos que $I \neq \{0\}$, por lo que al menos existe una $i \in I$ tal que $i \neq 0$. Como A es un anillo euclidiano, entonces, utilizando la función d como en la definición 33 (anillo euclidiano) y por el PBO (principio del buen orden), podemos escoger $i_0 \in I$ tal que $d(i_0)$ sea mínimo.

Sea $i \in I$, $\exists\ q, r \in A$ tales que $i = qi_0 + r$, en donde $r = 0$ o $d(r) < d(i_0)$. Como I es ideal de A, entonces, $qi_0 \in I$ e $i - qi_0 \in I$. Supongamos que $r \neq 0$, entonces, $d(r) < d(i_0)$ lo cual contradice el hecho de que $d(i_0)$ es mínimo, por

lo que $r = 0$. Así, $0 = r = i - qi_0$, y tenemos que $\forall\ i \in I$, $\exists\ q \in A$ tal que $i = qi_0 = i_0q$, por lo que $I = \{i_0a \mid a \in A\}$.

□

Definición 41. Sea D un dominio entero, se dice que D es un *anillo de ideales principales* si todo ideal I de D es de la forma $I = \langle i \rangle$ para algún $i \in D$.

Por el teorema 15, un anillo euclidiano es un anillo de ideales principales.

Lema 7. Sea A un anillo euclidiano, entonces, $\forall\ a, b \in A$, $\exists\ d \in A$ tal que $d = (a, b)$ y $d = \lambda a + \mu b$ con $\lambda, \mu \in A$.

Demostración. Sea $D = \{ra + sb \mid r, s \in A\}$. Veamos que D es un ideal de A.

Supongamos que $x, y \in D$, entonces, $x = r_1a + s_1b$ y $y = r_2a + s_2b$. Así, $x - y = (r_1a + s_1b) - (r_2a + s_2b) = (r_1 - r_2)a + (s_1 - s_2)b$, por lo que $x - y \in D$ y $xy = (r_1a + s_1b)(r_2a + s_2b) = (r_1ar_2 + r_1s_2b)a + (s_1r_2a + s_1bs_2)b$, por lo que $xy \in D$ y por lo tanto $D < A$. Ahora, sea $u \in A$, entonces, $ux = u(r_1a + s_1b) = (ur_1)a + (us_1)b$, de manera que $ux \in D\ \forall\ u \in A$ y D es un subanillo ideal de A.

Por el teorema 15, $\exists\ d \in D$ tal que $\forall\ z \in D, z = dt$ para algún $t \in A$, como $d \in D$, entonces, $d = \lambda a + \mu b$ para algunos $\lambda, \mu \in A$. Como A es un anillo euclidiano, tiene elemento unitario, así, $a = 1a + 0b \in D$ y $b = 0a + 1b \in D$, por lo tanto $d|a$ y $d|b$.

Supongamos que $\exists\ c \in A$ tal que $c|a$ y $c|b$, entonces, $c|\lambda a$ y $c|\mu b$ por lo que $c|(\lambda a + \mu b) = d$ y por lo tanto, $d = (a, b)$.

□

Proposición 20. Sea A un anillo euclidiano y sean $a, b \in A$ tal que b no es unidad de A, entonces, $d(a) < d(ab)$.

Demostración. Consideremos el ideal $I = \langle a \rangle = \{ax \mid x \in A\}$. Como A es un anillo euclidiano, entonces, $d(a) \leq d(ax)$, con $x \neq 0$, por lo que $d(a)$ es mínimo en I.

Supongamos que $d(a) = d(ab)$, entonces, $d(ab)$ es también mínimo y por el Teorema 15, todo elemento de I es un múltiplo de ab. En particular, $a \in I$ por lo que $a = abx$ para algún $x \in A$ de manera que $bx = 1$ y así b es una unidad, lo cual contradice nuestra hipótesis. Así, si b no es unidad de A, $d(a) < d(ab)$.

□

Lema 8. Sea A un anillo euclidiano, entonces, todo elemento en A o es una unidad o puede escribirse como el producto de un número finito de elementos primos en A.

Demostración. La prueba la haremos por inducción sobre $d(a)$.

Si $d(a) = d(1)$, entonces, a es una unidad (por la proposición 20) y se cumple la afirmación. Suponemos que esto es cierto para $d(x) < d(a)$ lo cual es nuestra hipótesis de inducción. Ahora sólo nos falta demostrarlo para a.

Si a es un elemento primo la afirmación queda demostrada. Supongamos entonces que a no es un elemento primo, por lo que $a = bc$ en donde b, c no son unidades, entonces, por la proposición 20, $d(b) < d(bc) = d(a)$ y $d(c) < d(bc) = d(a)$. Por nuestra hipótesis de inducción, b y c se pueden escibir como el producto de un número finito de elementos primos de A, esto es: $b = p_1 p_2 \cdots p_m$ y $c = q_1 q_2 \cdots q_n$ con $p_1, p_2, \ldots, p_m, q_1, q_2, \ldots, q_n$ elementos primos de A. De manera que $a = p_1 p_2 \cdots p_m q_1 q_2 \cdots q_n$ y a se puede escribir como el producto de un número finito de elementos primos de A.

□

Proposición 21. Sea A un anillo euclidiano y sean $a, b, c \in A$ tales que $a|bc$ y $(a, b) = 1$, entonces, $a|c$.

Demostración. Por el lema 7, sabemos que $\lambda a + \mu b = 1$ para algunos $\lambda, \mu \in A$. Multiplicando por c tenemos que $\lambda ac + \mu bc = c$. Sabemos que $a|\lambda ac$ y por hipótesis, $a|bc$. Por lo tanto, $a|\mu bc$. Así, $a|(\lambda ac + \mu bc) = c$ por lo que $a|c$.

□

Lema 9. Sea A un anillo euclidiano y sean $a, b, p \in A$ con p un elemento primo. Si $p|ab$, entonces, $p|a$ o $p|b$.

Demostración. Supongamos que $p \nmid a$, entonces, $(p, a) = 1$ y por la proposición 21, $p|b$.

□

Corolario 6. Sea A un anillo euclidiano y sean $p, a_1, a_2, \ldots, a_n \in A$ con p un elemento primo. Si $p|a_1a_2 \ldots a_n$, entonces, $p|a_i$ al menos para una i con $1 \leq i \leq n$.

Demostración. Veamos que $a_1a_2 \ldots a_n$ lo podemos escribir como $a_1(a_2 \ldots a_n)$. Si $p|a_1$ el corolario queda demostrado.

Supongamos que $p \nmid a_1$, entonces, por el lema 9, $p|a_2 \ldots a_n$ y continuamos con el mismo razonamiento. Al ser n un número finito, al cabo de $n-1$ pasos como máximo y con la ayuda del lema 9, si $p|a_1a_2 \ldots a_n$, entonces, $p|a_i$ al menos para una i con $1 \leq i \leq n$.

□

Teorema 16. (Teorema de la factorización única). Sea A un anillo euclidiano y $a \in A, a \neq 0$ y con a no una unidad. Supongamos que $a = p_1p_2 \cdots p_m = q_1q_2 \cdots q_n$, con $p_1, p_2 \ldots, p_m, q_1, q_2 \ldots, q_n$ elementos primos en A, entonces, $n = m$ y q_j es asociado de algún $p_i, 1 \leq i, j \leq n$.

Demostración. Supongamos, sin pérdida de generalidad, que $m < n$.

Sabemos que $p_1|p_1p_2 \cdots p_m = q_1q_2 \cdots q_n$, entonces, por el corolario 6 del lema 9, $p_1|q_j$ para algún $j \in \{1, \ldots, n\}$. Supongamos nuevamente sin pérdida de generalidad que $p_1|q_1$. Puesto que q_1 es un elemeto primo y por la definición 34, entonces, $q_1 = p_1u_1$, con u_1 una unidad en A. De esta manera, $p_1p_2 \cdots p_m = p_1u_1q_2 \cdots q_n$; cancelando p_1 tenemos que $p_2 \cdots p_m = u_1q_2 \cdots q_n$. Siguiendo este procedimiento, al cabo de m pasos tendremos que $1 = u_1u_2 \cdots u_mq_{m+1} \cdots q_n$.

Por el teorema 14, $1 = uq_{m+1} \cdots q_n$ con $u = u_1u_2 \cdots u_m$, u una unidad en A, de manera que $q_{m+1} \cdots q_n$ es también una unidad en A lo cual contradice el hecho de que todos los q_j son elementos primos y así, $m \not< n$.

Como $m \not< n$ y $n \not< m$, entonces, $n = m$ y $\forall\ i \in \{1, \ldots, n\}$, $q_i = p_iu_i$ con u_i una unidad en A y así q_i es asociado de p_i.

□

Observación: Podemos decir, con los resultados del lema 8 y del teorema 16, que en un anillo euclidiano A, todo elemento distinto de cero es o una unidad o puede ser escrito de forma única (salvo asociados) como el producto de elementos primos de A.

Proposición 22. Sean A un anillo euclidiano e $I = \langle i_0 \rangle$ un ideal de A, entonces, I es ideal máximo de A si y sólo si i_0 es un elemento primo de A.

Demostración. Supongamos que i_0 no es un elemento primo en A, por lo que $i_0 = bc$ con $b, c \in A$, b y c no unidades. Sea $B = \langle b \rangle$, así, $i_0 \in B$ e $I \subset B$.

> *i)* Supongamos que $B = A$. De esta manera, $1 \in B$ por lo que $1 = xb$ para algún $x \in A$ y, entonces, b es una unidad, lo cual es una contradicción y por lo tanto $B \neq A$.
>
> *ii)* Supongamos que $B = I$. De esta manera, $b \in I$ por lo que $b = yi_0$ para algún $y \in A$. Tenemos que $i_0 = bc = yci_0$ por lo que $yc = 1$, entonces, c es una unidad, lo cual es una contradicción y por lo tanto $B \neq I$.

Por *i)* y *ii)*, si i_0 no es un elemento primo, entonces, $\exists$ B un ideal de A tal que $I \subsetneq B \subsetneq A$ y por lo tanto, I no es ideal máximo, es decir, si I es un ideal máximo, entonces, i_0 es un elemento primo.

Por otra parte, supongamos que i_0 es un elemento primo de A y que M es un ideal de A tal que $I \subset M \subset A$. Por el teorema 15, $M = \langle m_0 \rangle$, $m_0 \in M$. Como $i_0 \in I \subset M = \langle m_0 \rangle$, entonces, $i_0 = zm_0$ para algún $z \in A$; por lo que z es unidad en A o m_0 es unidad en A.

> *i)* Si z es una unidad en A, $\exists$ $z^{-1} \in A$ tal que $zz^{-1} = 1$. Como $zm_0 = i_0$, entonces, $m_0 = z^{-1}i_0 \in I$, por lo que $M \subset I$ y, entonces, $M = I$.
>
> *ii)* Si m_0 es una unidad en A, entonces, $M = A$.

Por *i)* y *ii)*, si i_0 es un elemento primo, entonces, I es un ideal máximo.

□

Proposición 23. Sea $\Gamma = \{B_\lambda \mid \lambda \in \Lambda\}$ una familia de subanillos de A, entonces, $\bigcap\limits_{\lambda \in \Lambda} B_\lambda < A$.

Demostración. Sabemos que $(B_\lambda, +) < (A, +)$ $\forall$ $\lambda \in \Lambda$. Por el teorema 3, $\bigcap\limits_{\lambda \in \Lambda} (B_\lambda, +) < (A, +)$.

Sean $a, b \in \bigcap_{\lambda \in \Lambda} (B_\lambda, \cdot)$, entonces, $a, b \in (B_\lambda, \cdot)\ \forall\ \lambda \in \Lambda$. Como $(B_\lambda, \cdot)$ es un semigrupo $\forall\ \lambda \in \Lambda$, entonces, $ab \in (B_\lambda, \cdot)\ \forall\ \lambda \in \Lambda$ y así, $ab \in \bigcap_{\lambda \in \Lambda} (B_\lambda, \cdot)$.

Por lo tanto, $\bigcap_{\lambda \in \Lambda} B_\lambda < A$.

□

Definición 42. Sea $S \subset A$, a la intersección de todos los subanillos de A que contienen a S se le llama subanillo de A *generado por* S.

Definición 43. Sea A un anillo, definimos la *característica* de A como el menor entero positivo n que cumpla que $na = 0\ \forall\ a \in A$ y la denotamos como $car(A) = n$.

Si no existe tal entero positivo, entonces, decimos que el anillo A es de *característica* 0 y la denotamos como $car(A) = 0$.

Ejemplo 18. El anillo $\mathbb{Z}$ es de característica 0.

- Sea $n \in \mathbb{Z} \setminus \{0\}$, entonces, $nz \neq 0\ \forall\ z \neq 0$.

Así, $\mathbb{Z}$ tiene característica 0, esto es, $car(\mathbb{Z}) = 0$.

Ejemplo 19. El anillo $\mathbb{Z}_n$ es de característica n.

- Tenemos que $ni = 0\ \forall\ i \in \mathbb{Z}_n$.
- Sea $0 < k < n$, entonces, $k1 = k \neq 0$.

Así, n es el menor entero positivo tal que $ni = 0\ \forall\ i \in \mathbb{Z}_n$. Por lo tanto, $car(\mathbb{Z}_n) = n$.

4. Relaciones entre anillos

4.1. Homomorfismos e isomorfismos de anillos

Definición 44. Sean $(A, +, \cdot)$ y $(A', +', \cdot')$ dos anillos. Llamamos homomorfismo de anillos a una función φ que es un homomorfismo (de grupos) de $(A, +)$ en $(A', +')$ y es un homomorfismo del semigrupo $(A, \cdot)$ en $(A', \cdot')$, esto es, $\forall\ x, y \in A$ se cumplen las siguientes dos propiedades:

i) $\varphi(x + y) = \varphi(x) +' \varphi(y)$

ii) $\varphi(x \cdot y) = \varphi(x) \cdot' \varphi(y)$

y escribimos $\varphi : A \to A'$

Proposición 24. La composición de homomorfismos de anillos es un homomorfismo de anillos.

Demostración. Sean $\varphi : A \to A'$ y $\omega : A' \to A''$ dos homomorfismos de anillos. Por composición de funciones sabemos que $\omega \circ \varphi : A \to A''$ y que $\forall\ x, y \in A$:

i) $\omega \circ \varphi$ es un homomorfismo de $(A, +)$ en $(A', +')$ como se demostró en la proposición 5.

ii) $\omega \circ \varphi$ que es un homomorfismo de $(A, \cdot)$ en $(A', \cdot')$:

$$\begin{aligned}(\omega \circ \varphi)(x \cdot y) &= \omega(\varphi(x \cdot y)) \\ &= \omega(\varphi(x) \cdot' \omega(x)) \\ &= \omega(\varphi(x)) \cdot'' \omega(\varphi(y)) \\ &= (\omega \circ \varphi)(x) \cdot'' (\omega \circ \varphi)(y).\end{aligned}$$

Por *i)* y *ii)*, $\omega \circ \varphi$ es un homomorfismo de anillos de A en A''.

□

Lema 10. Si φ es homomorfismo, entonces, $\varphi(0) = 0'$.

Demostración. Sean $\varphi : A \to A'$ y $x \in A$, entonces, $\varphi(0) = \varphi(x - x) = \varphi(x) - \varphi(x) = 0'$, por lo tanto, $\varphi(0) = 0'$.

□

Definición 45. Sea $\varphi : A \to A'$ un homomorfismo.

El *núcleo* de φ es el conjunto de los elementos $x \in A$ tales que $\varphi(x) = 0'$ (neutro aditivo en el anillo A'). Al núcleo también se le conoce como *kernel* y se denota como kerφ.

$$\ker\varphi = \{\ x \in A \mid \varphi(x) = 0'\ \}$$

Llamamos *imagen* de φ al conjunto de todos los elementos $\varphi(x)$ tales que $x \in A$ y se denota como $\text{Img}\varphi$.

$$\text{Img}\varphi = \{\ \varphi(x) \mid x \in A\ \}$$

- Si φ es un homomorfismo y es inyectiva, diremos que φ es un *monomorfismo.*
- Si φ es un homomorfismo y es suprayectiva, diremos que φ es un *epimorfismo.*
- Si φ es monoformismo y epimorfismo, entonces, φ es biyectiva y diremos que φ es un *isomorfismo.*
- Si $\varphi : A \to A$ diremos que φ es un *endomorfismo.*
- Si $\varphi : A \to A$ y es biyectiva, diremos que φ es un *automorfismo.*
- Si $\varphi(x) = 0\ \forall\ x \in A$, esto es, $\text{Img}\varphi = \{0'\}$ o $\ker\varphi = A$, diremos que se trata de un *homomorfismo trivial.*

Proposición 25. Sea $\varphi : A \to A'$ un homomorfismo, entonces, $\ker\varphi = \{0\}$ si y sólo si φ es inyectiva.

Demostración. Supongamos que $\ker\varphi = \{0\}$ y sean $x, y \in A$ tales que $\varphi(x) = \varphi(y)$, entonces, $\varphi(x) - \varphi(y) = 0'$ y como φ es homomorfismo, tenemos que $\varphi(x - y) = \varphi(x) - \varphi(y) = 0'$ por lo que $x - y \in \ker\varphi = \{0\}$, así, $x - y = 0$ y $x = y$. Por lo tanto, φ es inyectiva.

Ahora, supongamos que φ es inyectiva. Sea $x \in \ker\varphi$, así, $\varphi(x) = 0' = \varphi(0)$ por lo que $\varphi(x) = \varphi(0)$ y, entonces $x = 0$. Por lo tanto, $\ker\varphi = \{0\}$.

□

Proposición 26. Si φ es isomorfismo, entonces, φ^{-1} es isomorfismo.

Demostración. Supongamos que $\varphi : A \to A'$ es un isomorfismo, entonces, φ es biyectiva, por lo tanto, $\varphi^{-1} : A' \to A$ es también biyectiva.

Sean $x', y' \in A'$, como φ es biyectiva, entonces, $\exists!\ x, y \in A$ tales que $\varphi(x) = x'$ y $\varphi(y) = y'$. Así, $\varphi^{-1}(\varphi(x)) = \varphi^{-1}(x')$ y $\varphi^{-1}(\varphi(y)) = \varphi^{-1}(y')$, por lo que $x = \varphi^{-1}(x')$ y $y = \varphi^{-1}(y')$, entonces:

i) φ^{-1} es un homomorfismo de $(A', +')$ en $(A, +)$ como se demostró en la proposición 7.

ii) φ^{-1} es un homomorfismo de $(A', \cdot')$ en $(A, \cdot)$:

$$\begin{aligned} \varphi^{-1}(x' \cdot' y') &= \varphi^{-1}(\varphi(x) \cdot' \varphi(y)) \\ &= \varphi^{-1}(\varphi(x \cdot y)) \\ &= \varphi^{-1}\varphi(x \cdot y) \\ &= x \cdot y \\ &= \varphi^{-1}(x') \cdot \varphi^{-1}(y') \end{aligned}$$

Por *i)* y *ii)*, φ^{-1} es homomorfismo y como φ^{-1} es biyectiva, entonces, φ^{-1} es un isomorfismo.

□

Definición 46. Llamamos *función identidad* a una función $\varphi : A \to A$ y está dada por:

$$\varphi(x) = x \ \forall \ x \in A$$

A la función identidad la denotamos por 1_A.

Proposición 27. Sea $(A, +, \cdot)$ un anillo, la función 1_A es un isomorfismo.

Demostración. Sea $\varphi = 1_A$.

i) φ es homomorfismo.

- $\varphi(x + y) = x + y = \varphi(x) + \varphi(y)$
- $\varphi(x \cdot y) = x \cdot y = \varphi(x) \cdot \varphi(y)$

ii) φ es inyectiva.

- Sea $\varphi(x) = \varphi(y)$, como $\varphi(x) = x$ y $\varphi(y) = y$, entonces, $x = y$.

iii) φ es suprayectiva.

- Sea $x \in A, x = \varphi(x)$.

Por *i)*, *ii)* y *iii)*, φ es un isomorfismo.

□

Definición 47. Sean A y B conjuntos, $A \subset B$, a la función $\iota : A \to B$ en donde $\iota(a) = a \ \forall \ a \in A$, se le llama función *inclusión* de A en B.

Proposición 28. Sean $\varphi : A \to A'$, $\omega : A' \to A''$ dos homomorfismos y $\Phi = \omega \circ \varphi$, entonces:

i) si Φ es monomorfismo, φ es monomorfismo.

ii) si Φ es epimorfismo, ω es epimorfismo.

Demostración. Sean φ y ω homomorfismos y $\Phi = \omega \circ \varphi$:

i) Supongamos que $\varphi(x) = \varphi(y)$, entonces, $\omega(\varphi(x)) = \omega(\varphi(y))$, esto es, $\Phi(x) = \Phi(y)$ y como Φ es monomorfismo, $x = y$. Por lo tanto, φ es monomorfismo.

ii) Φ es epimorfismo, entonces: $\forall \ z \in A'' \ \exists \ x \in A$ tal que $\Phi(x) = z$. $\Phi(x) = \omega(\varphi(x)) = z$. Así, $\forall \ z \in A'' \ \exists \ y \in A'$, a saber, $y = \varphi(x)$ tal que $\omega(y) = \omega(\varphi(x)) = z$ y por lo tanto, ω es epimorfismo.

□

Teorema 17. Sea $\varphi : A \to A'$ un homomorfismo de anillos, se cumplen:

i) Si I es ideal de A, entonces, $\varphi(I)$ es subanillo de A'.

ii) Si I' es ideal de A', entonces, $\varphi^{-1}(I')$ es ideal de A.

Demostración. Supongamos que φ es un homomorfismo de anillos, entonces:

i) Por el inciso *i)* del teorema 9, sabemos que $(\varphi(I), +)$ es subgrupo de $(A', +)$. Sean $a', b' \in \varphi(I)$, entonces, $\exists \ a, b \in I$ tales que $\varphi(a) = a'$ y $\varphi(b) = b'$. Como I es subanillo de A, tenemos que $ab \in I$ y como φ es homomorfismo, $\varphi(ab) = \varphi(a)\varphi(b) = a'b' \in \varphi(I)$ por lo que $\varphi(I)$ es cerrado bajo $\cdot$ y así, $\varphi(I)$ es subanillo de A'.

ii) Sea $\varphi^{-1}(I') = I$. Por el inciso *ii)* del teorema 9, sabemos que $(I, +)$ es subgrupo de $(A, +)$. Sean $x, y \in I$, entonces, $\varphi(x) = x'$ y $\varphi(y) = y'$ para algunos $x', y' \in I'$. Como I' es subanillo de A', entonces, $x'y' \in I'$ y así, $x'y' = \varphi(x)\varphi(y) = \varphi(xy) \in I'$ por lo que $xy \in I$. Así, I cerrado bajo $\cdot$ e I es subanillo de A.

Por último, sean $x' \in I'$ y $y \in A$. Así, $\exists\ x \in I$ y $y' \in A'$ tales que $\varphi(x) = x'$ y $\varphi(y) = y'$. Como I' es ideal de A', entonces, $x'y' \in I'$ y así, $x'y' = \varphi(x)\varphi(y) = \varphi(xy) \in I'$. Por lo tanto, $xy \in I\ \forall\ x \in I$ y $\forall\ y \in A$, de esta manera, I es ideal de A.

□

Corolario 7. Sea $\varphi : A \to A'$ un homomorfismo de anillos, entonces, Imgφ es subanillo de A' y kerφ es ideal de A.

Demostración. Img$\varphi = \{\varphi(a) \mid a \in A\} = \varphi(A)$ y como A es ideal de A, entonces, por el inciso *i)* del teorema 17, Imgφ es subanillo de A'.

ker$\varphi = \{a \in A \mid \varphi(a) = 0'\} = \varphi^{-1}(\{0'\})$ y como $\{0'\}$ es ideal de A', entonces, por el inciso *ii)* del teorema 17, kerφ es ideal de A.

□

4.2. Teoremas de isomorfismos de anillos

Definición 48. Sean A un anillo e I un ideal de A, definimos al conjunto $A/I = \{I + a \mid a \in A\}$. Este es el conjunto de *clases laterales* de I en A.

Observación: Como $(A, +)$ es un grupo abeliano, entonces, $a + I = I + a$.

Proposición 29. Sean A un anillo e I un ideal de A, entonces, $(A/I, +, \cdot)$ es un anillo con la operación $\cdot$ dada por $(I + a)(I + b) = I + ab\ \forall\ a, b \in A$.

Demostración. Como $(A, +)$ es un grupo abeliano e $I \subset A$, entonces, I es normal en A y $(A/I, +)$ es un grupo abeliano como se vio en la sección 1.2.

Primero veamos que la operación $\cdot$ está bien definida. Sean $a, a', b, b' \in A$ tales que $I+a = I+a'$ e $I+b = I+b'$, de esta manera, $a = u_1+a'$ y $b = u_2+b'$ con $u_1, u_2 \in I$, por lo que $ab = (u_1+a')(u_2+b') = u_1u_2+u_1b'+a'u_2+a'b'$. Como I es un ideal de A, entonces, $u_1b' \in I$ y $a'u_2 \in I$, por lo tanto, $ab = u+a'b'$ con

$u = u_1u_2 + u_1b' + a'u_2 \in I$, así, $I + ab = I + u + a'b' = I + a'b'$ ya que $I + u = I$ y de esta manera, $I + ab = I + a'b'$ por lo que la operación $\cdot$ está bien definida.

Veamos ahora que $(A, \cdot)$ es un semigrupo. Sean $x, y, z \in A/I$, entonces:

i) Cerradura: Sean $x = I + a$ y $y = I + b$ con $a, b \in A$, entonces, $xy = (I + a)(I + b) = I + ab$ y como $ab \in A$, entonces, $xy \in A/I$.

ii) Asociatividad: Sean $x = I + a, y = I + b$ y $z = I + c$ con $a, b, c \in A$, entonces:

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

Por *i)* y *ii)*, $(A/I, \cdot)$ es un semigrupo.

Por último, veamos que $\cdot$ distribuye a $+$. Sean $x = I + a, y = I + b$ y $z = I + c$ con $a, b, c \in A$, entonces:

i) $\cdot$ distribuye a $+$ por la izquierda:

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

ii) $\cdot$ distribuye a $+$ por la derecha:

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

Por *i)* y *ii)*, $\cdot$ distribuye a $+$.

Así, tenemos que $(A/I, +)$ es un grupo abeliano, $(A/I, \cdot)$ es un semigrupo y $\cdot$ distribuye a $+$, por lo tanto, $(A/I, +, \cdot)$ es un anillo.

□

Proposición 30. Sean A un anillo e I un ideal de A, entonces, existe un epimorfismo $\pi : A \to A/I$ y $\ker\pi = I$.

Demostración. Sea $\pi : A \to A/I$ dada por $\pi(a) = I + a \ \forall \ a \in A$:

i) Sean $a, b \in A$, entonces, $\pi(a + b) = I + (a + b) = (I + a) + (I + b) = \pi(a) + \pi(b)$, por lo tanto, π es un homomorfismo del grupo $(A, +)$ en $(A/I, +)$.

ii) Sean $a, b \in A$, entonces, $\pi(ab) = I + ab = (I + a)(I + b) = \pi(a)\pi(b)$, por lo tanto, π es un homomorfismo del semigrupo $(A, \cdot)$ en $(A/I, \cdot)$.

iii) Sea $x \in A/I$, entonces, $x = I + a$ para algún $a \in A$, por lo tanto, $\pi(a) = I + a = x$ y así, π es suprayectiva.

Por *i), ii)* y *iii)*, π es un epimorfismo de A sobre A/I.

Por último, veamos que:

$$\begin{aligned} \ker\pi &= \{a \in A \mid \pi(a) = 0'\} \\ &= \{a \in A \mid \pi(a) = I\} \\ &= \{a \in A \mid I + a = I\} \\ &= \{a \in A \mid a \in I\} \\ &= \{a \in I\} \\ &= I. \end{aligned}$$

Así, $\pi : A \to A/I$ es un epimorfismo y $\ker\pi = I$.

□

Al igual que en la sección 2.2 (isomorfismos de grupos), a la función π la conocemos como la *proyección canónica* de A sobre A/I.

Teorema 18. (Teorema de correspondencia). Sea I ideal de A. La proyección canónica $\pi : A \to A/I$ define una correspondencia biyectiva entre el conjunto de ideales de A que contienen a I y el conjunto de ideales de A/I.

Demostración. Supongamos que J' es ideal de A/I. Por el teorema 17, $\pi^{-1}(J')$ es un ideal de A. Sea $\pi^{-1}(J') = J$, de esta manera, $J' = \{I + j \mid j \in J\}$, en particular, $I + \pi(0) = I + 0' = I \in J'$ ya que $0 \in J$ por ser J ideal, esto es, $\pi(I) \subset J'$, por lo tanto, $\pi^{-1}(\pi(I)) \subset \pi^{-1}(J')$ y así, $I \subset J$.

Por otro lado, supongamos que $I \subset J$ y J es ideal de A. Por el teorema 17, $\pi(J) = J'$ es subanillo de A/I, a saber, $J' = \{I + j \mid j \in J\}$. Sea $x \in A/I$, así, $x = I + a$ para algún $a \in A$ por ser π epimorfismo. Como J es ideal de A, entonces, $aj \in J \; \forall \; a \in A$, de manera que, $xJ' = (I + a)(I + j) = I + aj \in J'$, por lo que, $AJ' \subset J'$ y J' es ideal de A/I.

Por lo tanto, existe una biyección entre los ideales de A que contienen a I con los ideales de A/I.

□

En otras palabras, si $I \subset J$ y J es ideal de A, entonces, $\pi(J)$ es ideal de A/I y si J' es ideal de A/I, entonces, $\pi^{-1}(J')$ es ideal de A e $I \subset \pi^{-1}(J')$.

Proposición 31. Sean I e I' ideales de A y A' respectivamente y las proyecciones canónicas $\pi : A \to A/I$ y $\pi' : A' \to A'/I'$. Si $\varphi : A \to A'$ es un homomorfismo tal que $\varphi(I) \subset I'$, entonces:

i) $\varphi^* : A/I \to A'/I'$, con $\varphi^*(I + a) = I' + \varphi(a)$ está bien definido y es un homomorfismo (inducido por φ).

ii) $\pi' \circ \varphi = \varphi^* \circ \pi$, es decir, el siguiente cuadro conmuta:

$$\begin{array}{ccc} A & \xrightarrow{\varphi} & A' \\ \downarrow{\scriptstyle \pi} & & \downarrow{\scriptstyle \pi'} \\ A/I & \xrightarrow{\varphi^*} & A'/I' \end{array}$$

iii) $\ker\varphi^* = \pi(\varphi^{-1}(I'))$ e $\mathrm{Img}\varphi^* = \pi'(\mathrm{Img}\varphi)$.

Demostración. Sea $\varphi : A \to A'$ un homomorfismo tal que $\varphi(I) \subset I'$, entonces:

i) Sean $x, y \in A/I$ tales que $x = y$. Como $x, y \in A/I$, entonces, $x = I + a$ y $y = I + b$ para algunos $a, b \in A$. De esta manera:

$$\begin{aligned} I + a = I + b &\Leftrightarrow a - b \in I \\ &\Rightarrow \varphi(a-b) \in I'; \quad \text{(por hipótesis, } \varphi(I) \subset I') \\ &\Leftrightarrow I' + \varphi(a-b) = I' \\ &\Leftrightarrow I' + \varphi(a) - \varphi(b) = I' \\ &\Leftrightarrow I' + \varphi(a) = I' + \varphi(b) \\ &\Leftrightarrow \varphi^*(I+a) = \varphi^*(I+b) \end{aligned}$$

Por lo tanto, φ^* está bien definido.

Ahora, sean $x, y \in A/I$, entonces, $x = I + a$ y $y = I + b$ para algunos $a, b \in A$, de manera que:

$$\begin{aligned} \varphi^*(x+y) &= \varphi^*((I+a)+(I+b)) \\ &= \varphi^*(I+(a+b)) \\ &= I' + \varphi(a+b) \\ &= I' + (\varphi(a)+\varphi(b)) \\ &= (I'+\varphi(a)) + (I'+\varphi(b)) \\ &= \varphi^*(x) + \varphi^*(y). \end{aligned}$$

Por último, veamos que:

$$\begin{aligned} \varphi^*(xy) &= \varphi^*((I+a)(I+b)) \\ &= \varphi^*(I+ab) \\ &= I' + ab \\ &= (I'+a)(I'+b) \\ &= \varphi^*(x)\varphi^*(y). \end{aligned}$$

De tal manera, $\varphi^*(x+y) = \varphi^*(x) + \varphi^*(y)$ y $\varphi^*(xy) = \varphi^*(x)\varphi^*(y)$ por lo que φ^* es homomorfismo (inducido por φ).

ii) Sean $\pi' \circ \varphi$ la composición de funciones y $a \in A$, entonces:

$$\begin{aligned} (\pi' \circ \varphi)(a) &= \pi'(\varphi(a)) \\ &= I' + \varphi(a) \\ &= \varphi^*(I+a) \\ &= \varphi^*(\pi(a)) \\ &= (\varphi^* \circ \pi)(a). \end{aligned}$$

Por lo que $\pi' \circ \varphi = \varphi^* \circ \pi$ y el cuadro conmuta.

iii) Veamos que $\ker\varphi^* = \pi(\varphi^{-1}(I'))$ y que $\text{Img}\varphi^* = \pi'(\text{Img}\varphi)$:

$$\begin{aligned}
\ker\varphi^* &= \{x \in A/I \mid \varphi^*(x) = I'\} \\
&= \{I + a \mid a \in A \text{ y } \varphi^*(I + a) = I'\} \\
&= \{I + a \mid a \in A \text{ e } I' + \varphi(a) = I'\} \\
&= \{I + a \mid a \in A \text{ y } \varphi(a) \in I'\} \\
&= \{I + a \mid a \in \varphi^{-1}(I')\} \\
&= \pi(\varphi^{-1}(I')).
\end{aligned}$$

$$\begin{aligned}
\text{Img}\varphi^* &= \{\varphi^*(x) \mid x \in A/I\} \\
&= \{\varphi^*(I + a) \mid a \in A\} \\
&= \{I' + \varphi(a) \mid a \in A\} \\
&= \{I' + \varphi(a) \mid \varphi(a) \in \text{Img}\varphi\} \\
&= \pi'(\text{Img}\varphi).
\end{aligned}$$

□

Teorema 19. (Primer teorema de isomorfismos de anillos). Sea $\varphi : A \to A'$ un homomorfismo, entonces, $A/\ker\varphi \cong \text{Img}\varphi$.

Demostración. Por el corolario 7 del teorema 17, $\text{Img}\varphi$ es un subanillo de A' y $\ker\varphi$ es ideal de A, por lo tanto, $\varphi : A \to \text{Img}\varphi$ es un epimorfismo y $A/\ker\varphi$ está bien definido.

Por la proposición 31, tenemos que φ^* es un homomorfismo, y es único puesto que $\varphi^*(I + a) = I' + \varphi(a)$, esto es, φ^* está determinado únicamente por φ. Sin pérdida de generalidad, tomamos $I' = \{0'\}$ por lo que $\varphi^*(I + a) = I' + \varphi(a) = 0' + \varphi(a) = \varphi(a)$ y tenemos:

i) $\ker\varphi^* = \pi(\varphi^{-1}(I')) = \pi(\varphi^{-1}(\{0'\})) = \pi(\ker\varphi) = 0_{A/\ker\varphi}$ por lo que φ^* es monomorfismo.

ii) $\text{Img}\varphi^* = \pi'(\text{Img}\varphi) = \text{Img}\varphi$ y como $\text{Img}\varphi \cong \text{Img}\varphi/\{0'\}$, entonces, φ^* es epimorfismo.

Por *i)* y *ii)*, φ^* es un isomorfismo.

Por lo tanto, $A/\ker\varphi \cong \text{Img}\varphi$ y el siguiente diagrama conmuta:

$$\begin{array}{ccc}
A & \xrightarrow{\varphi} & \text{Img}\varphi \\
\downarrow{\scriptstyle \pi} & \cong\nearrow_{\varphi^*} & \\
A/\ker\varphi & &
\end{array}$$

□

Teorema 20. (Segundo teorema de isomorfismos de anillos). Sean I y J ideales de A, entonces, $(I+J)/J \cong I/(I \cap J)$.

Demostración. Veamos que $I/(I \cap J)$ está bien definido:

i) $(I \cap J) \subset I$ y por el teorema 23, $(I \cap J) < I$.

ii) Sean $a \in I$ y $x \in (I \cap J)$:

- Como $x \in (I \cap J)$, entonces, $x \in I$ y como I es ideal de A, tenemos que $ax \in I$ y $xa \in I$.
- Como $x \in (I \cap J)$, entonces, $x \in J$ y como J es ideal de A, tenemos que $ax \in J$ y $xa \in J$.

Así, $\forall\ a \in I$ y $\forall\ x \in (I \cap J)$ tenemos que $ax \in (I \cap J)$ y $xa \in (I \cap J)$, por lo que $I \cap J$ es ideal de I.

Por *i)* y *ii)*, $I/(I \cap J)$ está bien definido.

Por otro lado, $(I+J) = \{i+j \mid i \in I \text{ y } j \in J\}$ y sea $\eta : (I+J) \to I/(I \cap J)$ dada por $\eta(i+j) = (I \cap J) + i$, veamos que η está bien definida y es un homomorfismo:

i) Sea $i'+j' = i+j$, entonces, $-i+i' = j-j'$, de manera que $-i+i' \in I$ y $-i+i' \in J$, por lo que $-i+i' \in (I \cap J)$. Así, en $I/(I \cap J)$ tenemos que $(I \cap J)+i = (I \cap J)+i'$ y $\eta(i+j) = \eta(i'+j')$, por lo que η está bien definida.

ii) Sean $x_1, x_2 \in (I+J)$, entonces, $x_1 = i_1 + j_1$ y $x_2 = i_2 + j_2$ con $i_1, i_2 \in I$ y $j_1, j_2 \in J$, de manera que:

$$\begin{aligned}
\eta(x_1 + x_2) &= \eta[(i_1 + j_1) + (i_2 + j_2)] \\
&= \eta[i_1 + j_1 + i_2 + j_2] \\
&= \eta[(i_1 + i_2) + (j_1 + j_2)] \\
&= \eta[(i_1 + i_2) + j] \\
&= (I \cap J) + (i_1 + i_2) \\
&= [(I \cap J) + i_1] + [(I \cap J) + i_2] \\
&= \eta(i_1 + j_1) + \eta(i_2 + j_2) \\
&= \eta(x_1) + \eta(x_2).
\end{aligned}$$

Con $j = j_1 + j_2 \in J$. Por otro lado, tenemos que:

$$\begin{aligned}
\eta(x_1x_2) &= \eta[(i_1 + j_1)(i_2 + j_2)] \\
&= \eta[i_1(i_2 + j_2) + j_1(i_2 + j_2)] \\
&= \eta[i_1i_2 + i_1j_2 + j_1i_2 + j_1j_2] \\
&= \eta[i_1i_2 + j] \\
&= (I \cap J) + i_1i_2 \\
&= [(I \cap J) + i_1][(I \cap J) + i_2] \\
&= \eta(i_1 + j_1)\eta(i_2 + j_2) \\
&= \eta(x_1)\eta(x_2).
\end{aligned}$$

Con $j = i_1j_2 + j_1i_2 + j_1j_2 \in J$. Por lo tanto, η es un homomorfismo.

Por último, veamos que:

$$\begin{aligned}
\ker\eta &= \{x \in I + J \mid \eta(x) \in (I \cap J)\} \\
&= \{i + j \mid i \in I,\ j \in J \text{ y } \eta(i + j) = (I \cap J)\} \\
&= \{i + j \mid i \in I,\ j \in J \text{ y } (I \cap J) + i = (I \cap J)\} \\
&= \{i + j \mid i \in I,\ j \in J \text{ e } i \in (I \cap J)\} \\
&= \{i + j \mid i \in I,\ j \in J \text{ e } i \in J\} \\
&= \{i + j \mid i \in J \text{ y } j \in J\} \\
&= J.
\end{aligned}$$

Sea $x \in I/(I \cap J)$, entonces, $x = (I \cap J) + i$ para algún $i \in I$. De manera que $\forall\ i \in I$, $\eta(i + j) = (I \cap J) + i$, por lo tanto, η es epimorfismo y así, por el teorema 19 (primer teorema de isomorfismos de anillos), $(I + J)/J \cong I/(I \cap J)$. □

Teorema 21. (Tercer teorema de isomorfismos de anillos). Sean I, J ideales de A tales que $J \subset I$, entonces, $A/I \cong (A/J)/(I/J)$.

Demostración. Sean $\eta : A \to (A/J)/(I/J)$ dada por $\eta(a) = (J + a) + (I/J)$ y $a_1, a_2 \in A$, entonces:

$$\begin{aligned}
\eta(a_1 + a_2) &= [J + (a_1 + a_2)] + (I/J) \\
&= [(J + a_1) + (J + a_2)] + (I/J) \\
&= [(J + a_1) + (I/J)] + [(J + a_2) + (I/J)] \\
&= \eta(a_1) + \eta(a_2).
\end{aligned}$$

$$\begin{aligned}
\eta(a_1a_2) &= [J + (a_1a_2)] + (I/J) \\
&= [(J + a_1)(J + a_2)] + (I/J) \\
&= [(J + a_1) + (I/J)][(J + a_2) + (I/J)] \\
&= \eta(a_1)\eta(a_2).
\end{aligned}$$

De manera que η es homomorfismo. Por último:

$$\begin{aligned}
\ker\eta &= \{a \in A \mid \eta(a) = I/J\} \\
&= \{a \in A \mid (J+a)+(I/J) = (I/J)\} \\
&= \{a \in A \mid (J+a)+(J+i) = (J+i') \text{ para algunos } i, i' \in I\} \\
&= \{a \in A \mid [(J+(a+i)] = (J+i') \text{ para algunos } i, i' \in I\} \\
&= \{a \in A \mid a+i = i' \text{ para algunos } i, i' \in I\} \\
&= \{a \in A \mid a \in I\} \\
&= I.
\end{aligned}$$

Por lo tanto, por el teorema 19 (primer teorema de isomorfismos de anillos), $A/I \cong (A/J)/(I/J)$.

□

Teorema 22. Sean A un anillo conmutativo con uno e I un ideal de A, entonces, I es ideal máximo si y sólo si, A/I es campo.

Demostración. Supongamos que I es ideal máximo de A, por lo que los únicos ideales que lo contienen son A y él mismo. Por el teorema 18, A/I tiene únicamente los ideales $\{0\}$ y él mismo. Como A es conmutativo con uno, entonces, A/I también es conmutativo con uno y, por la proposición 19, A/I es campo.

Ahora, supongamos que A/I es campo, entonces, A/I es un anillo con división. Por la proposición 18, A/I únicamente tiene ideales triviales, a saber, $\{0\}$ y él mismo. Por el teorema 18, A tiene únicamente dos ideales que contienen a I, estos son, los ideales A e I mismo, por lo tanto, I es ideal máximo.

□

5. Anillo de polinomios sobre un campo en una indeterminada

5.1. Definiciones y operaciones con polinomios

Definición 49. Sean F un campo y x una indeterminada. Un *polinomio* en x con coeficientes en F es un objeto de la forma:

$$a_0x^0 + a_1x^1 + \cdots + a_nx^n + a_{n+1}x^{n+1} + \cdots$$

en donde $a_i \in F \ \forall \ i \in \mathbb{N}$ y $a_m = 0 \ \forall \ m > n$ para algún $n \in \mathbb{N}$. A un polinomio en la indeterminada x generalmente lo denotamos por:

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

Observación: Si el polinomio $f(x) = \sum_{i=0}^{\infty} a_i x^i$, entonces, para algún $n \in \mathbb{N}$, $f(x) = \sum_{i=0}^{n} a_i x^i + \sum_{i=n+1}^{\infty} a_i x^i$, en donde $a_i = 0 \ \forall \ i > n$.

Al conjunto de todos los polinomios con coeficientes en el campo F sobre la indeterminada x lo denotamos por $F[x]$ y lo escribimos como:

$$F[x] = \{f(x) = \sum_{i=0}^{\infty} a_i x^i \mid a_i \in F \ \forall \ i \in \mathbb{N} \text{ y } a_m = 0 \ \forall \ m > n \text{ para algún } n \in \mathbb{N}\}.$$

Definición 50. Sean $F[x]$ como en la definición 49 y $f(x), g(x) \in F[x]$ con $f(x) = \sum_{i=0}^{\infty} a_i x^i$ y $g(x) = \sum_{j=0}^{\infty} b_j x^j$; definimos la *igualdad* de $f(x)$ y $g(x)$ como sigue:

$$f(x) = g(x) \text{ si y sólo si } a_i = b_i \ \forall \ i \in \mathbb{N}.$$

Definición 51. Sean $F[x]$ como en la definición 49 y $f(x), g(x) \in F[x]$ con $f(x) = \sum_{i=0}^{\infty} a_i x^i$ y $g(x) = \sum_{j=0}^{\infty} b_j x^j$; definimos la *suma* de $f(x)$ y $g(x)$ como sigue: $f(x) + g(x) = h(x) = c_0x^0 + c_1x^1 + \cdots$, en donde $c_k = a_k + b_k \ \forall \ k \in \mathbb{N}$, esto es:

$$f(x) + g(x) = h(x) = \sum_{k=0}^{\infty} (a_k + b_k)x^k.$$

Definición 52. Sean $F[x]$ como en la definición 49 y $f(x), g(x) \in F[x]$ con $f(x) = \sum_{i=0}^{\infty} a_i x^i$ y $g(x) = \sum_{j=0}^{\infty} b_j x^j$; definimos el *producto* de $f(x)$ y $g(x)$ como sigue: $f(x)g(x) = h(x) = c_0x^0 + c_1x^1 + \cdots$, en donde $\forall \ k \in \mathbb{N}$, $c_k = a_kb_0 + a_{k-1}b_1 + \cdots + a_0b_k$, esto es:

$$f(x)g(x) = h(x) = \sum_{k=0}^{\infty}(\sum_{h=0}^{k} a_h b_{k-h})x^k.$$

Corolario 8. Si $f(x) = x^i$ y $g(x) = x^j$, entonces, $f(x)g(x) = x^{i+j}$.

Demostración. Como $f(x) = x^i$, entonces, $f(x) = \sum_{k=0}^{\infty} a_k x^k$ con $a_i = 1$ y $a_k = 0 \ \forall \ k \neq i$; de igual manera, como $g(x) = x^j$, entonces, $g(x) = \sum_{k=0}^{\infty} b_k x^k$ con $b_j = 1$ y $b_k = 0 \ \forall \ k \neq j$.

Por la definición 52, $f(x)g(x) = h(x) = \sum_{k=0}^{\infty}(\sum_{h=0}^{k} a_h b_{k-h})x^k$. Observemos que $a_h b_{k-h} \neq 0$ si y sólo si $h = i$ y $k - h = j$, esto es, si y sólo si $k = i + j$, por lo que, $\sum_{h=0}^{k} a_h b_{k-h} \neq 0$ si y sólo si $k = i + j$, por lo tanto, $h(x) = (a_i b_j)x^{i+j}$; como $a_i = 1$ y $b_j = 1$, entonces, $h(x) = [(1)(1)]x^{i+j} = 1x^{i+j} = x^{i+j}$.

Por lo tanto, si $f(x) = x^i$ y $g(x) = x^j$, entonces, $f(x)g(x) = x^{i+j}$.

□

Proposición 32. $(F[x], +, \cdot)$ es un anillo conmutativo con las operaciones $+$ y $\cdot$ de las definiciones 51 y 52.

Demostración. 1.- Veamos que $(F[x], +)$ es un grupo abeliano. Por la definición 51, $\forall \ f(x), g(x) \in F[x]$ con $f(x) = \sum_{k=0}^{\infty} a_i x^i$ y $g(x) = \sum_{k=0}^{\infty} b_j x^j$, $f(x) + g(x) = \sum_{k=0}^{\infty}(a_k + b_k)x^k$, entonces, como $a_k, b_k \in F \ \forall \ k \in \mathbb{N}$, se cumplen:

i) $a_k + b_k \in F \ \forall \ k \in \mathbb{N}$. Por la observación en la definición 49, $a_i = 0$ $\forall \ i > m$ para algún $m \in \mathbb{N}$ y $b_j = 0 \ \forall \ j > n$ para algún $n \in \mathbb{N}$, así, $a_k + b_k = 0 \ \forall \ k > \text{máx}\{m, n\}$ y por lo tanto, $f(x) + g(x) \in (F[x], +)$ y así, $(F[x], +)$ es cerrado.

ii) Sean $f(x) = \sum_{i=0}^{\infty} a_i x^i, g(x) = \sum_{j=0}^{\infty} b_j x^j$ y $h(x) = \sum_{h=0}^{\infty} c_h x^h$, entonces:

$$\begin{aligned} f(x)+[g(x)+h(x)] &= \sum_{i=0}^{\infty} a_i x^i + [\sum_{j=0}^{\infty} b_j x^j + \sum_{h=0}^{\infty} c_h x^h] \\ &= \sum_{i=0}^{\infty} a_i x^i + \sum_{k=0}^{\infty} (b_k + c_k) x^k \\ &= \sum_{i=0}^{\infty} [a_i + (b_i + c_i)] x^i \\ &= \sum_{i=0}^{\infty} [(a_i + b_i) + c_i] x^i \\ &= \sum_{i=0}^{\infty} [(a_i + b_i) x^i + c_i x^i] \\ &= \sum_{i=0}^{\infty} (a_i + b_i) x^i + \sum_{i=0}^{\infty} c_i x^i \\ &= [\sum_{i=0}^{\infty} a_i x^i + \sum_{j=0}^{\infty} b_j x^j] + \sum_{h=0}^{\infty} c_h x^h \\ &= [f(x)+g(x)]+h(x). \end{aligned}$$

De esta manera, $(F[x],+)$ es asociativo.

iii) $\forall\ f(x), g(x) \in F[x]$ tenemos que $f(x)+g(x) = \sum_{k=0}^{\infty}(a_k+b_k)x^k = \sum_{k=0}^{\infty}(b_k+a_k)x^k = g(x)+f(x)$, por lo tanto, $(F[x],+)$ es conmutativo.

iv) Sea $0 \in F$, tomamos $\sum_{k=0}^{\infty} 0x^k \in F[x]$ y lo denotamos por $\overline{0}$, entonces, $\forall\ f(x) \in F[x]$ tenemos que:

$$\begin{aligned} f(x)+\overline{0} &= \sum_{k=0}^{\infty} a_k x^k + \sum_{k=0}^{\infty} 0x^k \\ &= \sum_{k=0}^{\infty} (a_k + 0) x^k \\ &= \sum_{k=0}^{\infty} a_k x^k \\ &= f(x). \end{aligned}$$

Por lo tanto, $\overline{0}$ es el neutro aditivo de $(F[x],+)$.

v) Sea $f(x) = \sum_{k=0}^{\infty} a_k x^k$. Como $a_k \in F\ \forall\ k \in \mathbb{N}$, $\exists\ b_k \in F$ tal que $b_k = -a_k$ $\forall\ k \in \mathbb{N}$. Sea $g(x) = \sum_{k=0}^{\infty} b_k x^k$, entonces, $f(x)+g(x) = \sum_{k=0}^{\infty}(a_k+b_k)x^k =$

$\sum_{k=0}^{\infty}(a_k + (-a_k))x^k = \sum_{k=0}^{\infty}0x^k = \overline{0}$, por lo que $g(x) = -f(x)$ y así, todo elemento de $F[x]$ tiene inverso aditivo.

Por *i), ii), iii), iv)* y *v)*, $(F[x], +)$ es un grupo abeliano.

2.- Ahora, veamos que $(F[x], \cdot)$ es un semigrupo conmutativo. La definición 52 indica que $\forall\ f(x), g(x) \in F[x]$, con $f(x) = \sum_{k=0}^{\infty}a_i x^i$ y $g(x) = \sum_{k=0}^{\infty}b_j x^j$, $f(x)g(x) = \sum_{k=0}^{\infty}(\sum_{h=0}^{k}a_h b_{k-h})x^k$, entonces, como $a_k, b_k \in F\ \forall\ k \in \mathbb{N}$, se cumplen:

i) $a_i b_j \in F\ \forall\ i, j \in \mathbb{N}$. Como $a_i = 0\ \forall\ i > m$ para algún $m \in \mathbb{N}$ y $b_j = 0$ $\forall\ j > n$ para algún $n \in \mathbb{N}$, entonces, $\sum_{h=0}^{k}a_h b_{k-h} = 0\ \forall\ k > m + n$, por lo tanto, $f(x)g(x) \in (F[x], \cdot)$ y así, $(F[x], \cdot)$ es cerrado.

ii) Sean $f(x) = \sum_{i=0}^{\infty}a_i x^i$ y $g(x) = \sum_{j=0}^{\infty}b_j x^j$, entonces:

$$\begin{aligned} f(x)g(x) &= (\sum_{i=0}^{\infty}a_i x^i)(\sum_{j=0}^{\infty}b_j x^j) \\ &= \sum_{k=0}^{\infty}(\sum_{h=0}^{k}a_h b_{k-h})x^k \\ &= \sum_{k=0}^{\infty}(\sum_{h=0}^{k}b_{k-h}a_h)x^k \\ &= \sum_{k=0}^{\infty}(\sum_{h=0}^{k}b_h a_{k-h})x^k \\ &= (\sum_{j=0}^{\infty}b_j x^j)(\sum_{i=0}^{\infty}a_i x^i) \\ &= g(x)f(x). \end{aligned}$$

De esta manera, $(F[x], \cdot)$ es conmutativo.

iii) Sean $f(x) = \sum_{i=0}^{\infty}a_i x^i, g(x) = \sum_{j=0}^{\infty}b_j x^j$ y $h(x) = \sum_{k=0}^{\infty}c_k x^k$, entonces:

$$
\begin{aligned}
f(x)[g(x)h(x)] &= \sum_{i=0}^{\infty} a_i x^i [\sum_{j=0}^{\infty} b_j x^j \sum_{k=0}^{\infty} c_k x^k] \\
&= \sum_{i=0}^{\infty} a_i x^i [\sum_{j=0}^{\infty} (\sum_{h=0}^{j} b_h c_{j-h}) x^j] \\
&= \sum_{i=0}^{\infty} [\sum_{r=0}^{i} a_r \sum_{s=0}^{i-r} b_s c_{i-r-s}] x^i \\
&= \sum_{i=0}^{\infty} [\sum_{r=0}^{i} \sum_{s=0}^{i-r} a_r b_s c_{i-r-s}] x^i \\
&= \sum_{i=0}^{\infty} [\sum_{r=0}^{i} \sum_{s=0}^{i-r} a_s b_{i-r-s} c_r] x^i \\
&= \sum_{i=0}^{\infty} [\sum_{r=0}^{i} c_r \sum_{s=0}^{i-r} a_s b_{i-r-s}] x^i \\
&= \sum_{i=0}^{\infty} c_i x^i [\sum_{j=0}^{\infty} (\sum_{h=0}^{j} a_h b_{j-h}) x^j] \\
&= [\sum_{j=0}^{\infty} (\sum_{h=0}^{j} a_h b_{j-h}) x^j] \sum_{i=0}^{\infty} c_i x^i \\
&= [f(x)g(x)]h(x).
\end{aligned}
$$

De esta manera, $(F[x], \cdot)$ es asociativo.

Por *i)*, *ii)* y *iii)*, $(F[x], \cdot)$ es un semigrupo conmutativo.

3.- Por último, vamos a demostrar que + distribuye a $\cdot$. Sean $f(x) = \sum_{i=0}^{\infty} a_i x^i$, $g(x) = \sum_{j=0}^{\infty} b_j x^j$ y $h(x) = \sum_{k=0}^{\infty} c_k x^k$, entonces:

$$\begin{aligned}
f(x)[g(x)+h(x)] &= \sum_{i=0}^{\infty} a_i x^i [\sum_{j=0}^{\infty} b_j x^j + \sum_{k=0}^{\infty} c_k x^k] \\
&= \sum_{i=0}^{\infty} a_i x^i [\sum_{j=0}^{\infty} (b_j + c_j) x^j] \\
&= \sum_{i=0}^{\infty} [\sum_{h=0}^{i} a_h (b_{i-h} + c_{i-h})] x^i \\
&= \sum_{i=0}^{\infty} [\sum_{h=0}^{i} (a_h b_{i-h} + a_h c_{i-h})] x^i \\
&= \sum_{i=0}^{\infty} [\sum_{h=0}^{i} (a_h b_{i-h} x^i + a_h c_{i-h} x^i)] \\
&= \sum_{i=0}^{\infty} [\sum_{h=0}^{i} a_h b_{i-h} x^i + \sum_{h=0}^{i} a_h c_{i-h} x^i] \\
&= \sum_{i=0}^{\infty} [\sum_{h=0}^{i} a_h b_{i-h} x^i] + \sum_{i=0}^{\infty} [\sum_{h=0}^{i} a_h c_{i-h} x^i] \\
&= \sum_{i=0}^{\infty} a_i x^i \sum_{j=0}^{\infty} b_j x^j + \sum_{i=0}^{\infty} a_i x^i \sum_{k=0}^{\infty} c_k x^k \\
&= f(x)g(x) + f(x)h(x).
\end{aligned}$$

De manera que $+$ distribuye a $\cdot$.

Así, por 1, 2 y 3, $(F[x], +, \cdot)$ es un anillo conmutativo.

□

Nota: A partir de este momento y para simplificar la notación al igual que lo hicimos en los capítulos de grupos y anillos, al anillo de polinomios en una indeterminada x con coeficientes en F lo denotaremos únicamente por $F[x]$, tomando en cuenta que las operaciones que utilizamos son las de las definiciones 51 y 52.

Proposición 33. $F[x]$ es un anillo con uno.

Demostración. Sean $0, 1 \in F$, tomamos $\sum_{i=0}^{\infty} b_i x^i \in F[x]$ con $b_0 = 1$ y $b_k = 0$ $\forall\ k \geq 1$ y lo denotamos por $\overline{1}$, esto es:

$$\begin{aligned}
\overline{1} &= 1x^0 + 0x^1 + 0x^2 + \cdots \\
&= 1x^0 + \sum_{k=1}^{\infty} 0x^k \\
&= (1+0)x^0 + \sum_{k=1}^{\infty} 0x^k \\
&= 1x^0 + 0x^0 + \sum_{k=1}^{\infty} 0x^k \\
&= x^0 + \sum_{k=0}^{\infty} 0x^k \\
&= x^0 + \overline{0} \\
&= x^0.
\end{aligned}$$

Sea $f(x) \in F[x]$ con $f(x) = \sum_{i=0}^{\infty} a_i x^i$, entonces, por el corolario 8 tenemos que:

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

Por la proposición 32, $F[x]$ es conmutativo, así, $f(x)\overline{1} = \overline{1}f(x) = f(x)$ y por lo tanto, $F[x]$ es un anillo con uno.

□

Nota: Cuando nos refiramos a los elementos $\overline{0}, \overline{1} \in F[x]$ de ahora en adelante lo haremos como 0 y 1 respectivamente y únicamente cuando el contexto no permita confusión con el 0 y 1 del campo F.

5.2. Función grado, algoritmo de la división y polinomios irreducibles

Definición 53. Sea $0 \neq f(x) = \sum_{i=0}^{\infty} a_i x^i$. Por la observación en la definición 49, $\exists\ n \in \mathbb{N}$ tal que $f(x) = \sum_{i=0}^{n} a_i x^i + \sum_{i=n+1}^{\infty} a_i x^i$ con $a_i = 0\ \forall\ i > n$ y $a_n \neq 0$, entonces, decimos que el polinomio $f(x)$ es de *grado* n y lo denotamos como $\text{grad} f(x) = n$.

Decimos que un polinomio es *constante* si se trata del polinomio 0 o si el grado del polinomio es 0.

Observación: A partir de este momento para simplificar la notacion, al referirnos al polinomio $f(x) = \sum_{i=0}^{\infty} a_i x^i$, lo podremos hacer únicamente como $f(x) = \sum_{i=0}^{n} a_i x^i$ teniendo en cuenta que $a_i = 0\ \forall\ i > n$ con a_n no necesariamente 0, esto es, $\text{grad} f(x) \leq n$.

Definición 54. Sea $f(x) = \sum_{i=0}^{n} a_i x^i$ tal que $\text{grad} f(x) = n$, decimos que $f(x)$ es *mónico* si $a_n = 1$.

Lema 11. Sean $f(x), g(x) \in F[x]$ tales que $f(x) \neq 0$, $g(x) \neq 0$ y $f(x) + g(x) \neq 0$, entonces, $\text{grad}(f(x) + g(x)) \leq \text{máx}\ \{\text{grad} f(x), \text{grad} g(x)\}$.

Demostración. Sean $f(x) = \sum_{i=0}^{m} a_i x^i$ y $g(x) = \sum_{j=0}^{n} b_j x^j$ para algunos $m, n \in \mathbb{N}$ tales que $a_m \neq 0$ y $b_n \neq 0$, entonces, $\text{grad} f(x) = m$ y $\text{grad} g(x) = n$. Sin pérdida de generalidad, suponemos que $m \geq n$, por la definición 51, sabemos que $f(x) + g(x) = h(x) = \sum_{k=0}^{\infty} c_k x^k$; $a_i = 0\ \forall\ i > m$ y $b_j = 0\ \forall\ j > n$. De esta manera, $a_k + b_k = 0\ \forall\ k > m$ y así tenemos que $h(x) = \sum_{k=0}^{l} c_k x^k + \sum_{k=l+1}^{\infty} c_k x^k$ para algún $l \leq m$, de manera que, $\text{grad} h(x) = l \leq m$. Por lo tanto, $\text{grad}(f(x) + g(x)) \leq \text{máx}\ \{\text{grad} f(x), \text{grad} g(x)\}$.

□

Lema 12. Sean $f(x), g(x) \in F[x]$ tales que $f(x) \neq 0$ y $g(x) \neq 0$, entonces, $\text{grad}(f(x)g(x)) = \text{grad} f(x) + \text{grad} g(x)$.

Demostración. Sean $f(x) = \sum_{i=0}^{m} a_i x^i$ y $g(x) = \sum_{j=0}^{n} b_j x^j$ con $\text{grad}f(x) = m$ y $\text{grad}g(x) = n$, entonces, $a_m \neq 0$ y $b_n \neq 0$, por lo que $a_m b_n \neq 0$. Por la definición 52, $f(x)g(x) = r(x) = \sum_{k=0}^{\infty}(\sum_{h=0}^{k} a_h b_{k-h})x^k$; $a_i = 0 \ \forall \ i > m$ y $b_j = 0$ $\forall \ j > n$, entonces, $\sum_{h=0}^{k} a_h b_{k-h} = 0 \ \forall \ k > m+n$ y $\sum_{h=0}^{k} a_h b_{k-h} = a_m b_n \neq 0$ para $k = m+n$.

Por lo tanto, $\text{grad}(f(x)g(x)) = k = m+n = \text{grad}f(x) + \text{grad}g(x)$, de manera que $\text{grad}(f(x)g(x)) = \text{grad}f(x) + \text{grad}g(x)$.

□

Corolario 9. Sean $f(x), g(x) \in F[x]$ tales que $f(x) \neq 0$ y $g(x) \neq 0$, entonces, $\text{grad}f(x) \leq \text{grad}(f(x)g(x))$.

Demostración. Como $f(x) \neq 0$ y $g(x) \neq 0$, entonces, $\text{grad}f(x) = m \geq 0$ y $\text{grad}g(x) = n \geq 0$ para algunos $m, n \in \mathbb{N}$. De esta manera tenemos que $m \leq m+n = \text{grad}f(x) + \text{grad}g(x)$. Por otro lado, por el lema 12, sabemos que $\text{grad}(f(x)g(x)) = \text{grad}f(x) + \text{grad}g(x)$.

Por lo tanto, $m = \text{grad}f(x) \leq m+n = \text{grad}f(x)+\text{grad}g(x) = \text{grad}(f(x)g(x))$ y así, $\text{grad}f(x) \leq \text{grad}(f(x)g(x))$.

□

Lema 13. $F[x]$ es un dominio entero.

Demostración. Sean $f(x), g(x) \in F[x]$ tales que $f(x) \neq 0$ y $g(x) \neq 0$, entonces, $f(x) = \sum_{i=0}^{m} a_i x^i$ y $g(x) = \sum_{j=0}^{n} b_j x^j$ para algunos $m, n \in \mathbb{N}$ con $a_m \neq 0$ y $b_n \neq 0$, así, $a_m b_n \neq 0$, por lo que $f(x)g(x) = h(x) \neq 0$.

Por lo tanto, si $f(x) \neq 0$ y $g(x) \neq 0$, entonces, $f(x)g(x) \neq 0$ y $F[x]$ es un dominio entero.

□

Teorema 23. (Algoritmo de la división). Sean $f(x), g(x) \in F[x]$ tal que $g(x) \neq 0$, entonces, existen $q(x), r(x) \in F[x]$ tales que $f(x) = q(x)g(x)+r(x)$ y $r(x) = 0$ o $\text{grad}r(x) < \text{grad}g(x)$.

Demostración. Sean $f(x) = \sum_{i=0}^{m} a_i x^i$ y $g(x) = \sum_{j=0}^{n} b_j x^j$ con $\text{grad} f(x) = m$ y $\text{grad} g(x) = n$. Si $m < n$, entonces, tomamos $q(x) = 0$ y $r(x) = f(x)$ de manera que $f(x) = 0g(x) + f(x)$ y el teorema se cumple.

Supongamos que $m \geq n$ y sea $r_1(x) = f(x) - (a_m/b_n)x^{m-n}g(x)$. Así, tenemos que $\text{grad} r_1(x) < m$, de manera que:

i) Si $\text{grad} r_1(x) < n$, tomamos $q(x) = (a_m/b_n)x^{m-n}$, $r(x) = r_1(x)$ y el teorema se cumple.

ii) Si $\text{grad} r_1(x) \not< n$, entonces, $r_1(x) = \sum_{i=0}^{k_1} r_{1_i} x^i$ con $k_1 < m$ y repetimos el procedimiento hasta que $\text{grad} r_h(x) < n$ o $r_h(x) = 0$, y obtenemos los siguientes polinomos:

$r_2(x) = r_1(x) - (r_{k_1}/b_n)x^{k_1-n}g(x)$; $r_2(x) = \sum_{i=0}^{k_2} r_{2_i} x^i$ con $k_2 < k_1$.

$r_3(x) = r_2(x) - (r_{k_2}/b_n)x^{k_2-n}g(x)$; $r_3(x) = \sum_{i=0}^{k_3} r_{3_i} x^i$ con $k_3 < k_2$.

$\vdots$

$r_h(x) = r_{h-1}(x) - (r_{k_{h-1}}/b_n)x^{k_{h-1}-n}g(x)$; $r_h(x) = \sum_{i=0}^{k_h} r_{k_i} x^i$ con $k_h < k_{h-1}$.

Por lo tanto, tenemos que:

$$\begin{array}{rcccl}
f(x) & = & r_1(x) + (a_m/b_n)x^{m-n}g(x) & = & r_1(x) + q_1(x)g(x), \\
r_1(x) & = & r_2(x) + (r_{k_1}/b_n)x^{k_1-n}g(x) & = & r_2(x) + q_2(x)g(x), \\
r_2(x) & = & r_3(x) + (r_{k_2}/b_n)x^{k_2-n}g(x) & = & r_3(x) + q_3(x)g(x), \\
 & & \vdots, & & \\
r_{h-1}(x) & = & r_h(x) + (r_{k_{h-1}}/b_n)x^{k_1-n}g(x) & = & r_h(x) + q_h(x)g(x).
\end{array}$$

y de esta manera:

$$\begin{array}{rcl}
f(x) & = & r_1(x) + q_1(x)g(x) \\
 & = & r_2(x) + q_2(x)g(x) + q_1(x)g(x) \\
 & = & r_3(x) + q_3(x)g(x) + q_2(x)g(x) + q_1(x)g(x) \\
 & \vdots & \\
 & = & r_h(x) + q_h(x)g(x) + q_{h-1}(x)g(x) + \cdots + q_1(x)g(x) \\
 & = & r_h(x) + [q_h(x) + q_{h-1}(x) + \cdots + q_1(x)]g(x).
\end{array}$$

Sea $q(x) = q_1(x) + q_2(x) + \cdots + q_h(x)$, entonces, $f(x) = q(x)g(x) + r_h(x)$ con $\text{grad}r_h(x) < \text{grad}g(x)$ o $r_h(x) = 0$.

□

Teorema 24. $F[x]$ es un anillo euclidiano.

Demostración. Por el lema 13, $F[x]$ es un dominio entero.

Definimos $\forall\ f(x) \in F[x], f(x) \neq 0$ la función $d(f(x)) = \text{grad}f(x)$. Por la definición 53, $\text{grad}f(x) : F[x] \setminus \{0\} \to \mathbb{Z}^+$; por el corolario 9 del lema 12, $\text{grad}f(x) \leq \text{grad}(f(x)g(x))$ y por el teorema 23, $\forall\ f(x), g(x) \neq 0$ existen $q(x), r(x)$ tales que $f(x) = q(x)g(x) + r(x)$ y $\text{grad}r(x) < \text{grad}g(x)$ o $r(x) = 0$.

Por lo tanto, $F[x]$ es un anillo euclidiano.

□

Proposición 34. Sea $u(x) \in F[x]$, $u(x) \neq 0$, entonces, $u(x)$ es unidad si y sólo si $u(x)$ es una constante.

Demostración. Supongamos que $u(x)$ es unidad, esto es, $\exists\ u'(x) \in F[x]$ tal que $u(x)u'(x) = 1$ por lo que $\text{grad}[u(x)u'(x)] = \text{grad}(1) = 0$. Por el lema 12, $\text{grad}u(x) + \text{grad}u'(x) = 0$ y como $\text{grad}f(x) \geq 0\ \forall\ f(x) \in F[x]$, entonces, $\text{grad}u(x) = \text{grad}u'(x) = 0$. Así, $u(x)$ es una constante.

Ahora, supongamos que $u(x) \neq 0$ es una constante, esto es, $\text{grad}u(x) = 0$ por lo que $u(x) = \alpha$ para algún $\alpha \in F$. Como F es un campo, $\exists\ \alpha' \in F$ tal que $\alpha\alpha' = 1$. Sea $u'(x) = \alpha'$, entonces, $u(x)u'(x) = \alpha\alpha' = 1$, por lo tanto, $u(x)$ es unidad.

□

Definición 55. Decimos que $p(x) \in F[x]$, $p(x) \neq 0$, es un polinomio *irreducible* sobre el campo F si siempre que $p(x) = a(x)b(x)$, $(a(x), b(x) \neq 0$ por ser $F[x]$ un dominio entero), entonces, $\text{grad}a(x) = 0$ o $\text{grad}b(x) = 0$, es decir, $a(x)$ o $b(x)$ es una unidad.

Observación: Los polinomios irreducibles son los elementos primos en $F[x]$ de acuerdo a la definición 27 y a la proposición 34.

5.3. Extensión de campos, raíces de polinomios, teorema del residuo y multiplicidad de raíces

Definición 56. Sea F un campo, decimos que el campo K es una *extensión* de F si $F \subset K$, es decir, si F es subcampo de K.

Observación: Si K es una extensión de F, entonces, K es un espacio vectorial sobre F con las operaciones de K ya que, por hipótesis, K es un campo, por lo que $(K, +)$ es un grupo abeliano y como $F \subset K$, entonces, $\forall\, f \in F$ y $\forall\, k \in K$, $fk \in K$ y así, K es un espacio vectorial sobre el campo F.

Definición 57. El *grado* de K sobre F es la dimensión de K como espacio vectorial sobre F y lo denotamos como $[K : F]$.

Nota: Si K es de dimensión finita, entonces, decimos que K es una *extensión finita* de F.

Teorema 25. Si L es una extensión finita de K y K es una extensión finita de F, entonces, L es una extensión finita de F y $[L : F] = [L : K][K : F]$.

Demostración. Como $F \subset K$ y $K \subset L$, entonces, $F \subset L$ y L es una extensión de F.

Como las extensiones de L sobre K y de K sobre F son finitas, entonces, $[L : K] = m$ y $[K : F] = n$ para algunos $m, n \in \mathbb{N}$. Sean $\{v_1, \ldots, v_m\}$ una base de L sobre K y $\{w_1, \ldots, w_n\}$ una base de K sobre F. Formamos el conjunto $\Gamma = \{v_i w_j \mid i \in \{1, \ldots, m\}; j \in \{1, \ldots, n\}\}$ de manera que $|\Gamma| = mn$.

Sea $l \in L$, entonces, $l = \alpha_1 v_1 + \cdots + \alpha_m v_m$, con $\alpha_1, \ldots, \alpha_m \in K$; además, $\forall\, i \in \{1, \ldots, m\}$, $\alpha_i = \beta_{i1} w_1 + \cdots + \beta_{in} w_n$, con $\beta_{i1}, \ldots, \beta_{in} \in F$. Sustituyendo las α_i en l tenemos que $l = (\beta_{11} w_1 + \cdots + \beta_{1n} w_n) v_1 + \cdots + (\beta_{m1} w_1 + \cdots + \beta_{mn} w_n) v_m$ y, entonces, $l = \beta_{11} v_1 w_1 + \cdots + \beta_{1n} v_1 w_n + \cdots + \beta_{m1} v_m w_1 + \cdots + \beta_{mn} v_m w_n$ por lo que $\forall\, l \in L$, l es combinación lineal de los elementos de Γ con coeficientes en F.

Por último, tenemos que demostrar que Γ es linealmente independiente. Supongamos que $\beta_{11}v_1w_1+\cdots+\beta_{1n}v_1w_n+\cdots+\beta_{m1}v_mw_1+\cdots+\beta_{mn}v_mw_n=0$, entonces, $(\beta_{11}w_1+\cdots+\beta_{1n}w_n)v_1+\cdots+(\beta_{m1}w_1+\cdots+\beta_{mn}w_n)v_m=0$, esto es, $\alpha_1v_1+\cdots+\alpha_mv_m=0$ y como $\{v_1,\ldots,v_m\}$ es una base de L sobre K, entonces, $\alpha_1=\cdots=\alpha_m=0$. Por lo tanto, $\beta_{i1}w_1+\cdots+\beta_{in}w_n=0$ $\forall\ i\in\{1,\ldots,m\}$ y como $\{w_1,\ldots,w_n\}$ es una base de K sobre F, entonces, $\beta_{ij}=0\ \forall\ i\in\{1,\ldots,m\}$ y $\forall\ j\in\{1,\ldots,n\}$.

De esta manera, Γ es base de L y como $|\Gamma|=mn$, entonces, L es una extensión finita de F y $[L:F]=mn=[L:K][K:F]$.

□

Corolario 10. Sea L una extensión finita de F y sea K un subcampo de L tal que $F\subset K$, entonces, $[K:F]|[L:F]$.

Demostración. Como K es un subcampo de L y $F\subset K$, tenemos que K es una extensión de F y como $[L:F]$ es finita, entonces, $[K:F]$ es finita. Por otro lado, L es de dimensión finita sobre F y $F\subset K$, entonces, $[L:K]$ es finito. De esta manera tenemos que $[L:F]=l$, $[L:K]=m$ y $[K:F]=n$ para algunos $l,m,n\in\mathbb{N}$. Así, por el teorema 25, $l=mn$, por lo tanto, $[L:F]=[L:K][K:F]$ por lo que $[K:F]|[L:F]$.

□

Definición 58. Sean $f(x)=\sum_{i=0}^{\infty}\alpha_ix^i\in F[x]$, K una extensión de F y $a\in K$; definimos la función $\varphi_a:F[x]\longrightarrow K$ como $\varphi_a:\sum_{i=0}^{\infty}\alpha_ix^i\longrightarrow\sum_{i=0}^{\infty}\alpha_ia^i$ y la denotamos como $\varphi_a(f(x))=\sum_{i=0}^{\infty}\alpha_ia^i=f(a)$.

Lema 14. φ_a es un homomorfismo de anillos.

Demostración. Sean $a\in K$ y $f(x),g(x)\in F[x]$ tales que $f(x)=\sum_{i=0}^{\infty}\alpha_ix^i$ y $g(x)=\sum_{j=0}^{\infty}\beta_jx^j$, entonces:

$$\begin{aligned}
\varphi_a(f(x)+g(x)) &= \varphi_a(\sum_{i=0}^{\infty}\alpha_i x^i + \sum_{j=0}^{\infty}\beta_j x^j) \\
&= \varphi_a(\sum_{i=0}^{\infty}(\alpha_i+\beta_i)x^i) \\
&= \sum_{i=0}^{\infty}(\alpha_i+\beta_i)a^i \\
&= \sum_{i=0}^{\infty}\alpha_i a^i + \sum_{j=0}^{\infty}\beta_j a^j \\
&= \varphi_a(f(x)) + \varphi_a(g(x)).
\end{aligned}$$

De la misma manera, tenemos que:

$$\begin{aligned}
\varphi_a(f(x)g(x)) &= \varphi_a((\sum_{i=0}^{\infty}\alpha_i x^i)(\sum_{j=0}^{\infty}\beta_j x^j)) \\
&= \varphi_a(\sum_{k=0}^{\infty}(\sum_{h=0}^{k}a_h b_{k-h})x^k) \\
&= \sum_{k=0}^{\infty}(\sum_{h=0}^{k}a_h b_{k-h})a^k \\
&= (\sum_{i=0}^{\infty}\alpha_i a^i)(\sum_{j=0}^{\infty}\beta_j a^j) \\
&= \varphi_a(f(x))\varphi_a(g(x)).
\end{aligned}$$

Por lo tanto, φ_a es un homomorfismo de anillos. A φ_a le llamamos el *homomorfismo evaluación en a*.

□

Definición 59. Sean K una extensión de F, φ_a el homomorfismo evaluación en a y $f(x) \in F[x]$. Si $\varphi_a(f(x)) = 0$, decimos que a es *raíz* de $f(x)$.

Definición 60. Sean K una extensión de F y $a \in K$, decimos que a es *algebraico sobre* F si existen elementos $\alpha_0, \alpha_1, \ldots, \alpha_n \in F$, con al menos una $\alpha_i \neq 0$ para $i \in \{0, 1, \ldots, n\}$ tales que $\alpha_0 a^0 + \alpha_1 a^1 + \cdots + \alpha_n a^n = 0$.

Esto es, decimos que $a \in K$ es algebraico sobre F si existe $f(x) \in F[x]$, $f(x) \neq 0$ tal que $f(a) = 0$, es decir, existe $f(x) \in F[x]$, $f(x) \neq 0$ para el que a es raíz.

Definición 61. Sea K una extensión de F, decimos que K es una *extensión algebraica* de F si $\forall\ a \in K$, a es algebraico sobre F.

Proposición 35. Si K es una extensión finita de F, entonces, K es una extensión algebraica de F.

Demostración. Como K es extensión finita de F, $[K : F] = m$ para algún $m \in \mathbb{N}$, esto es, K es un espacio vectorial sobre F de dimensión m, entonces, un conjunto de n vectores con $m < n$ es linealmente dependiente, por lo que $\forall\ a \in K$, existen $\alpha_0, \ldots, \alpha_n \in F$ tales que $\sum_{i=0}^{n} \alpha_i a^i = 0$ con al menos un $\alpha_i \neq 0$. Por lo tanto, $\forall\ a \in K\ \exists\ f(x) \in F[x]$, $f(x) \neq 0$ tal que $f(a) = 0$ y así, K es algebraico sobre F.

□

Definición 62. Sean K una extensión de F y $a \in K$, $F(a)$ es el *mínimo subcampo* de K tal que $F \subset F(a)$ y $a \in F(a)$. A este campo le llamamos el subcampo obtenido por la *adjunción* de a a F.

Observación 5. $F(a) = \{f(a)/g(a) \mid f(x), g(x) \in F[x] \text{ y } g(a) \neq 0\}$.

Demostración. Sea $M = \{f(a)/g(a) \mid f(x), g(x) \in F[x] \text{ y } g(a) \neq 0\}$, es fácil ver que M es un campo. Sea $g(x) = 1$, entonces, $\forall\ f(x) = \alpha$ con $\alpha \in F$ tenemos que $f(a)/g(a) = \alpha/1 = \alpha$ de manera que $F \subset M$; ahora, tomamos a $f(x) = x$, entonces, $f(a)/g(a) = a/1 = a$ y así, $a \in M$, de manera que $F(a) \subset M$.

Por otro lado, sea $f(x) \in F[x]$, esto es, $f(x) = \sum_{i=0}^{n} \alpha_i x^i$ y $f(a) = \sum_{i=0}^{n} \alpha_i a^i$. Como $F(a)$ es campo y $\alpha_i, a^i \in F(a)\ \forall\ i \in \{0, \ldots, n\}$, tenemos que $f(a) \in F(a)$ $\forall\ f(x) \in F[x]$. Sea $g(x) \in F[x]$ tal que $g(a) \neq 0$, sabemos que $g(a) \in F(a)$ y como $F(a)$ es campo, entonces, $g(a)^{-1} \in F(a)$ así, $f(a)/g(a) \in F(a)$ y $M \subset F(a)$.

De esta manera, $F(a) \subset M \subset F(a)$, por lo tanto:

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

□

Definición 63. Sea K una extensión de F, decimos que K es una *extensión simple* de F si existe $\alpha \in K$ tal que $K = F(\alpha)$.

Teorema 26. Sean K una extensión de F y $a \in K$, entonces, a es algebraico sobre F si y sólo si $F(a)$ es una extensión finita de F.

Demostración. Supongamos que $F(a)$ es una extensión finita de F, entonces, $[F(a) : F] = m$ para algún $m \in \mathbb{N}$. Sea $\beta = \{a^0 = 1, a, \ldots, a^m\} \in F(a)$ de manera que $|\beta| = m+1$, entonces, existen $\alpha_0, \alpha_1, \ldots, \alpha_m \in F$ no todos 0 tales que $\alpha_0 1 + \alpha_1 a + \cdots + \alpha_m a^m = 0$, de esta manera, a satisface al polinomio $f(x) = \alpha_0 + \alpha_1 x + \cdots + \alpha_m x^m$, por lo tanto, a es algebraico sobre F.

Ahora, supongamos que $a \in K$ es algebraico sobre F, entonces, $\exists\ f(x) \in F[x]$ de grado mínimo tal que $f(x) \neq 0$ y $f(a) = 0$. Sin pérdida de generalidad, supongamos que $\text{grad} f(x) = n$ con $n \in \mathbb{N}$, así, $f(x) = \alpha_0 x^0 + \cdots + \alpha_n x^n$ con $\alpha_0, \ldots, \alpha_n \in F$, no todos cero y $\alpha_n \neq 0$ tales que $\alpha_0 a^0 + \cdots + \alpha_n a^n = 0$. Sea $g(x) = (\alpha_0/\alpha_n)x^0 + \cdots + (\alpha_n/\alpha_n)x^n = \beta_0 x^0 + \cdots + \beta_n x^n$ con $\beta_i = \alpha_i/\alpha_n$ $\forall\ i \in \{0, \ldots, n\}$; de esta manera, $\beta_n = 1$ y $g(x) = \beta_0 x^0 + \cdots + x^n$, esto es, $g(x)$ es mónico. Sustituimos x por a y tenemos que $g(a) = \beta_0 a^0 + \cdots + a^n = 0$.

Así, $a^n = -\beta_0 a^0 - \cdots - \beta_{n-1} a^{n-1}$, multiplicamos por a y tenemos que $a^{n+1} = -\beta_0 a - \cdots - \beta_{n-1} a^n = -\beta_0 a - \cdots - \beta_{n-1}(-\beta_0 a^0 - \cdots - \beta_{n-1} a^{n-1})$. Siguiendo este mismo procedimiento vemos que a^{n+k}, con $k \geq 0$ se puede escribir como combinación lineal de los elementos $1, a, \ldots, a^{n-1}$ sobre el campo F. Sea $\Gamma = \{1, a, \ldots, a^{n-1}\} \in F(a)$, por lo anterior, sabemos que Γ genera a $F(a)$. Por último, supongamos que existen $\gamma_0, \ldots, \gamma_{n-1}$ tales que $\gamma_0 a^0 + \cdots + \gamma_{n-1} a^{n-1} = 0$, entonces, $\gamma_i = 0\ \forall\ i \in \{0, \ldots, n-1\}$, de no ser así, $f(x)$ no es de grado mínimo lo cual contradice nuestra hipótesis. Por lo tanto, Γ es linealmente independiente.

Γ genera a $F(a)$ sobre F y es linealmente independiente, entonces, Γ es base de $F(a)$ y como $|\Gamma| = n$, entonces, $F(a)$ es de dimensión finita sobre F, a saber, $[F(a) : F] = n$ y así, $F(a)$ es una extensión finita de F.

□

Definición 64. Sean K una extensión de F y $a \in K$, decimos que a es *algebraico de grado n* sobre F si a es raíz de algún polinomio $f(x) \in F[x]$, $f(x) \neq 0$, $\text{grad} f(x) = n$ y a no es raíz de ningún otro polinomio $g(x) \in F[x]$

tal que grad$g(x) <$ grad$f(x)$, entonces, como corolario del teorema anterior, tenemos:

Corolario 11. Sean K una extensión de F y $a \in K$ tal que a es algebraico de grado n sobre F, entonces, $[F(a) : F] = n$.

Demostración. Sea $a \in K$ algebraico de grado n sobre F, entonces, por la definición 64, $\exists\ f(x) \in F[x]$ tal que $f(x) \neq 0$, grad$f(x) = n$, $f(a) = 0$ y a no es raíz de ningún otro polinomio $g(x) \in F[x]$ con grad$g(x) <$ grad$f(x)$, esto es, $f(x)$ es de grado mínimo tal que $f(a) = 0$. Así, se cumplen las hipótesis del teorema anterior de lo que se sigue que $[F(a) : F] = n$.

□

Teorema 27. Sean K una extensión de F y $a, b \in K$ tales que a y b son algebraicos sobre F, entonces, $a \pm b, ab$ y a/b (si $b \neq 0$) son algebraicos sobre F

Demostración. Sean $a, b \in K$ algebraicos sobre F, entonces, por el teorema 26, $F(a)$ y $F(b)$ son extensiones finitas sobre F por lo que podemos suponer, sin pérdida de generalidad, que $[F(a) : F] = m$ y $[F(b) : F] = n$ para algunos $m, n \in \mathbb{N}$.

Sean $F(a) = T$ y $W = T(b)$ el mínimo subcampo de K tal que $T \subset W$ y $b \in W$ como en la definición 62. Como b es algebraico de grado n sobre F, $F \subset T \subset W$ y $b \in W$, entonces, b es algebraico de, cuando más, grado n sobre T, esto es, $[W : T] \leq n$. Por el teorema 25, $[W : T][T : F] = [W : F]$, entonces, $[W : F] \leq nm$ y W es una extensión finita de F.

Como $a, b \in W$, entonces, $a \pm b, ab, a/b \in W$ y como $[W : F]$ es finito, por el teorema 26, $a \pm b, ab$ y a/b son algebraicos sobre F.

□

Observación: Por la construcción de W, los elementos que son algebraicos sobre F forman un subcampo de la extensión K.

Corolario 12. Si $a, b \in K$ son algebraicos sobre F de grados m y n respectivamente, entonces, $a \pm b, ab$ y a/b (si $b \neq 0$) son algebraicos sobre F de, cuando más, grado mn.

Demostración. Por el teorema 27, $a \pm b, ab, a/b \in W$ y $[W : F] \leq mn$, entonces, $a \pm b, ab$ y a/b son raíces de un polinomio a lo más de grado mn.

□

Teorema 28. Sean L una extensión algebraica de K y K una extensión algebraica de F, entonces, L es una extensión algebraica de F.

Demostración. Sean $l \in L$ y L una extensión algebraica de K, entonces, l satisface a algún polinomio $\gamma_0 x^0 + \cdots + \gamma_n x^n \in K[x]$ para algún $n \in \mathbb{N}$ y $\gamma_0, \ldots, \gamma_n \in K$ no todos cero. Como K es algebraico sobre F, formamos las extensiones finitas como en el teorema 27 y tenemos: $M_0 = F(\gamma_0)$, $M_1 = M_0(\gamma_1), \ldots, M_n = M_{n-1}(\gamma_n)$ de manera que l es algebraico sobre M_n. Por último, formamos la extensión finita $M_n(l)$ de M_n.

Por el teorema 25, $[M_n(l) : M_n][M_n : F] = [M_n(l) : F]$ por lo que $M_n(l)$ es una extensión finita de F y así, l es algebraico sobre F. Como l es arbitrario, entonces, L es una extensión algebraica de F.

□

Teorema 29. (Teorema del residuo). Sean $f(x) \in F[x]$ y K una extensión de F, entonces, $\forall\ a \in K$, $f(x) = (x - a)g(x) + f(a)$ con $g(x) \in K[x]$ y si $\text{grad} f(x) \geq 1$, entonces, $\text{grad} g(x) = \text{grad} f(x) - 1$.

Demostración. Como $F \subset K$, entonces, $F[x] \subset K[x]$ y así, $f(x) \in K[x]$. Por otro lado, $a, x \in K[x]$, a saber, $a = ax^0$ y $x = 1x$ por lo que $x - a \in K[x]$ y $\text{grad}(x - a) = 1$.

Por el algoritmo de la división (teorema 23), existen $g(x), r(x) \in K[x]$ únicos tales que $f(x) = (x-a)g(x)+r(x)$ con $r(x) = 0$ o $\text{grad} r(x) < \text{grad}(x - a) = 1$, esto es, $\text{grad} r(x) = 0$, por lo tanto, $r(x) = r \in K$ y $f(x) = (x - a)g(x) + r$. Evaluamos $f(x)$ en a y tenemos: $f(a) = (a - a)g(a) + r = (0)g(a) + r = r$; por lo que $r = f(a)$, de esta manera, $f(x) = (x - a)g(x) + f(a)$ con $f(a) = r = r(x) \in K[x]$.

Por último, supongamos que $\text{grad} f(x) \geq 1$, por los lemas 11 y 12 (grados de un polinomio), tenemos que:

i) Si $f(a) = 0$, entonces, $f(x) = (x - a)g(x)$ y tenemos:

$$\begin{aligned} \text{grad}f(x) &= \text{grad}[(x-a)g(x)] \\ &= \text{grad}(x-a) + \text{grad}g(x) \\ &= 1 + \text{grad}g(x). \end{aligned}$$

Así, $\text{grad}g(x) = \text{grad}f(x) - 1$.

ii) Si $f(a) \neq 0$ y $\text{grad}f(a) = 0$, entonces:

- $f(x) = (x-a)g(x) + f(a)$ y tenemos:

$$\begin{aligned} \text{grad}f(x) &= \text{grad}[(x-a)g(x) + f(a)] \\ &\leq \text{máx}\{\text{grad}[(x-a)g(x)], \text{grad}f(a)\} \\ &= \text{máx}\{\text{grad}[(x-a)g(x)], 0\} \\ &= \text{grad}[(x-a)g(x)] \\ &= \text{grad}(x-a) + \text{grad}g(x) \\ &= 1 + \text{grad}g(x). \end{aligned}$$

- $f(x) - f(a) = (x-a)g(x)$ y tenemos:

$$\begin{aligned} \text{grad}[f(x) - f(a)] &= \text{grad}[(x-a)g(x)] \\ &= \text{grad}(x-a) + \text{grad}g(x) \\ &= 1 + \text{grad}g(x) \\ 1 + \text{grad}g(x) &= \text{grad}[f(x) - f(a)] \\ &\leq \text{máx}\{\text{grad}f(x), \text{grad}f(a)\} \\ &= \text{máx}\{\text{grad}f(x), 0\} \\ &= \text{grad}f(x). \end{aligned}$$

Así, $\text{grad}f(x) \leq \text{grad}g(x) + 1 \leq \text{grad}f(x)$ y $\text{grad}g(x) = \text{grad}f(x) - 1$.

Por *i)* y *ii)*, $\text{grad}g(x) = \text{grad}f(x) - 1$.

Por lo tanto, $f(x) = (x-a)g(x) + f(a)$ con $\text{grad}g(x) = \text{grad}f(x) - 1$ y $g(x) \in K[x]$.

□

Corolario 13. Sean $f(x) \in F[x]$ y K una extensión de F. Si $a \in K$ es raíz de $f(x)$, entonces, $(x-a)|f(x)$ en $K[x]$.

Demostración. Por el teorema 29, $f(x) = (x-a)g(x) + f(a)$ y como a es raíz de $f(x)$, entonces, $f(a) = 0$. Por lo tanto, $f(x) = (x-a)g(x) + 0 = (x-a)g(x)$ y así, $(x-a)|f(x)$.

□

Definición 65. Sean $f(x) \in F[x]$, K una extensión de F y $a \in K$ una raíz de $f(x)$. Decimos que la raíz a es de *multiplicidad* m si $(x-a)^m | f(x)$ y $(x-a)^{m+1} \nmid f(x)$.

Lema 15. Sean $f(x) \in F[x]$ un polinomio de grado $n \geq 1$ y K una extensión de F, entonces, $f(x)$ tiene, a lo más, n raíces en K.

Demostración. La haremos por inducción sobre $\text{grad} f(x) = n$. Supongamos que $\text{grad} f(x) = 1$, de esta manera, $f(x) = \alpha x + \beta$, con $\alpha, \beta \in F$ y $\alpha \neq 0$. Sea $a \in K$ raíz de $f(x)$, entonces, $f(a) = \alpha a + \beta = 0$, por lo que $a = -\beta/\alpha$. Así, $f(x)$ tiene únicamente una raíz en K por lo que el lema se cumple para $n = 1$.

Suponemos la hipótesis verdadera para los polinomios de grado menor a n. Sea $\text{grad} f(x) = n$. Si $f(x)$ no tiene raíces en la extensión K, el lema se cumple; por otro lado, supongamos que sí las tiene. Sea $a \in K$ raíz de $f(x)$ de multiplicidad $m \geq 1$, esto es, $(x-a)^m | f(x)$ y $(x-a)^{m+1} \nmid f(x)$. Por el corolario 13 del teorema 29 (teorema del residuo), $f(x) = (x-a)^m g(x)$, con $g(x) \in K[x]$ y $\text{grad} g(x) = n - \text{grad}(x-a)^m$.

Observación: $(x-a)^m = \underbrace{(x-a)\cdots(x-a)}_{m \text{ veces}}$, por lo tanto:

$$\begin{aligned} \text{grad}(x-a)^m &= \text{grad}[\underbrace{(x-a)\cdots(x-a)}_{m \text{ veces}}] \\ &= \underbrace{\text{grad}(x-a) + \cdots + \text{grad}(x-a)}_{m \text{ veces}} \\ &= \underbrace{1 + \cdots + 1}_{m \text{ veces}} \\ &= m. \end{aligned}$$

De manera que $\text{grad} g(x) = n - m < n$ y como $0 \leq \text{grad} g(x) = n - m$, entonces, $m \leq n$. Ahora, como $(x-a)^{m+1} \nmid f(x)$, entonces, $(x-a)^m (x-a) \nmid (x-a)^m g(x)$, esto es, $(x-a) \nmid g(x)$ y, por el corolario 13, a no es raíz de $g(x)$.

Por último, si $f(x)$ no tiene más raíces, entonces, su única raíz es de multiplicidad m y el lema se cumple; por otro lado, supongamos que sí las tiene. Sea $b \in K$, $b \neq a$, una raíz de $f(x)$. De esta manera, tenemos que $f(b) = (b-a)^m g(b) = 0$ y como $b - a \neq 0$, entonces, $g(b) = 0$; por lo tanto, b

es raíz de $g(x)$. Como grad$g(x) = n - m < n$, para $g(x)$ es válida la hipótesis de inducción, por lo que $g(x)$ tiene, a lo más, $n - m$ raíces. De esta manera, $f(x)$ tiene, a lo más, $m + (n - m) = n$ raíces en K lo que completa la demostración por inducción.

Por lo tanto, un polinomio $f(x)$ de grado n tiene, a lo más, n raíces en una extensión K.

□

Teorema 30. Sea $p(x) \in F[x]$ irreducible de grad$p(x) = n \geq 1$, entonces, existe una extensión finita E de F en donde $p(x)$ tiene una raíz y $[E : F] = n$.

Demostración. Sea $P = \langle p(x) \rangle$. Por la proposición 22, como $p(x)$ es irreducible, P es ideal máximo de $F[x]$, por lo que, por el teorema 22, $F[x]/P$ es campo.

Sean $E = F[x]/P$, $\varphi : F[x] \to E$ dada por $\varphi(f(x)) = P + f(x)$ la proyección canónica y $K = \{P + \alpha \mid \alpha \in F\} = \varphi(F) \subset E$. Veamos que $\varphi|_F : F[x] \to E$ es un isomorfismo:

> *i)* Sean $\alpha, \beta \in F$ tales que $\varphi(\alpha) = \varphi(\beta)$, esto es, $P + \alpha = P + \beta$, por lo que $P + (\alpha - \beta) = P$, de manera que, $\alpha - \beta \in P$. Como $P = \langle p(x) \rangle$, entonces, $\alpha - \beta = p(x)q(x)$ para algún $q(x) \in F[x]$. Como grad$p(x) = n \geq 1$, forzosamente $q(x) = 0$ y $\alpha - \beta = 0$, así, $\alpha = \beta$. Por lo tanto, $\varphi|_F$ es inyectiva sobre K.
>
> *ii)* Sea $\alpha' \in K$, entonces, $\alpha' = P + \alpha$ para algún $\alpha \in F$, de esta manera, $\varphi(\alpha) = \alpha'$ y $\varphi|_F$ es suprayectiva sobre K.
>
> Por *i)* y *ii)*, el campo F es isomorfo a $K \subset E$, esto es, identificamos a F con K y podemos ver a E como una extensión de F.

Ahora, aplicamos φ al polinomio $f(x) = x$, así, $\varphi(x) = P + x$ y lo denotamos por a, esto es, $\varphi(x) = P + x = a$. Afirmamos que $\Gamma = \{a^0, a, \ldots, a^{n-1}\} = \{P + 1, P + x, (P + x)^2 = P + x^2, \ldots, (P + x)^{n-1} = P + x^{n-1}\}$ es una base de E sobre F. Por el teorema 23 (algoritmo de la división), $\forall\ f(x) \in F[x]$, $f(x) = p(x)q(x) + r(x)$ con $q(x), r(x) \in F[x]$ y $r(x) = 0$ o grad$r(x) < n$ por lo que tenemos:

$$\begin{aligned} E &= F[x]/P \\ &= \{P + f(x) \mid f(x) \in F[x]\} \\ &= \{P + p(x)q(x) + r(x) \mid q(x), r(x) \in F[x] \\ &\quad \text{y } r(x) = 0 \text{ o } \text{grad}r(x) < n\} \\ &= \{P + r(x) \mid r(x) \in F[x] \text{ y } r(x) = 0 \text{ o } \text{grad}r(x) < n\}. \end{aligned}$$

Sea $\alpha \in E$, entonces, $\alpha = P + s(x)$ con $s(x) \in F[x]$ y $\text{grad}s(x) < n$, esto es, $\alpha = P + \alpha_0 + \alpha_1 x + \cdots + \alpha_{n-1}x^{n-1}$ para algunos $\alpha_0, \ldots, \alpha_{n-1} \in F$ y así:

$$\begin{aligned} \alpha &= P + \alpha_0 + \alpha_1 x + \cdots + \alpha_{n-1}x^{n-1} \\ &= (P + \alpha_0) + (P + \alpha_1 x) + \cdots + (P + \alpha_{n-1}x^{n-1}) \\ &= (\alpha_0 P + \alpha_0) + (\alpha_1 P + \alpha_1 x) + \cdots + (\alpha_{n-1}P + \alpha_{n-1}x^{n-1}) \\ &= \alpha_0(P + 1) + \alpha_1(P + x) + \cdots + \alpha_{n-1}(P + x^{n-1}) \\ &= \alpha_0 a^0 + \alpha_1 a + \cdots + \alpha_{n-1}a^{n-1}. \end{aligned}$$

Por lo tanto, Γ genera a E.

Sea $\beta \in E$, como $\langle \Gamma \rangle = E$, entonces, $\beta = \sum_{i=0}^{n-1} \alpha_i a^i$. Supongamos $\beta = 0_E = P$, como $a = P + x$, tenemos que $P = \sum_{i=0}^{n-1} \alpha_i a^i = \sum_{i=0}^{n-1} \alpha_i (P + x)^i = P + \sum_{i=0}^{n-1} \alpha_i x^i$, por lo que $\sum_{i=0}^{n-1} \alpha_i x^i = g(x) \in P$. Como $g(x) \in P$, entonces, $\exists\ q(x) \in F[x]$ tal que $g(x) = p(x)q(x)$. Como $\text{grad}p(x) = n$ y $\text{grad}g(x) \leq n - 1$ o $g(x) = 0$, entonces, $q(x) = 0$ y $g(x) = 0$. Por lo tanto, $g(x) = \sum_{i=0}^{n-1} \alpha_i a^i = 0$, por lo que $\alpha_i = 0\ \forall\ i \in \{0, \ldots, n-1\}$ y Γ es linealmente independiente.

Por último, sea $f(x) \in F[x]$, entonces, $f(x) = \alpha_0 + \alpha_1 x + \cdots + \alpha_k x^k$ con $\alpha_0, \ldots, \alpha_k \in F$ y $k \in \mathbb{N}$. Como $a = P + x$, tenemos que $\forall\ f(x) \in F[x]$ se cumple:

$$\begin{aligned} f(a) &= f(P + x) \\ &= \alpha_0 + \alpha_1(P + x) + \cdots + \alpha_k(P + x)^k \\ &= \alpha_0 + \alpha_1 P + \alpha_1 x + \cdots + \alpha_k P + \alpha_k x^k \\ &= \alpha_0 + P + \alpha_1 x + \cdots + P + \alpha_k x^k \\ &= P + \alpha_0 + \alpha_1 x + \cdots + \alpha_k x^k \\ &= P + f(x) \\ &= \varphi(f(x)). \end{aligned}$$

En particular, $\varphi(p(x)) = p(a)$; por otro lado, $\varphi(p(x)) = P + p(x) = P = 0_E$ ya que $p(x) \in P$, así, $p(a) = 0_E$, por lo tanto, $\varphi(x) = P + x = a \in E$ es raíz de $p(x)$.

□

Corolario 14. Sea $f(x) \in F[x]$, entonces, existe una extensión finita E de F en donde $f(x)$ tiene una raíz y $[E : F] \leq \text{grad} f(x)$.

Demostración. Sea $p(x) \in F[x]$ un factor irreducible de $f(x)$, de esta manera, $\text{grad} p(x) \leq \text{grad} f(x)$ y cualquier raíz de $p(x)$ es raíz de $f(x)$. Por el teorema 30, existe E extensión de F en donde $p(x)$ tiene una raíz y por lo tanto, $f(x)$ tiene una raíz, además, $[E : F] = \text{grad} p(x) \leq \text{grad} f(x)$.

□

Teorema 31. (Teorema de Kronecker). Sea $f(x) \in F[x]$ tal que $\text{grad} f(x) = n \geq 1$, entonces, existe una extensión finita E de F en donde $f(x)$ tiene n raíces y $[E : F] \leq n!$.

Demostración. La haremos por inducción sobre $\text{grad} f(x) = n$. Supongamos que $\text{grad} f(x) = 1$; por el corolario 14, existe una extensión finita E_1 de F en donde $f(x)$ tiene una raíz y $[E_1 : F] \leq 1 = 1!$; por el lema 15, $f(x)$ tiene a lo más 1 raíz. De esta manera, se cumple la hipótesis para $n = 1$.

Suponemos la hipótesis verdadera para los polinomios de grado menor a n. Sea $f(x) \in F[x]$ tal que $\text{grad} f(x) = n$, entonces, por el corolario 14, existe una extensión finita E_1 de F en donde $f(x)$ tiene una raíz y $[E_1 : F] \leq n$. Sea α la raíz de $f(x)$ en E_1, entonces, $f(x) = (x - \alpha)g(x)$ con $f(x), g(x) \in E_1$ y $\text{grad} g(x) = n - 1$, por lo que para $g(x)$ se cumple la hipótesis de inducción, esto es, existe una extensión E de E_1 en donde $g(x)$ tiene $n - 1$ raíces y $[E : E_1] \leq (n - 1)!$.

Como E y E_1 son extensiones finitas de E_1 y F respectivamente, entonces, $[E : F] = [E : E_1][E_1 : F] \leq (n - 1)!n = n!$ y E es una extensión finita de F en donde $f(x)$ tiene $(n - 1) + 1 = n$ raíces lo que completa la demostración por inducción.

Por lo tanto, si $\text{grad} f(x) = n$, entonces, existe una extensión finita en donde $f(x)$ tiene n raíces y $[E : F] \leq n!$.

□

Nota: Cuando un polinomio $f(x)$ de grado n tiene n raíces en una extensión, decimos que tiene un *juego completo de raíces*.

Definición 66. Sean K una extensión de F y $a \in K$, decimos que a es *separable* sobre F si a es raíz de algún $f(x) \in F[x]$ y no es raíz múltiple.

Definición 67. Sean $f(x) \in F[x]$ y su factorización $f(x) = \alpha p_1(x) \cdots p_h(x)$ en polinomios irreducibles mónicos y $\alpha \in F$, decimos que $f(x)$ es *separable* si para cada p_i toda raíz no es múltiple.

Definición 68. Sea K una extensión de F, decimos que K es una *extensión separable* sobre F si $\forall\ a \in K$, a es separable sobre F.

5.4. Campo de descomposición

Definición 69. Sean $f(x) \in F[x]$, $\text{grad} f(x) = n$ y E una extensión finita de F; decimos que E es un *campo de descomposición* de $f(x)$ sobre F si E es una extensión mínima en donde $f(x)$ tiene n raíces.

Esto es, E es un *campo de descomposición* de $f(x)$ sobre F si E es una extensión mínima en donde $f(x)$ puede ser descompuesto en factores lineales.

Lema 16. Sean F y F' dos campos y $\tau : F \longrightarrow F'$ un isomorfismo; denotamos a $\tau(\alpha)$ como $\alpha' \in F'$ para cualquier $\alpha \in F$. Consideremos $F[x]$ y $F'[t]$, entonces, $\sigma : F[x] \to F'[t]$ definido por $\sigma(f(x)) = \sigma(\alpha_0 + \alpha_1 x + \cdots + \alpha_n x^n) = \tau(\alpha_0) + \tau(\alpha_1)t + \cdots + \tau(\alpha_n)t^n = \alpha'_0 + \alpha'_1 t + \cdots + \alpha'_n t^n$ es un isomorfismo tal que $\sigma|_F = \tau$, esto es, σ *extiende* a τ.

Demostración. Sean $f(x), g(x) \in F[x]$; $f(x) = \alpha_0 + \alpha_1 x + \cdots + \alpha_n x^n$ y $g(x) = \beta_0 + \beta_1 x + \cdots + \beta_m x^m$, sin pérdida de generalidad, suponemos que $m \leq n$, entonces, $g(x) = \beta_0 + \beta_1 x + \cdots + \beta_m x^m + \beta_{m+1} x^{m+1} + \cdots + \beta_n x^n$ con $\beta_{m+1} = \cdots = \beta_n = 0$ y tenemos:

$$\begin{aligned}
\sigma(f(x)+g(x)) &= \sigma(\sum_{i=0}^{n}(\alpha_i+\beta_i)x^i) \\
&= \sigma((\alpha_0+\beta_0)+(\alpha_1+\beta_1)x+\cdots+(\alpha_n+\beta_n)x^n) \\
&= \tau(\alpha_0+\beta_0)+\tau(\alpha_1+\beta_1)t+\cdots+\tau(\alpha_n+\beta_n)t^n \\
&= \tau(\alpha_0)+\tau(\beta_0)+[\tau(\alpha_1)+\tau(\beta_1)]t+\cdots \\
&\quad +[\tau(\alpha_n)+\tau(\beta_n)]t^n \\
&= \tau(\alpha_0)+\tau(\beta_0)+\tau(\alpha_1)t+\tau(\beta_1)t+\cdots \\
&\quad +\tau(\alpha_n)t^n+\tau(\beta_n)t^n \\
&= (\alpha'_0+\alpha'_1t+\cdots+\alpha_nt^n)+(\beta'_0+\beta'_1t+\cdots+\beta_mt^m) \\
&= \sigma(f(x))+\sigma(g(x)).
\end{aligned}$$

De la misma manera, tenemos que:

$$\begin{aligned}
\sigma(f(x)g(x)) &= \sigma(\sum_{k=0}^{m+n}(\sum_{h=0}^{k}\alpha_h\beta_{k-h})x^k) \\
&= \sum_{k=0}^{m+n}\tau[\sum_{h=0}^{k}(\alpha_h\beta_{k-h})]t^k \\
&= \sum_{k=0}^{m+n}[\sum_{h=0}^{k}\tau(\alpha_h\beta_{k-h})]t^k \\
&= \sum_{k=0}^{m+n}[\sum_{h=0}^{k}\tau(\alpha_h)\tau(\beta_{k-h})]t^k \\
&= [\alpha'_0+\alpha'_1t+\cdots+\alpha'_nt^n][\beta'_0+\beta'_1t+\cdots+\beta'_mt^m] \\
&= \sigma(f(x))\sigma(g(x))
\end{aligned}$$

De manera que σ es un homomorfismo.

Sean $f(x), g(x) \in F[x]$ tales que $\sigma(f(x)) = \sigma(g(x))$, como σ es homomorfismo, entonces:

$$\begin{aligned}
\sigma(f(x)-g(x)) = 0' &\Leftrightarrow \sigma(\sum_{i=0}^{\infty}(\alpha_i-\beta_i)x^i) = 0' \\
&\Leftrightarrow \tau(\alpha_0-\beta_0)+\tau(\alpha_1-\beta_1)t+\cdots \\
&\quad +\tau(\alpha_n-\beta_n)t^n+\cdots = 0' \\
&\Leftrightarrow \tau(\alpha_i-\beta_i) = 0' \ \forall\ i \in \{1,\ldots\} \\
&\Leftrightarrow \alpha_i = \beta_i \ \forall\ i \in \{1,\ldots\} \\
&\Leftrightarrow f(x) = g(x).
\end{aligned}$$

Por lo tanto, σ es monomorfismo.

Sea $f'(t) \in F'[t]$, entonces, $f'(t) = \alpha'_0+\alpha'_1t+\cdots+\alpha'_kt^k$ con $\alpha'_0,\ldots,\alpha'_k \in F'$. Como τ es un isomorfismo de F en F', para cada $\alpha'_j \in F'$ existe $\alpha_j \in F$

tal que $\tau(\alpha_j) = \alpha'_j$. Sea $f(x) = \alpha_0 + \alpha_1 x + \cdots + \alpha_k x^k \in F[x]$, entonces, $\sigma(f(x)) = f'(t)$ y σ es epimorfismo.

Por último, $F \subset F[x]$; sea $\alpha \in F$, $\sigma(\alpha) = \tau(\alpha) = \alpha'$, por lo tanto, $\sigma|_F = \tau$.

□

Nota: Para simplificar la notación, a $\sigma(f(x))$ con $f(x) \in F[x]$ lo denotaremos por $f'(t) \in F[t]$, esto es, $\sigma(f(x)) = f'(t)$.

Corolario 15. $f(x) \in F[x]$ es irreducible si y sólo si $f'(t) \in F'[t]$ es irreducible.

Demostración. Sea $f'(t) \in F'[t]$, $f'(t) \neq 0$ y $f'(t) = q'(t)g'(t)$ para algunas $q'(t), g'(t) \in F'[t]$. Como $F \overset{\tau}{\cong} F'$, entonces, $q'(t) = \sigma(q(x))$ y $g'(t) = \sigma(g(x))$ para algunas $q(x), g(x) \in F[x]$. Sea $f(x) = q(x)g(x)$. Supongamos que $f(x)$ es irreducible, sin pérdida de generalidad, suponemos que $g(x)$ es unidad, por lo que $g(x) = \alpha$ para alguna $\alpha \in F$, $\alpha \neq 0$, de esta manera, tenemos:

$$\begin{aligned} q'(t)g'(t) &= f'(t) \\ &= \sigma(f(x)) \\ &= \sigma(q(x))\sigma(g(x)) \\ &= \sigma(q(x))\sigma(\alpha) \\ &= q'(t)\alpha' \end{aligned}$$

Así, $g'(t) = \alpha'$ para algún $\alpha' \in F'$ por lo que $g'(t)$ es una unidad en $F'[t]$, por lo tanto, $f'(t)$ es irreducible.

Análogamente, si $f'(t)$ es irreducible, entonces, $f(x)$ es irreducible.

□

Lema 17. Sean $F \overset{\tau}{\cong} F'$, $f(x) \in F[x]$, $f'(t) \in F'[t]$ y los ideales $\langle f(x)\rangle$ y $\langle f'(t)\rangle$ de $F[x]$ y $F'[t]$ respectivamente, entonces, existe un isomorfismo $\rho : F[x]/\langle f(x)\rangle \longrightarrow F'[t]/\langle f'(t)\rangle$ tal que $\rho|_F = \tau$.

Demostración. Sean $\langle f(x)\rangle = P$ y $\langle f'(t)\rangle = P'$, de esta manera podemos tomar $E = F[x]/P$ y $E' = F'[t]/P'$.

Sea $\sigma : F[x] \longrightarrow F'[t]$ como se definió en el lema 16; como σ es isomorfismo, veamos que $\sigma(P) = P'$:

$$\begin{aligned}\sigma(P) &= \{\sigma(f(x)g(x)) \mid g(x) \in F[x]\} \\ &= \{\sigma(f(x))\sigma(g(x)) \mid g(x) \in F[x]\} \\ &= \{f'(t)g'(t) \mid g'(t) \in F'[t]\} \\ &= P'.\end{aligned}$$

Sea $\rho : E \longrightarrow E'$ dado por $\rho(P + g(x)) = P' + \sigma(g(x)) \ \forall \ g(x) \in F[x]$ (recordemos que $\sigma(g(x)) = g'(t) \ \forall \ g(x) \in F[x]$), por la proposición 31, ρ está bien definido y es un homomorfismo, asimismo, $\ker\rho = \pi(\sigma^{-1}(P'))$ e $\text{Img}\rho = \pi'(\text{Img}\sigma)$, esto es:

i) $\ker\rho = \pi(\sigma^{-1}(P')) = \pi(P) = P/P = P = 0_E$ y, por lo tanto, ρ es monomorfismo.

ii) $\text{Img}\rho = \pi'(\text{Img}\sigma) = \pi'(F'[t]) = F'[t]/P' = P' + g'(t) \ \forall \ g'(t) \in F'[t]$, por lo tanto, $\text{Img}\rho = E'$ y ρ es epimorfismo.

Por *i)* y *ii)*, ρ es isomorfismo.

Como en el teorema 30, identificamos a $F \cong F[x]/P = \{P + \alpha \mid \alpha \in F\}$ y a $F' \cong F'[t]/P' = \{P' + \alpha' \mid \alpha' \in F'\}$, de manera que $\rho(\alpha) = \rho(P + \alpha) = P' + \sigma(\alpha) = P' + \alpha' = \alpha' \ \forall \ \alpha \in F$.

Por lo tanto, existe un isomorfismo $\rho : F[x]/\langle f(x)\rangle \longrightarrow F'[t]/\langle f'(t)\rangle$ tal que $\rho|_F = \tau$.

□

Teorema 32. Sean $F \overset{\tau}{\cong} F'$, $p(x) \in F[x]$ irreducible con $\text{grad}p(x) = n \geq 1$ y ν, ω raíces de $p(x)$ y $p'(t)$ respectivamente, entonces, existe un isomorfismo único $\psi : F(\nu) \longrightarrow F'(\omega)$ tal que $\psi(\nu) = \omega$ y $\psi|_F = \tau$.

Demostración. Tomemos $E = F[x]/\langle p(x)\rangle$ como en el teorema 30, E es una extensión finita en donde $p(x)$ tiene una raíz y $[E : F] = n$; sea $\nu \in E$ raíz de $p(x)$.

Por otro lado, como $\text{grad}p(x) = n$ y $p(x)$ es irreducible, por el teorema 26, $[F(\nu) : F] = n$. Así, podemos definir un isomorfismo $\phi : E \longrightarrow F(\nu)$ dado por $\phi(P + f(x)) = f(\nu)$. Análogamente, con $E' = F'[t]/\langle p'(t)\rangle$ y ω una raíz de $p'(t)$ definimos $\phi' : E' \longrightarrow F'(\omega)$ dado por $\phi'(P' + f'(t)) = f'(\omega)$.

Como ϕ es isomorfismo, entonces, ϕ^{-1} también es isomorfismo. Sea ρ como en el lema 17, definimos el isomorfismo $\psi : F(\nu) \longrightarrow F'(w)$ dado por $\psi(f(\nu)) = (\phi \circ \rho \circ \phi^{-1})(f(\nu)) = f'(w)$ y tenemos:

i) sean $\nu = P + x$ la raíz de $p(x)$ en E y $\omega = P' + t$ la raíz de $p'(t)$ en E' como en el teorema 30, entonces, para $\nu \in F(\nu)$, tenemos:

$$\begin{aligned}
\psi(\nu) &= (\phi' \circ \rho \circ \phi^{-1})(\nu) \\
&= (\phi' \circ \rho)(\phi^{-1}(\nu)) \\
&= (\phi' \circ \rho)(\nu) \\
&= (\phi' \circ \rho)(P + x) \\
&= \phi'(\rho(P + x)) \\
&= \phi'(P' + t) \\
&= \phi'(\omega) \\
&= \omega.
\end{aligned}$$

ii) sea $\alpha \in F \subset F(\nu)$ tal que $\alpha \neq \nu$, tenemos:

$$\begin{aligned}
\psi(\alpha) &= (\phi' \circ \rho \circ \phi^{-1})(\alpha) \\
&= (\phi' \circ \rho)(\phi^{-1}(\alpha)) \\
&= (\phi' \circ \rho)(\alpha) \\
&= (\phi' \circ \rho)(P + \alpha) \\
&= \phi'(\rho(P + \alpha)) \\
&= \phi'(P' + \alpha') \\
&= \phi'(\alpha') \\
&= \alpha'.
\end{aligned}$$

Con $\alpha' \in F' \subset F'(\omega)$. De manera que $\psi(\alpha) = \alpha' \ \forall \ \alpha \in F$.

Así, $\psi : F(\nu) \longrightarrow F'(\omega)$ es un isomorfismo tal que $\psi(\nu) = \omega$ y $\psi|_F = \tau$.

Por último, supongamos que existe un isomorfismo $\psi' : F(\nu) \longrightarrow F(\omega)$ tal que $\psi'(\nu) = \omega$ y $\psi'|_F = \tau$. Sea $a \in F(\nu)$, entonces, existen $f(x), g(x) \in F[x]$ tales que $a = f(\nu)/g(\nu)$ con $g(\nu) \neq 0$; $f(x) = \sum_{i=0}^{n} \alpha_i x^i$ y $g(x) = \sum_{j=0}^{m} \beta_j x^j$ con $\alpha_i, \beta_j \in F \ \forall \ i \in \{0, \ldots, n\}$ y $\forall \ j \in \{0, \ldots, m\}$. De esta manera, $\forall \ a \in F(\nu)$:

$$\begin{aligned}
\psi'(a) &= \psi'(f(\nu)g(\nu)^{-1}) \\
&= \psi'((\sum_{i=0}^{n}\alpha_i\nu^i)(\sum_{j=0}^{m}\beta_j\nu^j)^{-1}) \\
&= (\sum_{i=0}^{n}\psi'(\alpha_i\nu^i))(\sum_{j=0}^{m}\psi'(\beta_j\nu^j))^{-1} \\
&= (\sum_{i=0}^{n}\alpha_i\omega^i))(\sum_{j=0}^{m}\beta_j\omega^j))^{-1} \\
&= (\sum_{i=0}^{n}\psi(\alpha_i\nu^i))(\sum_{j=0}^{m}\psi(\beta_j\nu^j))^{-1} \\
&= \psi((\sum_{i=0}^{n}\alpha_i\nu^i)(\sum_{j=0}^{m}\beta_j\nu^j)^{-1}) \\
&= \psi(f(\nu)g(\nu)^{-1}) \\
&= \psi(a).
\end{aligned}$$

Por lo tanto, el isomorfismo ψ es único.

□

Corolario 16. Sean $p(x) \in F[x]$ irreducible y a y b dos raíces de $p(x)$, entonces, $\psi : F(a) \longrightarrow F(b)$ es un isomorfismo tal que $\psi(a) = b$ y $\psi(\alpha) = \alpha$ $\forall\ \alpha \in F$, $\alpha \neq a$.

Demostración. Sea grad$p(x) = n$. Sabemos que $[F(a) : F] = n$ y que $[F(b) : F] = n$. Por el teorema 30, sabemos que existen extensiones finitas E y E' de F en las cuales a y b son raíces respectivamente y $[E : F] = [E' : F] = n$.

Se cumplen las hipótesis del teorema 32, por lo tanto, $F(a) \cong F(b)$, $\psi(a) = b$ y ψ tiene la propiedad de que $\psi(\alpha) = \alpha'$ $\forall\ \alpha \in F$, $\alpha \neq a$, como $F = F'$, entonces, $\psi(\alpha) = \alpha$ $\forall\ \alpha \in F$, $\alpha \neq a$.

□

Teorema 33. Sean $F \overset{\tau}{\cong} F'$, E campo de descomposición de $f(x) \in F[x]$ y E' campo de descomposición de $f'(t) \in F'[t]$, entonces:

i) existe un isomorfismo $\psi : E \longrightarrow E'$ tal que $\psi|_F = \tau$.

ii) si $f(x)$ es separable, existen exactamente $[E : F]$ isomorfismos de E en E' que extienden a τ.

Demostración. La demostración la haremos por inducción sobre la dimensión de E sobre F, esto es, sobre n con $[E : F] = n$.

i) Sea $[E : F] = 1$, entonces, la base de E sobre F es $\Gamma_1 = \{1\}$ y $E = \{\alpha 1 \mid \alpha \in F\} = F$; análogamente, $E' = F'$ y así, tomamos $\psi = \tau$ y ψ hace válido el resultado del teorema para $n = 1$.

Suponemos que el resultado es válido para los campos de descomposición tales que $[E : F] < k$, $k \in \mathbb{N}$. Sean E un campo de descomposición de $f(x)$ tal que $[E : F] = k > 1$ y $p(x)$ un factor irreducible de $f(x)$ tal que grad$p(x) = m > 1$. Como E es campo de descomposición de $f(x)$ y toda raíz de $p(x)$ es raíz de $f(x)$, entonces, en E existen m raíces de $p(x)$. Sea $\nu \in E$ raíz de $p(x)$, esto es, $p(\nu) = 0$; como ν es raíz de $p(x)$, sabemos que $[F(\nu) : F] = m$.

Por otro lado, sabemos que $[E : F] = [E : F(\nu)][F(\nu) : F]$, así, $[E : F(\nu)] = [E : F]/[F(\nu) : F] = n/m < n$. Por el teorema 32, existe un isomorfismo único $\psi' : F(\nu) \longrightarrow F'(\omega)$ tal que $\psi'(\nu) = \omega$ y $\psi'|_F = \tau$, entonces, como E es un campo de descomposición de $f(x) \in F(\nu)[x]$ y E' es un campo de descomposición de $f'(t) \in F'(\omega)[t]$, por la hipótesis de inducción, existe un isomorfismo $\psi : E \longrightarrow E'$ tal que $\psi|_F = \tau$ lo cual concluye la demostración por inducción.

ii) Sea $[E : F] = 1$, entonces, $E = F$ y únicamente existe un isomorfismo ψ tal que $\psi|_F = \tau$, a saber, $\psi = \tau$ y el resultado del teorema es válido para $n = 1$.

Suponemos que el resultado es válido para los campos de descomposición tales que $[E : F] < k$, $k \in \mathbb{N}$. Sean $[E : F] = k > 1$ y $f(x) = p(x)g(x)$ con $p(x)$ irreducible y $1 <$ grad$p(x) = r \leq k$. Sea ν una raíz de $p(x)$ en E y ψ un isomorfismo como en el inciso *i)* tal que $\psi(\nu) = \nu'_i$ con ν'_i una raíz de $p'(t)$ en E', como $p'(t)$ es irreducible en E', entonces, $p'(t)$ tienen exactamente r raíces en E'. Por el teorema 32, existen r isomorfismos distintos $\psi_i : F(\nu) \longrightarrow F'(\nu'_i)$ que extienden a τ.

Ahora, E y E' son campos de descomposición de $f(x)$ sobre $F(\nu)$ y de $f'(t)$ sobre $F'(\nu'_i)$ respectivamente; $[E : F] = [E : F(\nu)][F(\nu) : F] = [E : F(\nu)]r$ por lo que $[E : F(\nu)] = k/r < k$. Por la hipótesis de inducción, existen k/r isomorfismos de E en E' para cada uno de los isomorfismos $\psi_i : F(\nu) \longrightarrow F'(\nu'_i)$, esto es, existen $(k/r)r = k$ isomorfismos de E en E' pues cada isomorfismo de E en E'que extienede a τ, al restringirlo a

$F(\nu)$ coincide con algún ψ_i.

□

Corolario 17. Sean E_1 y E_2 campos de descomposición de $f(x) \in F[x]$, entonces, $E_1 \cong E_2$.

Demostración. Como $F \overset{\tau}{\cong} F$, entonces, sea $F[x] = F'[t]$, aplicamos el teorema 33 y obtenemos el isomorfismo $\psi : E_1 \longrightarrow E_2$ tal que $\psi|_F = \tau$. □

Observaciíon: Como cualesquiera dos campos de descomposición son isomorfos (corolario 17), podemos hablar de *el* campo de descomposición de $f(x) \in F[x]$.

Lema 18. Sean E una extensión de F, $f(x) \in F[x]$ y $\psi : E \longrightarrow E$ un automorfismo que fija a F; si $a \in E$ es una raíz de $f(x)$, entonces, $\psi(a)$ es raíz de $f(x)$.

Demostración. Sea $f(x) = \sum_{i=0}^{n} \alpha_i x^i$, tenemos:

$$\begin{aligned} f(\psi(a)) &= \sum_{i=0}^{n} \alpha_i \psi(a)^i \\ &= \sum_{i=0}^{n} \psi(\alpha_i a^i) \\ &= \psi(\sum_{i=0}^{n} \alpha_i a^i) \\ &= \psi(f(a)) \\ &= \psi(0) \\ &= 0. \end{aligned}$$

Por lo tanto, $\psi(a)$ es raíz de $f(x)$.

□

Lema 19. Sea K extensión finita de F, entonces, existe un campo de descomposición E de algún polinomio $f(x) \in F[x]$ tal que $K \subset E$.

Demostración. Como K es una extensión finita, por la proposición 35, K es algebraica por lo que existen $a_1, \ldots, a_n \in K$ tales que $K = F(a_1, \ldots, a_n)$ con a_i raíz de un polinomio irreducible $p_i(x) \in F[x]$ $\forall\ i \in \{1, \ldots, n\}$.

Sea $f(x) = \prod_{i=1}^{n} p_i(x) \in F[x]$, por el teorema 31, existe un campo de descomposición E de $f(x) \in F[x]$ tal que $K \subset E$.

□

6. Teoría de Galois

6.1. Automorfismos, campo fijo, grupo de Galois

Definición 70. Sea K un campo, un *automorfismo* de K es un isomorfismo $\sigma : K \longrightarrow K$.

Dos automorfismos σ_1 y σ_2 de K son iguales si $\sigma_1(\alpha) = \sigma_2(\alpha)\ \forall\ \alpha \in K$.

Al conjunto de todos los automorfismos del campo K lo denotamos por:

$$\mathrm{Aut}(K) = \{\sigma \mid \sigma \text{ es automorfismo de } K\}$$

Proposición 36. Sea K un campo y $\circ$ la composición de funciones, entonces, $(\mathrm{Aut}(K), \circ)$ forma un grupo.

Demostración. Sea I_K la función identidad sobre K; $I_K \in \mathrm{Aut}(K)$ de manera que $\mathrm{Aut}(K) \neq \emptyset$. Sean $\sigma_1, \sigma_2, \sigma_3 \in \mathrm{Aut}(K)$, entonces:

i) $\forall\ \alpha \in K$ tenemos que:

$$\begin{aligned} \sigma_3(\sigma_2 \circ \sigma_1)(x) &= \sigma_3(\sigma_2 \circ \sigma_1(x)) \\ &= \sigma_3(\sigma_2(\sigma_1(x))) \\ &= \sigma_3(\sigma_2(\sigma_1(x))) \\ &= (\sigma_3 \circ \sigma_2)(\sigma_1(x)) \\ &= (\sigma_3 \circ \sigma_2)\sigma_1(x) \end{aligned}$$

Por lo tanto, $(\mathrm{Aut}(K), \circ)$ es asociativa. Es bien sabido que la composición de funciones es asociativa.

ii) como $\sigma_1 : K \longrightarrow K$ y $\sigma_2 : K \longrightarrow K$ son isomorfismos, entonces, $\sigma_2 \circ \sigma_1 : K \longrightarrow K$ es isomorfismo y $\mathrm{Aut}(K)$ es cerrado bajo $\circ$.

iii) sea $\sigma_I = I_K$, entonces, $\forall\ \alpha \in K$ tenemos que:

$$\begin{aligned}(\sigma_1 \circ \sigma_I)(\alpha) &= \sigma_1(\sigma_I(\alpha)) \\ &= \sigma_1(\alpha) \\ &= \sigma_I(\sigma_1(\alpha)) \\ &= (\sigma_I \circ \sigma_1)(\alpha)\end{aligned}$$

Por lo tanto, σ_I es elemento neutro de $(\mathrm{Aut}(K), \circ)$.

iv) como σ_1 es isomorfismo, entonces, existe σ_1^{-1} isomorfismo y $\sigma_1 \circ \sigma_1^{-1} = \sigma_I$, por lo tanto, $\forall\ \sigma \in \mathrm{Aut}(K)$ existe un elemento inverso.

Por *i), ii), iii)* y *iv)*, $(\mathrm{Aut}(K), \circ)$ forma un grupo.

□

Definición 71. Sea G un conjunto de automorfismos de K ($G \subset \mathrm{Aut}(K)$), llamamos *campo fijo de* G al conjunto de elementos $\alpha \in K$ tales que $\sigma(\alpha) = \alpha$ $\forall\ \sigma \in G$.

Al campo fijo de $G \subset \mathrm{Aut}(K)$ lo denotamos por:

$$K^G = \{\alpha \in K \mid \sigma(\alpha) = \alpha\ \forall\ \sigma \in G\}$$

Proposición 37. Sea K un campo y $G \subset \mathrm{Aut}(K)$, entonces, K^G es un subcampo de K.

Demostración. Sean $\alpha, \beta \in K^G$, esto es, $\sigma(\alpha) = \alpha$ y $\sigma(\beta) = \beta\ \forall\ \sigma \in G$; como σ es un isomorfismo, entonces, $\sigma(\alpha - \beta) = \sigma(\alpha) - \sigma(\beta) = \alpha - \beta$, por lo que $\alpha - \beta \in K^G$; de la misma manera, $\sigma(\alpha\beta) = \sigma(\alpha)\sigma(\beta) = \alpha\beta$ y así, $\alpha\beta \in K^G$, por lo tanto, K^G es un subanillo de K.

Supongamos que $\beta \neq 0$, como K es campo, $\exists\ \beta^{-1} \in K$ inverso multiplicativo de β y tenemos que $\sigma(\beta^{-1}) = \sigma(\beta)^{-1} = \beta^{-1}$ por lo que $\beta^{-1} \in K^G$ y así, K^G es un subcampo de K.

□

Definición 72. Sea F un subcampo del campo K, llamamos *grupo de automorfismos relativos a* F al conjunto de todos los automorfismos de K tales que $\sigma(\alpha) = \alpha \ \forall \ \alpha \in F$ (σ fija a F) y lo denotamos por:

$$\mathrm{Gal}_{(K,F)} = \{\sigma \in \mathrm{Aut}(K) \mid \sigma(\alpha) = \alpha \ \forall \ \alpha \in F\}$$

Proposición 38. Sean K un campo y F un subcampo de K, entonces, $(\mathrm{Gal}_{(K,F)}, \circ) < \mathrm{Aut}(K)$ con $\circ$ la composición de funciones.

Demostración. Sean $\sigma_1, \sigma_2 \in \mathrm{Gal}_{(K,F)}$, entonces, $\sigma_2 \circ \sigma_1 : K \longrightarrow K$ y $\forall$ $\alpha \in F$, $(\sigma_2 \circ \sigma_1)(\alpha) = \sigma_2(\sigma_1(\alpha)) = \sigma_2(\alpha) = \alpha$, por lo tanto, $\sigma_2 \circ \sigma_1 \in \mathrm{Gal}_{(K,F)}$ y $\mathrm{Gal}_{(K,F)}$ es cerrado bajo $\circ$; sabemos que la composición de funciones es asociativa.

Sea $I_K : K \longrightarrow K$ la función identidad sobre K, esto es, $\forall\, \alpha \in K$, $I_K(\alpha) = \alpha$, por lo tanto, $I_K \in \mathrm{Gal}_{(K,F)}$. Sea $\sigma \in \mathrm{Gal}_{(K,F)}$, tenemos que $\forall\ \alpha \in K$, $(I_K \circ \sigma)(\alpha) = I_K(\sigma(\alpha)) = \sigma(\alpha) = \sigma(I_K(\alpha)) = (\sigma \circ I_K)(\alpha)$, por lo tanto, I_K es el elemento neutro de $\mathrm{Gal}_{(K,F)}$ bajo $\circ$. Por último, como σ es isomorfismo, es invertible y como $\sigma(\alpha) = \alpha \ \forall \ \alpha \in F$, entonces, $\sigma^{-1}(\alpha) = \alpha \ \forall \ \alpha \in F$, de manera que $\sigma^{-1} \in \mathrm{Gal}_{(K,F)}$. Por lo tanto, $(\mathrm{Gal}_{(K,F)}, \circ) < \mathrm{Aut}(K)$.

□

A $\mathrm{Gal}_{(K,F)}$ se le conoce como *el grupo de Galois* de la extensión K de F.

Lema 20. Sean E extensión de K y K extensión de F tal que es el campo de descomposición de $f(x) \in F[x]$; si $\sigma \in \mathrm{Gal}_{(E,F)}$, entonces, $\sigma|_K \in \mathrm{Gal}_{(K,F)}$.

Demostración. Como K es campo de descomposición de $f(x) \in F$, todas las raíces de $f(x) : a_1, \ldots, a_h \in K$ y $K = F(a_1, \ldots, a_h)$. Por el lema 18, $\sigma(a_i) \in K$ es raíz de $f(x)\ \forall\ i \in \{1, \ldots, h\}$, de esta manera tenemos:

$$\begin{aligned} \sigma(K) &= \sigma(F(a_1, \ldots, a_h)) \\ &= F(\sigma(a_1), \ldots, \sigma(a_h)) \\ &= K. \end{aligned}$$

Así, $\sigma|_K \in \mathrm{Aut}(K)$ y fija a $F \subset K$, por lo tanto, $\sigma|_K \in \mathrm{Gal}_{(K,F)}$.

□

Teorema 34. Sean E el campo de descomposición de $f(x) \in F[x]$ y $f(x)$ separable, entonces, $\mathrm{o}(\mathrm{Gal}_{(E,F)}) = [E : F]$.

Demostración. Por el inciso *ii)* del teorema 33, sean $F = F'$ y $E = E'$, entonces, existen $[E : F]$ isomorfismos que dejan fijo al campo F, esto es, $o(\text{Gal}_{(E,F)}) = [E : F]$.

□

Teorema 35. Sean K extensión de F y E extensión de K tales que K es el campo de descomposición de $f(x) \in F[x]$ y E es el campo de descomposición de $g(x) \in F[x]$, entonces, $\text{Gal}_{(E,K)} \lhd \text{Gal}_{(E,F)}$ y $\text{Gal}_{(E,F)}/\text{Gal}_{(E,K)} \cong \text{Gal}_{(K,F)}$.

Demostración. Sea $\psi : \text{Gal}_{(E,F)} \longrightarrow \text{Gal}_{(K,F)}$ dada por $\psi(\sigma) = \sigma|_K$. Por el lema 20, ψ está bien definida. Sean $\sigma_1, \sigma_2 \in \text{Gal}_{(E,F)}$ y $\alpha \in K$, tenemos:

$$\begin{aligned}
\psi(\sigma_1 \circ \sigma_2)(\alpha) &= (\sigma_1 \circ \sigma_2)|_K(\alpha) \\
&= (\sigma_1 \circ \sigma_2)(\alpha) \\
&= \sigma_1(\sigma_2(\alpha)) \\
&= \sigma_1|_K(\sigma_2|_K(\alpha)) \\
&= (\sigma_1|_K \circ \sigma_2|_K)(\alpha) \\
&= (\psi(\sigma_1) \circ \psi(\sigma_2))(\alpha).
\end{aligned}$$

Por lo tanto, ψ es un homomorfismo.

Sean $\sigma \in \text{Gal}_{(E,F)}$ tal que $\psi(\sigma) = I_K$ y $\alpha \in K$, entonces, $\sigma(\alpha) = \sigma|_K(\alpha) = \alpha$ y así, $\sigma \in \text{Gal}_{(E,K)}$ y $\ker\psi \subset \text{Gal}_{(E,K)}$. Por otro lado, sean $\sigma \in \text{Gal}_{(E,K)}$ y $\alpha \in K$. Como $F \subset K$, $\sigma \in \text{Gal}_{(E,F)}$ y así, $\sigma(\alpha) = \sigma|_K(\alpha) = \alpha$ por lo que $\psi(\sigma) = I_K$ y $\text{Gal}_{(E,K)} \subset \ker\psi$. Por lo tanto, $\text{Gal}_{(E,K)} = \ker\psi$ y, por el corolario 4, $\text{Gal}_{(E,K)} \lhd \text{Gal}_{(E,F)}$.

Por último, sea $\rho' \in \text{Gal}_{(K,F)}$, como E y K son campos de descomposición de $f(x), g(x) \in F[x]$ respectivamente, entonces, por el teorema 33, existe un automorfismo $\rho \in E$ que extiende a ρ', esto es, $\psi(\rho) = \rho'$, por lo tanto, ψ es epimorfismo y así, $\text{Img}\psi = \text{Gal}_{(K,F)}$. Por el teorema 11 (primer teorema de isomorfismos), $\text{Gal}_{(E,F)}/\text{Gal}_{(E,K)} \cong \text{Gal}_{(K,F)}$.

□

Lema 21. Sean K un campo, $\alpha_1, \ldots, \alpha_n \in K$ y $\sigma_1, \ldots, \sigma_n \in \text{Aut}(K)$ tales que $\sigma_1 \neq \cdots \neq \sigma_n$. Si $\alpha_1\sigma_1(a) + \cdots + \alpha_n\sigma_n(a) = 0 \ \forall \ a \in K$, entonces, $\alpha_1 = \cdots = \alpha_n = 0$.

Demostración. Supongamos que existen $\alpha_1, \ldots, \alpha_n \in K$, no todos cero, tales que $\alpha_1\sigma_1(a) + \cdots + \alpha_n\sigma_n(a) = 0 \ \forall \ a \in K$. Así, podemos renombrar las α_i's

y obtenemos $\alpha_1\sigma_1(a) + \cdots + \alpha_m\sigma_m(a) = 0 \ \forall \ a \in K$ con $\alpha_1 \neq 0, \ldots, \alpha_m \neq 0$ y $m \leq n$ con m un número mínimo de términos.

Supongamos que $m = 1$, tenemos que $\alpha_1\sigma_1(a) = 0 \ \forall \ a \in K$ por lo que $\alpha_1 = 0$, lo cual contradice la hipótesis, entonces, $1 < m \leq n$. Como $\sigma_1 \neq \sigma_m$, $\exists \ b \in K$ tal que $\sigma_1(b) \neq \sigma_m(b)$. Por un lado, sabemos que $\alpha_1\sigma_1(ab)+\cdots+\alpha_m\sigma_m(ab) = \alpha_1\sigma_1(a)\sigma_1(b)+\cdots+\alpha_m\sigma_m(a)\sigma_m(b) = 0$, por otro lado, multiplicamos la expresión original por $\sigma_1(b)$ y obtenemos: $\alpha_1\sigma_1(a)\sigma_1(b) + \cdots + \alpha_m\sigma_m(a)\sigma_1(b) = 0$.

Restamos las dos igualdades de manera que $\alpha_1\sigma_1(a)(\sigma_1(b) - \sigma_1(b)) + \cdots + \alpha_m\sigma_m(a)(\sigma_m(b) - \sigma_1(b)) = 0$. Sea $\beta_i = \alpha_i(\sigma_i(b) - \sigma_1(b)) \ \forall \ i \in \{1, \ldots, m\}$, entonces, $\beta_1 = 0$ y $\beta_m \neq 0$ puesto que $\alpha_m \neq 0$ y $\sigma_m(b) - \sigma_1(b) \neq 0$; de esta manera tenemos que $\beta_2\sigma_2(a) + \cdots + \beta_m\sigma_m(a) = 0 \ \forall \ a \in K$ lo cual contradice el hecho de que m es un número mínimo de términos y así, no existen $\alpha_1, \ldots, \alpha_n \in K$, no todos cero, tales que $\alpha_1\sigma_1(a)+\cdots+\alpha_n\sigma_n(a) = 0 \ \forall \ a \in K$.

Por lo tanto, sean $\sigma_1, \ldots, \sigma_n$ automorfismos distintos, si $\alpha_1\sigma_1(a) + \cdots + \alpha_n\sigma_n(a) = 0 \ \forall \ a \in K$, entonces, $\alpha_1 = \cdots = \alpha_n = 0$.

□

Teorema 36. Sea K una extensión finita de F, entonces, $\mathrm{Gal}_{(K,F)}$ es un grupo finito y $\mathrm{o}(\mathrm{Gal}_{(K,F)}) \leq [K : F]$.

Demostración. Como K es una extensión finita de F, entonces, $[K : F] = n$ para algún $n \in \mathbb{N}$. Sea $\Gamma = \{\gamma_1, \ldots, \gamma_n\}$ una base de K sobre F. Sean $\alpha_1, \ldots, \alpha_{n+1} \in K$ y supongamos que existen $n + 1$ automorfismos distintos de K en $\mathrm{Gal}_{(K,F)}$. Sea $\alpha_1\sigma_1(\gamma_i) + \cdots + \alpha_{n+1}\sigma_{n+1}(\gamma_i) = 0 \ \forall \ i \in \{1, \ldots, n\}$ con $\alpha_1, \ldots, \alpha_{n+1} \in K$. Tenemos un sistema homogéneo de n ecuaciones lineales en $n + 1$ incógnitas, por lo tanto, tiene solución no trivial y las α_k's no son todas cero para $k \in \{1, \ldots, n + 1\}$.

Sea $a \in K$, entonces, $a = \beta_1\gamma_1 + \cdots + \beta_n\gamma_n$ para algunos $\beta_1, \ldots, \beta_n \in F$. De esta manera, tenemos que $\forall \ a \in K$ se cumple:

$$
\begin{aligned}
& \alpha_1\sigma_1(a) + \cdots + \alpha_{n+1}\sigma_{n+1}(a) \\
= \;& \alpha_1\sigma_1(\beta_1\gamma_1 + \cdots + \beta_n\gamma_n) + \cdots + \alpha_{n+1}\sigma_{n+1}(\beta_1\gamma_1 + \cdots \\
& +\beta_n\gamma_n) \\
= \;& \alpha_1[\sigma_1(\beta_1\gamma_1) + \cdots + \sigma_1(\beta_n\gamma_n)] + \cdots + \alpha_{n+1}[\sigma_{n+1}(\beta_1\gamma_1) + \cdots \\
& +\sigma_{n+1}(\beta_n\gamma_n)] \\
= \;& \alpha_1[\sigma_1(\beta_1)\sigma_1(\gamma_1) + \cdots + \sigma_1(\beta_n)\sigma_1(\gamma_n)] + \cdots \\
& +\alpha_{n+1}[\sigma_{n+1}(\beta_1)\sigma_{n+1}(\gamma_1) + \cdots + \sigma_{n+1}(\beta_n)\sigma_{n+1}(\gamma_n)] \\
= \;& \alpha_1[\beta_1\sigma_1(\gamma_1) + \cdots + \beta_n\sigma_1(\gamma_n)] + \cdots + \alpha_{n+1}[\beta_1\sigma_{n+1}(\gamma_1) + \cdots \\
& +\beta_n\sigma_{n+1}(\gamma_n)] \\
= \;& \alpha_1\beta_1\sigma_1(\gamma_1) + \cdots + \alpha_1\beta_n\sigma_1(\gamma_n) + \cdots + \alpha_{n+1}\beta_1\sigma_{n+1}(\gamma_1) + \cdots \\
& +\alpha_{n+1}\beta_n\sigma_{n+1}(\gamma_n) \\
= \;& \beta_1[\alpha_1\sigma_1(\gamma_1) + \cdots + \alpha_{n+1}\sigma_{n+1}(\gamma_1)] + \cdots + \beta_n[\alpha_1\sigma_1(\gamma_n) + \cdots \\
& +\alpha_{n+1}\sigma_{n+1}(\gamma_n)] \\
= \;& \beta_1 0 + \cdots + \beta_n 0 \\
= \;& 0.
\end{aligned}
$$

Lo cual es una contradicción con el resultado del lema 21, por lo tanto, en $\mathrm{Gal}_{(K,F)}$ no existen $n+1$ automorfismos distintos y así, $\mathrm{o}(\mathrm{Gal}_{(K,F)}) \leq [K : F]$. □

Lema 22. Sean K un campo y $G = \{\sigma_1, \ldots, \sigma_n\} \subset \mathrm{Aut}(K)$, entonces, $[K : K^G] \geq n$.

Demostración. Supongamos que existe $m < n$ tal que $[K, K^G] = m$ y sea $\Gamma = \{\gamma_1, \ldots, \gamma_m\} \subset K$ una base de K sobre K^G. Sean las ecuaciones $\alpha_1\sigma_1(\gamma_i) + \cdots + \alpha_n\sigma_n(\gamma_i) = 0 \; \forall \; i \in \{1, \ldots, m\}$ con $\alpha_1, \ldots, \alpha_n \in K$. Tenemos un sistema homogéneo de m ecuaciones lineales en n incógnitas, por lo tanto, tiene solución no trivial y las α_k's no son todas cero para $k \in \{1, \ldots, n\}$.

Sea $a \in K$, entonces, $a = \beta_1\gamma_1 + \cdots + \beta_m\gamma_m$ para algunos $\beta_1, \ldots, \beta_m \in K^G$; multiplicamos la ecuación i del sistema de ecuaciones por b_i y obtenemos las m ecuaciones $\beta_i\alpha_1\sigma_1(\gamma_i) + \cdots + \beta_i\alpha_n\sigma_n(\gamma_i) = 0$, como $\beta_i \in K^G$, entonces, $\alpha_1\sigma_1(\beta_i\gamma_i) + \cdots + \alpha_n\sigma_n(\beta_i\gamma_i) = 0 \; \forall \; i \in \{1, \ldots, m\}$; sumamos las m ecuaciones y tenemos que $\alpha_1\sigma_1(a) + \cdots + \alpha_n\sigma_n(a) = 0 \; \forall \; a \in K$ y las $\alpha_k's$ no todas cero, lo cual es una contradicción al lema 21, por lo tanto, $[K : K^G] \geq n$.

□

Teorema 37. Sean K un campo y $G = \{\sigma_1, \ldots, \sigma_n\} < \mathrm{Aut}(K)$, entonces, $[K : K^G] = n = \mathrm{o}(G)$.

Demostración. Supongamos que $[K : K^G] \leq n$, por el lema 22, $[K : K^G] \geq n$ y así, $[K : K^G] = n$.

Supongamos que $[K : K^G] > n$ de manera que existe $\Gamma = \{\gamma_1, \ldots, \gamma_{n+1}\} \subset K$ linealmente independiente sobre K^G. Sean las ecuaciones $\alpha_1\sigma_i(\gamma_1) + \cdots + \alpha_{n+1}\sigma_i(\gamma_{n+1}) = 0 \ \forall \ i \in \{1, \ldots, n\}$. Tenemos un sistema homogéneo de n ecuaciones con $n+1$ incógnitas, por lo tanto, tiene solución no trivial y las α_k's no son todas cero para $k \in \{1, \ldots, n+1\}$.

Sea $a = (a_1, \ldots, a_m, 0, \ldots, 0)$ solución al sistema de ecuaciones tal que m es el menor número de elementos distintos de cero y $a_m = 1$. Reordenamos el índice de los vectores, eliminamos aquellos que son cero y obtenemos las ecuaciónes: $a_1\sigma_i(\gamma_1) + \cdots + a_m\sigma_i(\gamma_m) = 0 \ \forall \ i \in \{1, \ldots, n\}$. Afirmamos que existe $a_j \notin K^G$. Supongamos que $a_i \in K^G \ \forall \ i \in \{1, \ldots, m\}$, entonces, $\forall \ \sigma \in G$ tenemos:

$$\begin{aligned} \sigma(a_1\gamma_1 + \cdots + a_m\gamma_m) &= \sigma(a_1\gamma_1) + \cdots + \sigma(a_m\gamma_m) \\ &= \sigma(a_1)\sigma(\gamma_1) + \cdots + \sigma(a_m)\sigma(\gamma_m) \\ &= a_1\sigma(\gamma_1) + \cdots + a_m\sigma(\gamma_m) \\ &= 0. \end{aligned}$$

Como σ es isomorfismo, entonces, $a_1\gamma_1 + \cdots + a_m\gamma_m = 0$ lo cual es una contradicción ya que Γ es un conjunto linealmente independiente; por lo tanto, existe $a_j \notin K^G$. Sin pérdida de generalidad supongamos que $a_1 \notin K^G$, esto es, $\exists \ \sigma_k \in G$ tal que $\sigma_k(a_1) \neq a_1$.

Como $G < \mathrm{Aut}(K)$, entonces, $\sigma_k \circ \sigma_j = \sigma_h$ para algún $h \in \{1, \ldots, n\}$; sea $j \neq k$, como $a_m = 1$, tenemos:

$$\begin{aligned} 0 &= a_1\sigma_j(\gamma_1) + \cdots + \sigma_j(\gamma_m) \\ &= \sigma_k(a_1\sigma_j(\gamma_1) + \cdots + \sigma_j(\gamma_m)) \\ &= \sigma_k(a_1\sigma_j(\gamma_1)) + \cdots + \sigma_k(\sigma_j(\gamma_m)) \\ &= \sigma_k(a_1)\sigma_k(\sigma_j(\gamma_1)) + \cdots + \sigma_k(\sigma_j(\gamma_m)) \\ &= \sigma_k(a_1)(\sigma_k \circ \sigma_j)(\gamma_1) + \cdots + (\sigma_k \circ \sigma_j)(\gamma_m) \\ &= \sigma_k(a_1)\sigma_h(\gamma_1) + \cdots + \sigma_h(\gamma_m). \end{aligned}$$

Restamos esta ecuación a la ecuación h del sistema de ecuaciones y tenemos:

$$\begin{aligned} 0 &= \sigma_k(a_1)\sigma_h(\gamma_1) + \cdots + \sigma_h(\gamma_m) - (a_1\sigma_h(\gamma_1) + \cdots + \sigma_h(\gamma_m)) \\ &= \sigma_h(\gamma_1)(\sigma_k(a_1) - a_1) - \cdots - \sigma_h(\gamma_{m-1})(\sigma_k(a_{m-1}) - a_{m-1}) \\ &\quad -(\sigma_h(\gamma_m) - \sigma_h(\gamma_m)) \\ &= \sigma_h(\gamma_1)(\sigma_k(a_1) - a_1) - \cdots - \sigma_h(\gamma_{m-1})(\sigma_k(a_{m-1}) - a_{m-1}). \end{aligned}$$

Como $\sigma_k(a_1) - a_1 \neq 0$, entonces, existe una solución no trivial con menos de m elementos distintos de cero lo cual es una contradicción ya que m es mínimo. Por lo tanto, $[K : K^G] = n = \mathrm{o}(G)$.

□

Corolario 18. Sean K un campo y $G, H < \mathrm{Aut}(K)$ subgrupos finitos tales que $K^G = K^H$, entonces, $G = H$.

Demostración. Sean $G, H < \mathrm{Aut}(K)$ finitos tales que $K^G = K^H$ y $|G| = n$. Supongamos que $G \neq H$, entonces, sin pérdida de generalidad, existe $\sigma \in H$ tal que $\sigma \notin G$. Como $\sigma \in H$, entonces, σ fija a $K^H = K^G$, por lo que σ fija a K^G; de esta manera, K^G queda fijo bajo $G \cup \{\sigma\}$ por lo que $K^G \subset K^{G\cup\{\sigma\}}$ y así, $[K : K^G] \geq [K : K^{G\cup\{\sigma\}}]$.

Como $|G \cup \{\sigma\}| = n + 1$, por el lema 22, $[K : K^{G\cup\{\sigma\}}] \geq n + 1$. Por otro lado, por el teorema 37, $[K : K^G] = n$, de esta manera tenemos que $n = [K : K^G] \geq [K : K^{G\cup\{\sigma\}}] \geq n + 1$ lo cual es una contradicción, por lo tanto, $G = H$.

□

6.2. Extensión de Galois, Teorema Fundamental de la Teoría de Galois, teorema del elemento primitivo

Definición 73. Sea K una extensión finita de F, si $K^{\mathrm{Gal}_{(K,F)}} = F$ decimos que K es una *extensión normal* de F o una *extensión de Galois* de F .

Observación 6. Si K es una extensión de Galois de F, entonces, $[K : F] = [K : K^{\mathrm{Gal}_{(K,F)}}] = |\mathrm{Gal}_{(K,F)}|$.

Demostración. Como K es una extensión de Galois de F, entonces, es una extensión finita y $K^{\mathrm{Gal}_{(K,F)}} = F$; como $\mathrm{Gal}_{(K,F)} < \mathrm{Aut}(K)$, por el teorema 37, $[K : K^{\mathrm{Gal}_{(K,F)}}] = |\mathrm{Gal}_{(K,F)}|$.

Por lo tanto, $[K : F] = [K : K^{\mathrm{Gal}_{(K,F)}}] = |\mathrm{Gal}_{(K,F)}|$.

□

Teorema 38. Sean E una extensión finita de F y $\mathrm{Gal}_{(E,F)}$, entonces, las siguientes condiciones son equivalentes:

i) $E^{\mathrm{Gal}_{(E,F)}} = F$.

ii) si $p(x) \in F[x]$ es irreducible y con una raíz en E, entonces, $p(x)$ es separable y se descompone en E.

iii) E es campo de descomposición para algún $f(x) \in F[x]$ separable.

Demostración. Como E es finita, entonces, $[E : F] = n$ para algún $n \in \mathbb{N}$ y, por el teorema 37, $|\mathrm{Gal}_{(E,F)}| = n$.

i) $\Rightarrow$ *ii)* Supongamos que $E^{\mathrm{Gal}_{(E,F)}} = F$ y $p(x) \in F[x]$ es irreducible con una raíz $\alpha \in E$; sea $\mathrm{Gal}_{(E,F)} = \{\sigma_1, \ldots, \sigma_n\}$. Definimos el conjunto $\{\alpha_1 = \sigma_1(\alpha), \ldots, \alpha_n = \sigma_n(\alpha)\}$ y a $g(x) \in E[x]$ como $g(x) = \prod_{i=1}^{n}(x - \alpha_i) = \sum_{i=1}^{n} a_i x^i$ con $a_1, \ldots, a_n \in F$.

Sea $\sigma \in \mathrm{Gal}_{(E,F)}$, como α es raíz de $p(x)$, entonces, α_i es raíz de $p(x)$ $\forall\, i \in \{1, \ldots, n\}$ y $\sigma(\alpha_i) = \alpha_j$ para algún $j \in \{1, \ldots, n\}$; de esta manera, $\sigma(g(x)) = g(x)$, por lo que $a_1, \ldots, a_n \in E^{\mathrm{Gal}_{(E,F)}} = F$ y $g(x)$ no tiene raíces múltiples. Como $p(x)$ es irreducible y α es raíz de $p(x)$ y de $g(x)$, entonces, $p(x)|g(x)$ y por lo tanto, $p(x)$ no tiene raíces múltiples en $E[x]$ y se descompone en E.

ii) $\Rightarrow$ *iii)* Sea $\alpha_1 \in E$ y $\alpha_1 \notin F$. Como E es extensión finita, por la proposición 35, E es algebraica por lo que existe $p_1(x) \in F[x]$ irreducible con raíz $\alpha_1 \in E$, de manera que $p_1(x)$ es separable y se descompone en E. Sea K_1 el campo de descomposición de $p_1(x)$, $K_1 \subset E$; si $K_1 = E$ la implicación queda demostrada. Supongamos que $K_1 \neq E$, repetimos el procedimiento con $\alpha_2 \in E$ y $\alpha_2 \notin K_1$. Sea $p_2(x) \in F[x]$ su polinomio irreducible, entonces, $p_2(x)$ es separable y se descompone en E. Sea

$K_2 \subset E$ el campo de descomposición de $p_1(x)p_2(x)$ que es separable. Si $K_2 = E$ la implicación queda demostrada, de no ser así, repetimos el proceso y como E es finita, entonces, para algún $m \in \mathbb{N}$, $K_m = E$, así, E es campo de descomposición para algún $f(x) \in F[x]$ separable.

iii) $\Rightarrow$ *i)* Por el teorema 34, $[E : F] = |\mathrm{Gal}_{(E,F)}|$ y por el teorema 37, $[E : E^{\mathrm{Gal}_{(E,F)}}] = |\mathrm{Gal}_{(E,F)}|$, por lo que $[E : F] = [E : E^{\mathrm{Gal}_{(E,F)}}]$ y como $F \subset E^{\mathrm{Gal}_{(E,F)}}$, entonces, $F = E^{\mathrm{Gal}_{(E,F)}}$.

□

Proposición 39. Sean E una extensión de Galois de F y K un campo tal que $F \subset K \subset E$ (campo intermedio), entonces, E es una extensión de Galois de K.

Demostración. Como E una extensión de Galois de F, entonces, E es un campo de descomposición para algún $f(x) \in F[x] \subset K[x] \subset E[x]$, por lo tanto, E es un campo de descomposición para algún $f(x) \in K[x] \subset E[x]$, por el teorema 38, $E^{\mathrm{Gal}_{(E,K)}} = K$ y E es una extensión de Galois de K.

□

Definición 74. Sean E extensión finita de F y los campos intermedios K y L; si existe un isomorfismo $\psi : K \longrightarrow L$ tal que ψ fija a F, decimos que L es *campo conjugado* de K .

Teorema 39. Sean E una extensión de Galois de F y K un campo intermedio, entonces, las siguientes condiciones son equivalentes:

i) K es extensión de Galois de F.

ii) si L es campo conjugado de K, entonces, $L = K$.

iii) si $\sigma \in \mathrm{Gal}_{(E,F)}$, entonces, $\sigma|_K \in \mathrm{Gal}_{(K,F)}$.

Demostración. Como E es extensión de Galois de F, entonces, E es extensión finita de F y $E^{\mathrm{Gal}_{(E,F)}} = F$ y como K es campo intermedio, $F \subset K \subset E$.

i) $\Rightarrow$ *ii)* Como K es extensión de Galois de F, entonces, K es extensión finita de F y $K^{\mathrm{Gal}_{(K,F)}} = F$. Por el teorema 38, K es campo de descomposición para algún $f(x) \in F[x]$ separable, esto es, $K = F(\alpha_1, \ldots, \alpha_n)$, donde $\alpha_1, \ldots, \alpha_n$ son todas las raíces de $f(x)$ en K. Por el lema 18, si ψ es un automorfismo que fija a F, entonces, $\forall\ i \in \{1, \ldots, n\}$, $\psi(\alpha_i) = \alpha_j$ para algún $j \in \{1, \ldots, n\}$ y tenemos:

$$\begin{aligned}\psi(K) &= \psi(F(\alpha_1,\ldots,\alpha_n)) \\ &= (F(\alpha_1,\ldots,\alpha_n)) \\ &= K.\end{aligned}$$

De esta manera, todo campo conjugado de K es K.

ii) $\Rightarrow$ *iii)* Supongamos que existe $\sigma \in \mathrm{Gal}_{(E,F)}$ tal que $\sigma|_K \notin \mathrm{Gal}_{(K,F)}$. Como $\sigma|_K$ fija a F y $\sigma|_K \notin \mathrm{Gal}_{(K,F)}$, entonces, existe $a \in K$ tal que $\sigma|_K(a) \notin K$ por lo que $\sigma(a) \notin K$. Como σ es automorfismo, entonces, $\sigma|_K : K \longrightarrow \mathrm{Img}(\sigma|_K)$ es un isomorfismo, así, $K \cong \mathrm{Img}(\sigma|_K) \neq K$, lo cual es una contradicción. Por lo tanto, *ii)* $\Rightarrow$ *iii).*

iii) $\Rightarrow$ *i)* Como E es extensión finita de F y K es campo intermedio, entonces, K es extensión finita de F. Por otro lado, $F \subset K^{\mathrm{Gal}_{(K,F)}}$; por hipótesis, $E^{\mathrm{Gal}_{(E,F)}} = F$ y $\{\sigma|_K \mid \sigma \in \mathrm{Gal}_{(E,F)}\} \subset \mathrm{Gal}_{(K,F)}$, entonces, $F \subset K^{\mathrm{Gal}_{(K,F)}} \subset F$, por lo tanto, $K^{\mathrm{Gal}_{(K,F)}} = F$ y K es extensión de Galois de F.

□

Definición 75. Sea G un grupo, definimos al conjunto de subgrupos de G como:

$$\mathrm{Sub}(G) = \{H \mid H < G\}.$$

Definición 76. Sea E una extensión de F, definimos al conjunto de campos intermedios de E sobre F como:

$$\mathrm{Lat}_{(E,F)} = \{K \mid K \text{ es campo y } F \subset K \subset E\}.$$

Definición 77. Sea A un conjunto finito, definimos $\#A$ como la cardinalidad del conjunto A, es decir, el número de elementos del conjunto A.

Teorema 40. (Teorema Fundamental de la Teoría de Galois). Sean E una extensión de Galois de F, entonces:

i) $\xi : \mathrm{Sub}(\mathrm{Gal}_{(E,F)}) \longrightarrow \mathrm{Lat}_{(E,F)}$ dado por $\xi(H) \longrightarrow E^H$ es un biyección que revierte el orden y cuyo inverso es $\zeta : \mathrm{Lat}_{(E,F)} \longrightarrow \mathrm{Gal}_{(E,F)}$ dado por $\zeta(K) \longrightarrow \mathrm{Gal}_{(E,K)}$.

ii) K es una extensión de Galois de F si y sólo si $\mathrm{Gal}_{(E,K)} \lhd \mathrm{Gal}_{(E,F)}$.

Demostración. Sea $H \in \mathrm{Sub}(\mathrm{Gal}_{(E,F)})$, por la proposición 37, $E^H = K$ para algún K subcampo de E. Sea $\sigma \in H$, entonces, $\sigma \in \mathrm{Gal}_{(E,F)}$ y σ fija a F de manera que $F \subset E^H = K \subset E$, por lo tanto, $H = \mathrm{Gal}_{(E,K)}$ para algún campo intermedio K y $\mathrm{Gal}_{(E,K)} \in \mathrm{Sub}(\mathrm{Gal}_{(E,F)})$.

Sea K campo intermedio de la extensión E de F, por la proposición 39, E es una extensión de Galois de K y $E^{\mathrm{Gal}_{(E,K)}} = K$.

i) Sean $I, J \in \mathrm{Sub}(\mathrm{Gal}_{(E,F)})$ tales que $\xi(I) = \xi(J)$, esto es, $E^I = E^J$ y, por el corolario 18, $I = J$, por lo tanto, ξ es inyectiva. Consideremos la composición de funciones $\xi \circ \zeta$, entonces, $\forall\ K \in \mathrm{Lat}_{(E,F)}$ tenemos:

$$\begin{aligned}(\xi \circ \zeta)(K) &= \xi(\zeta(K)) \\ &= \xi(\mathrm{Gal}_{(E,K)}) \\ &= E^{\mathrm{Gal}_{(E,K)}} \\ &= K.\end{aligned}$$

Por lo tanto, $\xi \circ \zeta = I_{\mathrm{Lat}_{(E,F)}}$ y ξ es una biyección cuyo inverso es ζ.

Sean $I, J \in \mathrm{Sub}(\mathrm{Gal}_{(E,F)})$ tales que $I \subset J$, entonces, $E^J \subset E^I$, esto es, $\xi(J) \subset \xi(I)$ y así, ξ revierte el orden.

ii) Sea K extensión de Galois de F, por el teorema 35, $\mathrm{Gal}_{(E,K)} \lhd \mathrm{Gal}_{(E,F)}$.

Ahora, supongamos que $\mathrm{Gal}_{(E,K)} \lhd \mathrm{Gal}_{(E,F)}$, como K es campo intermedio, sin pérdida de generalidad, podemos suponer que $E^{\mathrm{Gal}_{(E,K)}} = K$. Sean $\sigma \in \mathrm{Gal}_{(E,F)}$, $\tau \in \mathrm{Gal}_{(E,K)}$ y $\alpha \in K$, como $\mathrm{Gal}_{(E,K)}$ es normal, tenemos que $(\sigma^{-1} \circ \tau \circ \sigma) \in \mathrm{Gal}_{(E,K)}$ y así:

$$\begin{aligned}(\sigma^{-1} \circ \tau \circ \sigma)(\alpha) = \alpha &\Leftrightarrow (\tau \circ \sigma)(\alpha) = \sigma(\alpha) \\ &\Leftrightarrow \tau(\sigma(\alpha)) = \sigma(\alpha) \\ &\Leftrightarrow \sigma(\alpha) \in K \\ &\Rightarrow \sigma(K) \subset K \\ &\Rightarrow \sigma(K) = K\end{aligned}$$

Por lo tanto, todo campo conjugado de K es K y, por el teorema 39, K es extensión de Galois de F.

□

Corolario 19. Sea E una extensión de Galois de F, entonces, $\#\mathrm{Lat}_{(E,F)}$ es finita.

Demostración. Como E es una extensión de Galois de F, entonces, E es finita, así, por el teorema 36, $\mathrm{o}(\mathrm{Gal}_{(E,F)})$ es finito de manera que $\#\mathrm{Sub}(\mathrm{Gal}_{(E,F)})$ es finita y, por el teorema 40, $\#\mathrm{Lat}_{(E,F)}$ es finita.

□

Teorema 41. Sea E una extensión finita de F, entonces, E es una extensión simple si y sólo si $\#\mathrm{Lat}_{(E,F)}$ es finita.

Demostración. Supongamos que E una extensión simple de F, por lo tanto, $\exists\ \alpha \in E$ tal que $E = F(\alpha)$. Como E es una extensión finita, entonces, E es algebraica. Luego, $\exists\ p(x) \in F[x]$ mónico irreducible tal que $p(\alpha) = 0$.

Sean K un campo intermedio y $g(x) = \sum_{i=0}^{m} \beta_i x^i \in K[x]$ mónico irreducible con $\beta_0, \ldots, \beta_m \in K$ tal que $g(\alpha) = 0$. Consideremos el campo intermedio $K' = F(\beta_0, \ldots, \beta_m)$, entonces, $g(x)$ es irreducible en $K'[x]$. De esta manera tenemos que $E = F(\alpha) \subset K'(\alpha) \subset K(\alpha) \subset E$ y por lo tanto, $E = K'(\alpha) = K(\alpha)$, así, $[E : K] = [K(\alpha) : K]$ y $[E : K'] = [K'(\alpha) : K']$.

Como $g(x)$ es irreducible en $K[x]$ y en $K'[x]$, entonces, $[K(\alpha) : K] = m = [K'(\alpha) : K']$ y así, $[E : K] = [E : K']$, por lo tanto, $K = K'$ y para cada $f(x)|p(x)$ el campo intermedio está determinado de manera única. Como $p(x)$ es irreducible, entonces, tiene un número finito de divisores mónicos y así, $\#\mathrm{Lat}_{(E,F)}$ es finita.

Ahora, supongamos que $\#\mathrm{Lat}_{(E,F)}$ es finita. Como E es una extensión finita, es algebraica y por lo tanto existen $\alpha_1, \ldots, \alpha_n \in E$ tales que $E = F(\alpha_1, \ldots, \alpha_n)$. La demostración la haremos por inducción sobre n. Si $n = 1$, entonces, $E = F(\alpha_1)$ y E es una extensión simple, suponemos el resultado válido para $n = k$.

Sea $n = k + 1$, así, $E = F(\alpha_1, \ldots, \alpha_{k+1})$ y tenemos la siguiente cadena de extensiones: $F \subset F(\alpha_1, \ldots, \alpha_k) \subset F(\alpha_1, \ldots, \alpha_{k+1}) = E$. Por hipótesis de inducción, $F(\alpha_1, \ldots, \alpha_k)$ es extensión simple de F, esto es, $\exists\ \beta \in E$ tal que $F(\alpha_1, \ldots, \alpha_k) = F(\beta)$ por lo que $E = F(\beta, \alpha_{k+1})$.

Supongamos que F es infinito, entonces, los elementos β_t son infinitos. Sea $\beta_t = \beta + t(\alpha_{k+1})\ \forall\ t \in F$, así, $F(\beta_t) \subset F(\beta, \alpha_{k+1})$. Como $\#\mathrm{Lat}_{(E,F)}$ es finita, los campos intermedios de la forma $F(\beta_t)$ son finitos, por lo tanto, existen $t, t' \in F$ tales que $t \neq t'$ y $F(\beta_t) = F(\beta_{t'})$, de manera que $(t - t')\alpha_{k+1} = \beta_t - \beta_{t'} \in F(\beta_t) = F(\beta_{t'})$. Ya que $t \neq t'$, entonces, $\alpha_{k+1} \in F(\beta_t)$ y $\beta = \beta_t - t(\alpha_{k+1}) \in F(\beta_t)$. Así, $F(\beta, \alpha_{k+1}) \subset F(\beta_t)$ por lo tanto, $F(\beta, \alpha_{k+1}) = F(\beta_t)$ y $E = F(\beta_t)$, esto es, E es extensión simple de F lo cual concluye la demostración por inducción.

Observación: Para el caso en que F es finito, por hipótesis E es una extensión finita de F, entonces E es un campo finito y F y E tienen la misma característica por lo que E es una extensión simple de F.

□

Corolario 20. Sean E una extensión simple de F y K un campo intermedio, entonces, K es extensión simple de F.

Demostración. Sabemos que $\mathrm{Lat}_{(K,F)} \subset \mathrm{Lat}_{(E,F)}$; por el teorema 41, $\#\mathrm{Lat}_{(E,F)}$ es finita por lo que $\#\mathrm{Lat}_{(K,F)}$ es finita y así, K es extensión simple de F.

□

Teorema 42. (Teorema del elemento primitivo). Sea K una extensión finita separable de F, entonces, K es extensión simple de F.

Demostración. Como K es una extensión finita de F, por el lema 19, existe un campo de descomposición E sobre F para algún $f(x) \in F[x]$ tal que $F \subset K \subset E$.

Como K es una extensión separable de F, entonces, $\forall\ f(x) \in F[x]$, $f(x)$ es separable en $K \subset E$ por lo que $f(x)$ es también separable en E. Como E es un campo de descomposición de $f(x)$, entonces, E es una extensión finita de F y por el teorema 38, $E^{\mathrm{Gal}_{(E,F)}} = F$, por lo tanto, E es extensión de Galois de F.

Por el corolario 19, $\#\mathrm{Lat}_{(E,F)}$ es finita; sabemos que $\mathrm{Lat}_{(K,F)} \subset \mathrm{Lat}_{(E,F)}$, por lo tanto, $\#\mathrm{Lat}_{(K,F)}$ es finita y así, por el teorema 41, K es extensión simple de F.

□

7. Conclusiones

Hemos visto paso a paso una forma de construir la Teoría de Galois partiendo de la definición de grupo. Una parte muy importante en el desarrollo de este trabajo es ver cómo al ir dotando de más elementos y propiedades a una estructura algebraica esta se empieza a comportar de maneras distintas, conservando algunas propiedades y perdiendo otras pero sobre todo nos deja ver (en los últimos teoremas) cómo distintos problemas que en un principio parecen no tener relación alguna entre sí pueden ser solucionados de manera similar al estudiar su estructura algebraica.

Bibliografía

[1] A. Baker, *An Introduction to Galois Theory*, School of Mathematics & Statistics, University of Glasgow, 2011.

[2] I. N. Herstein, *Álgebra moderna: grupos, anillos, campos, teoría de Galois*, Editorial Trillas, 1990.

[3] E. LLuis-Puebla, *Teoría de grupos, un primer curso*, Publicaciones Electrónicas Sociedad Matemática Mexicana, 2006.

[4] E. LLuis-Puebla y F. de María Aceff, *Teoría de Galois, un primer curso*, Publicaciones Electrónicas Sociedad Matemática Mexicana, 2011.