none

A L G E B R A

POR:
FRANCISCO RIVERO

Departamento de Matemáticas
Facultad de Ciencias
Universidad de los Andes
Mérida - Venezuela

Contenido

Introducción

El presente libro contiene el material de Algebra, de un curso de un semestre, para estudiantes de la carrera de Matemáticas o Educación.

El plan de la obra consiste en dar una exposición de las tres estructuras algebraicas fundamentales, como son: los grupos, los anillos y los cuerpos, mediante el estudio de sus propiedades más resaltantes con suficientes ejemplos.

Cada capítulo contiene una buena cantidad de ejercicios, los cuales complementan la teoría y permiten tener un manejo práctico de los conceptos y resultados obtenidos en el texto.

En los capítulos 1-4 se estudian los grupos, comenzando por las definiciones básicas del capítulo 1, en donde se obtiene el teorema de Lagrange, hasta el teorema de la Descomposición para Grupos Abelianos Finitos en el capítulo 4. Se ha incluido un capítulo especial para el grupo de las Permutaciones, dada la importancia del mismo. En este se demuestra la simplicidad del grupo Alternante A_n, para $n \geq 5$.

La teoría de anillos se estudia en los capítulos 5-7. Se definen los anillos más importantes del álgebra conmutativa como son los complejos, los polinomios y las matrices. También se estudian los enteros de Gauss, como un ejemplo de anillo Euclideano. Dentro del capítulo dedicado a los polinomios, se destacan algunos hechos de la teoría clásica, como el estudio de la factorización y el cálculo de las raíces, así como también aspectos más modernos como lo es la condición de Dominio de Factorización Unica.

En el último capítulo se estudian los cuerpos y sus propiedades más importantes. En particular se estudian las extensiones algebraicas de los racionales.

Capítulo

1

Los Números Enteros

1.1 Introducción

En este capítulo nos dedicaremos al estudio de los números enteros los cuales son el punto de partida de toda la teoría de números. Estudiaremos una serie de propiedades básicas de este conjunto, que son fundamentales para el posterior desarrollo de esta materia, como lo son el algoritmo de la división y el teorema de la factorización única.

Advertimos al lector sobre la necesidad de estudiar cuidadosamente el material expuesto en todas estas secciones de este capítulo, antes de pasar a los siguientes.

El enfoque usado en estas notas consiste en exponer inicialmente las propiedades básicas de los enteros, y a partir de éstas, ir deduciendo propiedades más avanzadas, como proposiciones, teoremas,..etc. En ningún momento nos planteamos dar un tratamiento formal y riguroso del tema de los números enteros, cosa que esta fuera del alcance de este curso. Para un estudio completo acerca de la construcción de los enteros a partir de los naturales, ver [**?**].

1.2 Definiciones Básicas

Supondremos que el lector está familiarizado con la notación de conjunto y además maneja los conceptos de pertenencia, inclusión, unión e intersección.

Definición 1.2.1 *Sean A y B dos conjuntos, una* **función de A en** *B, es una ley que asocia a cada elemento a de A, un único elemento b de B.*

Usamos la letra f para indicar la función, o bien el símbolo $f : A \longrightarrow B$. El elemento b se llama la **imagen** de a bajo la función f, y será denotada por $f(a)$.

Definición 1.2.2 *Sea $f : A \longrightarrow B$ una función y E un subconjunto de A, entonces la* **Imagen de E** *bajo f es el conjunto*

$$f(E) = \{b \in B \mid b = f(c), \text{ para algún } c \text{ en } E\}.$$

Es claro que $f(E)$ es un subconjunto de B.

Definición 1.2.3 *Sea $f : A \longrightarrow B$ una función y G es un subconjunto de B, la* **imagen inversa de G** *bajo f es el conjunto*

$$f^{-1}(G) = \{d \in A \mid f(d) \in G\}.$$

Definición 1.2.4 *Una función $f : A \longrightarrow B$ se dice* **Inyectiva** *si para todo b en B, $f^{-1}(\{b\})$ posee a lo sumo un elemento.*

Observación: Otra forma de definir la inyectividad de una función es la siguiente: Si cada vez que tengamos un par de elementos a y b en A, entonces si estos elementos son diferentes, sus imágenes deben ser diferentes.

Ejemplo: La función $F : \mathbb{N} :\longrightarrow \mathbb{N}$, donde $\mathbb{N}$ denota al conjunto de los números naturales, dada por $F(n) = 2n$, es inyectiva. ¿Podría el lector dar una demostración de este hecho?

Definición 1.2.5 *Sea $f : A \longrightarrow B$ una función. Diremos que f es* **Sobreyectiva** *si $f(A) = B$.*

Observación: El conjunto imagen de A, se llama también el **rango de la función**. Luego f es sobreyectiva si su rango es igual al conjunto de llegada.

Ejemplo: La función del ejemplo anterior no es sobreyectiva ¿Porqué?

Ejemplo: Sea $g : \mathbb{N} \longrightarrow \mathbb{N}$ dada por $g(n) = n + 1$. Entonces esta función tampoco es sobreyectiva. Sin embargo si denotamos por $\mathbb{Z}$ al conjunto de los enteros y $G : \mathbb{Z} \longrightarrow \mathbb{Z}$, mediante $G(z) = z + 1$, entonces G si es una función sobreyectiva.

Definición 1.2.6 *Una función $f : A \longrightarrow B$ se dice* **biyectiva** *si f es inyectiva y sobreyectiva.*

Definición 1.2.7 *Sea A un conjunto cualquiera, una* **relación en A**, *es un subconjunto R del producto cartesiano $A \times A$.*

Si el par (a, b) está en R, diremos que a **está relacionado con** b, y lo denotamos por $a \sim b$, ó aRb.

Definición 1.2.8 *Una relación R sobre A, se dice que es de* **equivalencia**, *si satisface las tres condiciones*

1. *Reflexiva*
   $a \sim a$ para todo a en A.

2. *Simétrica*
   $a \sim b$ implica $b \sim a$, para todos a y b en A.

3. *Transitiva*
   Si $a \sim b$ y $b \sim c$, entonces $a \sim c$, para todos a, b y c en A.

Para cada a en A, el conjunto

$$[a] = \{b \in A \mid b \sim a\}$$

se llama **la clase de equivalencia de a**.

Definición 1.2.9 *Una* **operación binaria** *sobre un conjunto A, es una función $g : A \times A \longrightarrow A$.*

La imagen del elemento (a, b) bajo la función g se denota por $a * b$.

Ejemplos de operaciones son la suma y producto de números enteros. También se pueden definir operaciones en forma arbitraria. Por ejemplo, si $\mathbb{N}$ es el conjunto de números naturales, podemos construir la operación

$$* : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$$

$$(a, b) \longrightarrow a * b = ab + 1.$$

1.3 Propiedades de los Enteros

Nosotros supondremos que el lector está familiarizado con el sistema de los números enteros $\ldots -2, -1, 0, 1, 2, 3, \ldots$, el cual denotaremos por $\mathbb{Z}$, así como también, con las propiedades básicas de adición y multiplicación. Podemos dar algunas de estas propiedades como axiomas y deducir otras, a partir de las primeras, como teoremas.

I) **Axiomas de Suma**

Existe una operación binaria en $\mathbb{Z}$, llamada la **suma de enteros**, la cual será denotada por $+$ y satisface :

1. **Cerrada**
   Para a y b números enteros, $a + b$ es un número entero

2. **Conmutativa**
   $a + b = b + a$, para todos a y b enteros .

3. **Asociativa**
   $(a + b) + c = a + (b + c)$, para todos a, b y c enteros.

4. **Elemento neutro**
   Existe un elemento en $\mathbb{Z}$ llamado el cero, el cual se denota por 0, y satisface:
   $$0 + a = a + 0 = a$$
   para todo a entero.

5. **Elemento opuesto**
   Para todo a en $\mathbb{Z}$ existe un elemento, llamado el opuesto de a, el cual denotamos por $-a$, y que satisface:
   $$a + (-a) = -a + a = 0$$

II) **Axiomas de Multiplicación**

Existe una operación binaria en $\mathbb{Z}$, llamada **producto de números enteros**, la cual se denota por $\cdot$, y satisface:

1. **Cerrada**
   Para a y b números enteros, $a \cdot b$ es un número entero

2. **Asociativa**
   Para a, b y c enteros

$$a \cdot (b \cdot c) = (a \cdot b) \cdot c$$

3. **Conmutativa**
   Para a y b enteros

$$a \cdot b = b \cdot a$$

4. **Elemento neutro**
   Existe un entero, llamado el uno y denotado por 1, tal que para todo entero a se tiene

$$1 \cdot a = a \cdot 1 = a$$

III) **Axioma de distributividad**
Para a, b y c enteros se cumple que

$$(a + b) \cdot c = a \cdot c + b \cdot c$$

$$a \cdot (b + c) = a \cdot b + a \cdot c$$

Antes de pasar a ver otros axiomas de los números enteros, como son los axiomas de orden, necesitamos la siguiente definición.

Definición 1.3.1 *Una* **relación de orden** *en un conjunto A, es una relación R sobre A, con las siguientes propiedades:*

1. *Propiedad simétrica*
   Para todo a en A, se verifica aRa.

2. *Propiedad Transitiva*
   Para a, b y c en A se verifica: Si aRb y bRc, entonces aRc

3. *Propiedad antisimétrica*
   Si aRb y bRa entonces $a = b$.

Ejemplo: La relación "Menor o igual que", en el conjunto de los enteros, es ciertamente, una relación de orden. Esto puede ser verificado sin ninguna dificultad por el lector.

A continuación daremos una forma, quizás un poco rigurosa, de introducir esta relación, usando la suma de enteros y la existencia de un conjunto P. (Conjunto de enteros positivos).

IV) **Axiomas de Orden**

Existe un conjunto de enteros, llamados **enteros positivos**, el cual denotaremos por P, y que satisface:

1. Para todos a y b en P, $a+b$ y $a.b$ están en P.
2. 1 está en P.
3. **Ley de tricotomía**
   Para todo entero a se tiene una y sólo una de las siguientes:
   i) a está en P, ii) $-a$ está en P, iii) $a=0$.

Usando los axiomas de orden, se define la siguiente relación en el conjunto de los enteros:

Definición 1.3.2 *Sean a y b dos enteros, diremos que a* **es menor o igual que** *b, y lo denotamos por $a \leq b$, si y sólo si $b-a$ es positivo o cero.*

Definición 1.3.3 *Sean a y b dos enteros, diremos que a* **es menor que** *b, y lo denotamos por $a < b$ si y sólo si $a \leq b$ y $a \neq b$.*

También diremos que: a **es mayor o igual a** b, y lo denotamos por $a \geq b$ si b es menor o igual que a.

Igualmente, diremos que a es **mayor que** b, y se denota por $a > b$, si b es menor que a.

Observación: El conjunto P de enteros positivos es igual al conjunto de los números naturales $\mathbb{N} = \{1, 2, 3, \ldots\}$, como veremos a continuación:

Notemos en primer lugar que 1 está en P (Axioma 2 de orden). Por la primera parte del axioma 1, se sigue que $2 = 1 + 1$, también está en P. De igual manera $3 = 2 + 1$, está en P, ... y así sucesivamente. De esta forma se concluye que el conjunto de los números naturales está en P. ¿Habrán otros elementos en P además de estos? La respuesta a esta pregunta, la podremos obtener como una consecuencia del teorema del mínimo elemento.

1.4 Axioma del Elemento Mínimo

Los axiomas estudiados hasta ahora no son suficientes para caracterizar el conjunto de los números enteros, en el sentido de determinar, sin ningún tipo de duda, todas y cada una de sus propiedades. A manera de ejemplo, la propiedad de infinitud de los enteros, no se puede derivar de ninguno de los axiomas o propiedades antes vistas. De aquí se concluye que es necesario incluir más axiomas, si se quiere tener un sistema completo, suficientemente bueno como para deducir, esta y otras propiedades que caracterizan a los enteros.

Definición 1.4.1 *Sea A un conjunto no vacío de $\mathbb{Z}$, entonces diremos que un entero a es una* **cota superior** *para A, si se cumple:*

$$n \leq a, \text{ para todo } n \text{ en } A \ .$$

Definición 1.4.2 *Diremos que un conjunto A está* **acotado superiormente***, si A posee una cota superior.*

Definición 1.4.3 *Sea A un conjunto no vacío de $\mathbb{Z}$. Un elemento a del conjunto A se dice* **elemento maximal** *, si $n \leq a$ para todo n en A.*

Observación: La diferencia entre las definiciones **??** y **??** radica en lo siguiente: Un conjunto A de enteros puede tener una cota superior a, pero, posiblemente a no es un elemento del conjunto A, por tanto a no es un elemento maximal.

Definición 1.4.4 *Sea A un conjunto no vacío de $\mathbb{Z}$. Un entero b se llama* **cota inferior** *para el conjunto A, si se cumple:*

$$b \leq x, \text{ para todo } x \text{ en } A$$

Definición 1.4.5 *Sea A un conjunto no vacío de $\mathbb{Z}$. Un elemento a de A se llama* **elemento minimal***(o elemento mínimo), si satisface:*

$$a \leq x, \text{ para todo } x \text{ en } A \ .$$

La misma observación que hicimos para el elemento maximal, se aplica al elemento minimal.

Axioma del mínimo elemento

Todo conjunto no vacío de números enteros positivos, posee un elemento minimal.

El axioma del mínimo elemento, es equivalente a otro axioma, llamado Principio de Inducción, el cual damos a continuación:

Principio de Inducción

Sea $P(n)$ una proposición que depende de un entero positivo n, y supongamos que:

1. $P(1)$ es cierta.
2. Si $P(k)$ es cierta, para un entero k, entonces $P(k+1)$ también es cierta.

Luego $P(n)$ es cierta para todo entero positivo n.

A partir del principio de inducción es posible probar una gran cantidad de fórmulas o identidades, que involucran un número positivo n.

Ejemplo: Probar la fórmula:

$$1 + 2 + 3 + \ldots + n = \frac{n(n+1)}{2} \tag{1.1}$$

Demostración:

A fin de utilizar el principio de inducción, haremos una proposición que depende de n, y la llamaremos $P(n)$. Luego probaremos que esta proposición satisface las condiciones 1) y 2) del principio, con lo cual se estará verificando para todo n. Por lo tanto hacemos:

$$\text{P(n)} = \text{“la fórmula (}\mathbf{??}\text{) vale para todo } n\text{”}.$$

Notemos en primer lugar, que $P(1)$ se reduce a afirmar lo siguiente:

$$1 = \frac{1(1+1)}{2}$$

lo cual es evidentemente cierto.

Sea ahora, k un entero y supóngase que $P(k)$ es cierto, esto es:

$$1 + 2 + 3 + \ldots + k = \frac{k(k+1)}{2}.$$

Partiendo de esta ecuación, y sumando $k + 1$ a ambos lados, se tiene

$$1 + 2 + 3 + \ldots + k + (k+1) = \frac{k(k+1)}{2} + (k+1)$$

Luego podemos sumar los dos términos en el lado derecho de la ecuación para obtener:

$$1 + 2 + 3 + \ldots + k + (k+1) = \frac{(k+1)(k+2)}{2}$$

Vemos entonces que esta última fórmula es igual a (**??**), con $n = k + 1$. Por lo tanto $P(k+1)$ es cierto, si se asume que $P(k)$ es cierto. Esto, unido a la veracidad de P(1), nos permite afirmar la validez de $P(n)$ para todo n.

♠

Ejemplo: Consideremos el **triángulo de Pascal:**

$$
\begin{array}{ccccccccc}
 & & & & 1 & & & & \\
 & & & 1 & & 1 & & & \\
 & & 1 & & 2 & & 1 & & \\
 & 1 & & 3 & & 3 & & 1 & \\
1 & & 4 & & 6 & & 4 & & 1 \\
 & & & & \ldots & & & &
\end{array}
$$

donde todos los elementos situados sobre los lados oblicuos son iguales a uno, y cada elemento interior es igual a la suma de los dos elementos adyacentes sobre la fila anterior.

Podemos denotar por $C(n, r)$ al elemento del triángulo de Pascal situado en la fila n y en la posición r (dentro de esta fila).

Luego se tendrá

$$C(0,0) = 1$$

$$C(1,0) = 1, \quad C(1,1) = 1$$

$$C(2,0) = 1, \quad C(2,1) = 2, \quad C(2,2) = 1$$

$$\ldots$$

y así sucesivamente.

En general se tiene la fórmula

$$C(n, r) = C(n-1, r-1) + C(n-1, r)$$

Este tipo de fórmula, en donde un elemento se define en función de los anteriores se llama **fórmula de recurrencia**. La posibilidad de definir elementos enteros mediante esta técnica de la recurrencia se debe al principio de inducción, ver [**?**].

Existe otra forma de expresar los coeficientes del triángulo de Pascal, explícitamente en función de n, la cual probaremos usando inducción. Más precisamente:

Proposición 1.4.1 *Si n es un entero positivo, entonces se tiene*

$$C(n,r) = \frac{n!}{(n-r)!\ r!} \qquad 0 \leq r \leq n. \tag{1.2}$$

Demostración:

Denotaremos por $P(n)$ la proposición (**??**), y probaremos que $P(n)$ es cierta para todo n, usando el principio de inducción.

El primer paso de la inducción corresponde a $n = 0$, lo cual nos da:

$$1 = C(0,0) = \frac{0!}{(0-0)!\ 0!}$$

siendo esto cierto, se tiene que $P(0)$ es cierto.

Sea n un entero positivo cualquiera, y supongamos que la relación (**??**) sea cierta. Luego debemos probar $P(n+1)$:

$$C(n+1,r) = \frac{(n+1)!}{(n+1-r)!\ r!} \qquad 0 \leq r \leq n+1$$

Sea r entero positivo, $0 < r < n+1$. Luego usando la fórmula de recurrencia para $C(n+1,r)$ se obtiene:

$$\begin{aligned} C(n+1,r) &= C(n,r) + C(n,r-1) \\ &= \frac{n!}{(n-r)!r!} + \frac{n!}{(n-r+1)!\ (r-1)!} \\ &= \frac{(r+1)!}{(n+1-r)!\ r!} \end{aligned}$$

Si $r = 0$, se tiene:

$$C(n+1,0) = 1 = \frac{(n+1)!}{(n+1-0)!\ 0!}$$

Si $r = n+1$ se tiene:

$$C(n+1,n+1) = 1 = \frac{(n+1)!}{((n+1)-(n+1))!\ (n+1)!}$$

Por lo tanto, hemos demostrado la veracidad de $P(n+1)$, a partir de la veracidad de $P(n)$. Luego la fórmula (**??**) es cierta para todo n. ♠

Observación: Los números $C(n,r)$ son los coeficientes de la expansión del binomio $(x+y)^n$ y por ello se les llama **coeficientes binomiales**

Ejercicios

1) (Binomio de Newton) Sean x e y números reales cualesquiera y sea n un entero positivo. Probar

$$(x+y)^n = \sum_{r=1}^{n} \left(\begin{array}{c} n \\ r \end{array} \right) x^{n-r} y^r$$

2) La **sucesión de Fibonacci**. La sucesión a_n definida por recurrencia $a_0 = 0$, $a_1 = 1 \ldots, a_{n+1} = a_n + a_{n-1}$, se denomina sucesión de Fibonacci. Demostrar, usando inducción sobre n, que el término general de esta sucesión viene dado por:

$$a_n = \frac{1}{\sqrt{5}} \left(\frac{1+\sqrt{5}}{2} \right)^n - \frac{1}{\sqrt{5}} \left(\frac{1-\sqrt{5}}{2} \right)^n$$

3) **El Número de Oro:**

El número $\varphi = (\frac{1+\sqrt{5}}{2})$ que aparece en la sucesión de Fibonacci, se llama el Número de Oro y posee propiedades muy interesantes. Este se obtiene como el cociente de los lados del rectángulo de lados a y b, tal que es proporcional al rectángulo de lados b, $a+b$. Esto es

$$\frac{b}{a} = \frac{a+b}{b}$$

Probar que el radio $\dfrac{b}{a}$ es igual a φ.

4) Si a_n es el término enésimo de la sucesión de Fibonacci, probar

$$\lim_{n\to\infty} \frac{a_{n+1}}{a_n} = \varphi$$

5) Usando el principio de inducción, probar las fórmulas

1. $1 + 2^2 + 3^2 + \ldots + n^2 = \dfrac{n(n+1)(2n+1)}{6}$
2. $1 + 3 + 5 + 7 + \ldots + 2n - 1 = n^2$
3. $1 + 2 + 2^2 + 2^3 + \ldots + 2^{n-1} = 2^n - 1$

6) Probar

$$\left(\begin{array}{c} n \\ 0 \end{array}\right) + \left(\begin{array}{c} n \\ 1 \end{array}\right) + \cdots + \left(\begin{array}{c} n \\ n \end{array}\right) = 2^n$$

7) Probar

$$\left(\begin{array}{c} n \\ 0 \end{array}\right)^2 + \left(\begin{array}{c} n \\ 1 \end{array}\right)^2 + \cdots + \left(\begin{array}{c} n \\ n \end{array}\right)^2 = \left(\begin{array}{c} 2n \\ n \end{array}\right)$$

8) Probar que no existe un número entero x con la propiedad:

$$0 < x < 1.$$

Ayuda: Suponiendo que tal x exista, consideremos el conjunto de enteros positivos $\{x, x^2, \ldots\}$, el cual es distinto del vacío y no tiene elemento minimal. Esto contradice el axioma del mínimo elemento.

9) Usando el ejercicio anterior, probar que si n es un número entero cualquiera, entonces no existe entero x con la propiedad:

$$n < x < n + 1$$

10) Probar el principio de inducción a partir del principio del mínimo elemento.

11) Probar que el conjunto de los números enteros no está acotado superiormente.

12) Probar que en $\mathbb{Z}$ valen las dos leyes de cancelación, es decir, para todo a, b y c en $\mathbb{Z}$, con $a \neq 0$, se tiene

$$ab = ac \Longrightarrow b = c$$

$$ba = ca \Longrightarrow b = c$$

13) Probar que si a y b son dos enteros diferentes de cero, entonces

$$ab = 0 \Longrightarrow a = 0 \quad \text{ó} \quad b = 0$$

14) Demuestre que no existe un entero $a \neq 0$, con la propiedad.

$$a + x = x,$$

para todo x entero.

15) Probar que toda función inyectiva $f : A \to A$, donde A es conjunto finito, es sobre.

16) Demuestre que cualquier elemento $a \in \mathbb{Z}$ satisface:
i) $a^m.a^n = a^{m+n}$
ii) $(a^n)^m = a^{nm}$,
para todos m y n enteros.

17) Una **partición** en un conjunto A, es una familia de subconjuntos $\{A_i\}$ de A, tales que.
i) $A_i \cap A_j \neq \emptyset$, para $i \neq j$.
ii) $\bigcup_{i \geq 1} A_i = A$.

Probar que toda relación de equivalencia en A determina una partición

18) Demuestre que cualquier conjunto de números enteros acotado superiormente posee un máximo.

19) Demuestre que si a es un entero positivo y b es un entero negativo, entonces ab es negativo.

20) Demuestre que si a y b son impares, entonces su producto es un número impar.

1.5 Máximo Común Divisor

En esta sección estudiaremos el famoso teorema de la división de los números enteros, y algunos resultados importantes que se derivan del mismo.

Teorema 1.5.1 *Sea a un entero positivo, y b un entero arbitrario. Entonces existen enteros p y q, únicos, tales que*

$$b = qa + r, \quad 0 \leq r < a.$$

El entero q se llama el **cociente** *y r se llama el* **resto**

Demostración:

Primero, probaremos que q y r existen, y posteriormente, probaremos que ellos son únicos.

En primer lugar, si $b = 0$, tomamos $q = r = 0$.

Sea b distinto de cero y consideremos el conjunto

$$D = \{b - ua \mid u \text{ es un entero}\}$$

Este conjunto contiene enteros positivos, pues si $b > 0$, basta tomar $u = 0$.

Si por el contrario $b < 0$, hacer $u = b$, con lo cual $b - ba > 0$, y $b - ba \in D$.

Por lo tanto el conjunto D^+, de elementos no negativos de D es diferente del vacío.

Por el axioma del mínimo elemento, este conjunto posee un elemento minimal r el cual pertenece a D^+.

Así pues, existe un entero q, tal que

$$r = b - qa,$$

o bien

$$b = qa + r, \quad 0 \leq r.$$

Si suponemos $r \geq a$, se tiene $r - a \geq 0$ y por lo tanto

$$b - qa - a = b - (q + 1)a \geq 0.$$

Esto es,

$$b - (q+1)a \in D^+$$

y

$$b - (q+1)a < r,$$

lo cual contradice la minimalidad del elemento r. Luego se debe tener $r < a$.

Unicidad:

Supongamos que existen otro par de enteros q' y r' los cuales satisfacen

$$b = q'a + r', \quad 0 \leq r' < a.$$

Probaremos que $q = q'$, para lo cual supondremos que $q' > q$. Luego se tiene

$$0 = b - b = (q'a + r') - (qa + r) = (q' - q)a - (r - r'),$$

de donde se obtiene

$$(q' - q)a = r - r' \geq a.$$

lo cual es una contradicción, pues $r - r' < a$. Similarmente si suponemos $q > q'$ llegamos a la misma contradicción. Por lo tanto, se debe tener $q = q'$, y de esto se sigue $r = r'$.

♠

Definición 1.5.1 *Sea a un entero positivo, y b un entero cualquiera. Diremos que a* **divide a** *b, y lo denotamos por $a \mid b$, si existe otro entero c tal que $b = ac$.*

También se dice que b **es divisible por** a, o bien a **es un divisor de** b. El concepto de divisibilidad es uno de los más importantes en toda la teoría de números. Uno de los problemas aún no resueltos, consiste en hallar todos los divisores de un número cualquiera dado.

Algunas de las propiedades básicas de la divisibilidad, se exponen en la siguiente proposición.

Proposición 1.5.1 *Sean a, b y c enteros distintos de cero. Entonces*

1. $1 \mid a$
2. $a \mid 0$
3. $a \mid a$
4. *Si* $a \mid b$ *y* $b \mid c$, *entonces* $a \mid c$.
5. *Si* $a \mid b$ *y* $a \mid c$, *entonces* $a \mid bx + cy$, *para todo par de enteros* x *e* y.

Demostración:
Ejercicio. ♠

Definición 1.5.2 *Sean* a *y* b *dos enteros positivos. Un entero positivo* d, *se dice* **Máximo Común Divisor** *entre* a *y* b, *si y sólo si satisface*

1. $d \mid a$ *y* $d \mid b$
2. *Si* c *es otro entero positivo con la condición :*

$$c \mid a \quad \text{y} \quad c \mid b, \quad \text{entonces} \quad c \mid d.$$

El entero positivo d, se denota por $d = (a, b)$. De acuerdo a la definición, se tiene que el Máximo Común Divisor d, es el mayor de los divisores comunes de a y b.

Ejemplo: Hallar el Máximo Común Divisor entre 12 y 18.
En primer lugar, buscamos por tanteo, todos los divisores comunes de ambos números

Divisores de 12 : 1, 2, 3, 4, 6 y 12.
Divisores de 18 : 1, 2, 3, 6, 9 y 18.

Es evidente que el mayor divisor común es 6, y por lo tanto concluimos

$$(12, 18) = 6.$$

Existe un método práctico para calcular el Máximo Común Divisor entre dos números, el cual está basado en el algoritmo de división. Este método, llamado **Método de Euclides para el M.C.D.** consiste en una serie de divisiones sucesivas y, el Máximo Común Divisor se obtiene como uno de los restos en el proceso de división. Además de dar una forma constructiva de calcular el M.C.D., permite al mismo tiempo dar una demostración de la existencia de éste.

Teorema 1.5.2 Método de Euclides

Dados dos enteros positivos a y b, el Máximo Común Divisor entre ellos, $d = (a, b)$, siempre existe.

Demostración:

Podemos suponer, sin pérdida de generalidad que $b > a > 0$. Luego por el teorema de división, existen enteros q_1 y r_1 tales que

$$b = q_1 a + r_1, \quad 0 \leq r_1 < a.$$

Si $r_1 = 0$, entonces $b = q_1 a$ y por lo tanto $(b, a) = a$, con lo cual queda demostrado el teorema.

Si $r \neq 0$, podemos aplicar de nuevo el teorema de la división, para obtener un par de enteros q_2, r_2 tales que

$$a = q_2 r_1 + r_2, \quad 0 \leq r_2 < r_1$$

Continuando de esta manera, se obtiene una sucesión de enteros positivos decrecientes: $r_1 > r_2 > \ldots > 0$. Es evidente que esta sucesión es finita y por lo tanto existe n, tal que $r_n \neq 0$ y $r_{n+1} = 0$. Luego existen enteros $q_1, q_2, \ldots q_{n+1}, r_1, r_2, \ldots, r_n$ que cumplen las relaciones:

$$\begin{aligned} b &= aq_1 + r_1, \quad 0 < r_1 < b \\ a &= r_1q_2 + r_2, \quad 0 < r_2 < r_1 \\ r_1 &= r_2q_3 + r_3, \quad 0 < r_3 < r_2 \\ &\vdots \\ r_{n-2} &= r_{n-1}q_n + r_n, \quad 0 < r_n < r_{n-1} \\ r_{n-1} &= r_nq_{n+1} \end{aligned}$$

Afirmamos que $(a, b) = r_n$.

En primer lugar, notemos que de la última ecuación se tiene que r_n divide a r_{n-1} . Por lo tanto, $r_n \mid (r_{n-1}q_n + r_n)$, es decir r_n divide a r_{n-2}. Continuando de esta manera, llegamos finalmente, a que r_n divide a todos los demás r_i . En particular

$$r_n \mid r_1 \quad y \quad r_n \mid r_2, \quad \text{implica que} \quad r_n \mid r_1q_2 + r_2$$

luego $r_n \mid a$.

Igualmente, usando $r_n \mid a$ y $r_n \mid r_1$ se deduce $r_n \mid b$.

Finalmente, si c es un entero positivo que divide a a y a b, se tiene

$$c \mid b - aq_1,$$

o sea, $c \mid r_1$. Continuando de esta manera, se tiene que $c \mid r_i$ para todo i y por tanto $c \mid r_n$.

Con esto hemos demostrado las dos condiciones de la definición de Máximo Común Divisor para r_n y por lo tanto $(a, b) = r_n$.

♠

Ejemplo: Podemos calcular el Máximo Común Divisor entre 672 y 38, usando el método anterior, para lo cual haremos las divisiones correspondientes. Luego

$$672 = 17 \cdot 38 + 26$$

$$38 = 1 \cdot 26 + 12$$

$$26 = 2 \cdot 12 + 2$$
$$12 = 6 \cdot 2$$

El último resto diferente de cero es 2, luego $(672, 38) = 2$.

En la demostración del teorema anterior, obtuvimos las ecuaciones

$$\begin{aligned} r_1 &= b - aq_1 \\ r_2 &= a - r_1 q_2 \\ &\vdots \\ r_{n-1} &= r_{n-3} - r_{n-2} q_{n-1} \\ r_n &= r_{n-2} - r_{n-1} q_n \end{aligned}$$

Observamos que el Máximo Común Divisor entre a y b, dado por r_n viene expresado en función de r_{n-2} y r_{n-1}. Ahora bien, en la penúltima ecuación se puede reemplazar r_{n-1} en función de r_{n-2} y r_{n-3}. Continuando de esta forma, podemos ir sustituyendo los valores de r_i en función de los anteriores, hasta que tengamos r_n en función de a y b. Así pues hemos demostrado el siguiente resultado:

Teorema 1.5.3 *El Máximo Común Divisor entre dos enteros a y b, se expresa como combinación lineal de a y b. Es decir, existen enteros x e y tales que*

$$(a, b) = ax + by$$

Ejemplo: Podemos expresar el Máximo Común Divisor entre 672 y 38 como combinación lineal de ambos, para lo cual usamos las cuatro ecuaciones del ejemplo anterior.

$$\begin{aligned} 2 &= 26 - 2 \cdot 12 \\ 2 &= 26 - 2 \cdot (38 - 26) \\ 2 &= 3 \cdot 26 - 2 \cdot 38 \\ 2 &= 3 \cdot (672 - 17 \cdot 38) - 2 \cdot 38 \\ 2 &= 3 \cdot 672 - 53 \cdot 38 \end{aligned}$$

Una de las aplicaciones de mayor utilidad que ofrece el teorema de la división, es la representacion de cualquier número mediante combinación lineal de potencias de 10.

Teorema 1.5.4 *Si b es un entero positivo, entonces existen enteros únicos $r_0, r_1, \ldots, r_n$ tales que*

$$b = r_n 10^n + r_{n-1} 10^{n-1} + \ldots + r_1 10 + r_0$$

con $0 \leq r_i < 10$ para todo i.

Demostración:

Usaremos inducción sobre b. Si $b = 1$ es cierto. Supongamos el resultado cierto para todo entero menor que b, y probaremos la afirmación para b. Podemos dividir b entre 10 para obtener enteros únicos q y r_0 tales que

$$b = q \cdot 10 + r_0, \quad 0 \leq r_0 < 10$$

Como q es menor que b, aplicamos la hipótesis de inducción a q. Luego existen enteros únicos $r_1, r_2, \ldots, r_n$, con $0 \leq r_i < 10$, tales que

$$q = r_n 10^{n-1} + \ldots + r_2 10 + r_1$$

Por lo tanto

$$b = (r_1 + r_2 10 + \ldots + r_n 10^{n-1})10 + r_0$$

$$= r_n 10^n + \ldots + r_1 10 + r_0$$

Es claro que todos los r_i son únicos. Con esto termina la demostración.

♠

Definición 1.5.3 *Dos enteros positivos a y b, se dicen* **primos relativos** *si el Máximo Común Divisor entre ellos es uno.*

Ejemplo: Los enteros 20 y 9 son primos relativos, pues $(20, 9) = 1$. Nótese que 20 y 9 no son números primos.

El siguiente resultado, que caracteriza las parejas de enteros primos relativos, será de mucha utilidad en el futuro:

Teorema 1.5.5 *Dos enteros positivos a y b son primos relativos, si y sólo si existen enteros x e y tales que*

$$ax + by = 1$$

Demostración:

Es claro que existen enteros x e y, tal que

$$ax + by = 1$$

pues 1 es el Máximo Común Divisor entre a y b.

Por otro lado, si suponemos $ax + by = 1$, para algunos enteros x e y, podemos probar $(a, b) = 1$. En efecto, si c es un divisor de a y b, se tendrá que c divide a $ax + by$, o sea c divide a 1. Luego $c = 1$, y por lo tanto el Máximo Común Divisor entre a y b es 1.

♠

Definición 1.5.4 *Sean a y b dos enteros positivos, el* **mínimo común múltiplo** *entre a y b, es otro entero positivo c, el cual satisface:*

1. *$a \mid c$ y $b \mid c$*
2. *Si e es otro entero, tal que $a \mid e$ y $b \mid e$, se tiene $c \mid e$.*

De la definición anterior se sigue que c es el menor múltiplo común entre a y b.

Usaremos la notación :

$$[a, b] = \text{mínimo común múltiplo entre } a \text{ y } b.$$

Proposición 1.5.2 *Sean a, b, y c tres enteros positivos, tales que $(a, b) = 1$ y $a \mid bc$. Luego $a \mid c$.*

Demostración:

Por el teorema anterior, existen enteros x e y tales que

$$ax + by = 1$$

Multiplicando por c tenemos

$$cax + cby = c$$

Por hipótesis, sabemos que $a \mid bc$, luego $a \mid cby$. También se tiene $a \mid cax$, y por lo tanto concluimos

$$a \mid cax + cby$$

lo cual implica que $a \mid c$.

♠

Para finalizar esta sección, daremos una serie de propiedades fundamentales del Máximo Común Divisor:

Proposición 1.5.3 *Sean a, b y c enteros positivos. Entonces*

1. *Si m es otro entero tal que $m \mid a$ y $m \mid b$ se tiene*

$$\left(\frac{a}{m}, \frac{b}{m}\right) = \frac{(a,b)}{m}$$

2. *Si n es cualquier entero*

$$(na, nb) = n(a, b)$$

3. *Si $(a, b) = d$, entonces*

$$\left(\frac{a}{d}, \frac{b}{d}\right) = 1$$

4. *Si x es cualquier entero, entonces*

$$(b, a + bx) = (a, b)$$

Demostración:
1) Sea $d = (a, b)$, y probaremos

$$\left(\frac{a}{m}, \frac{b}{m}\right) = \frac{d}{m}$$

Notemos en primer lugar que d/m es un entero. En efecto se tiene $ax + by = d$, y por lo tanto

$$\frac{a}{m}x + \frac{b}{m}y = \frac{d}{m}$$

en el lado izquierdo de la ecuación tenemos un entero, luego d/m es entero.

Por otra parte, como d divide a a, se tiene que d/m divide a a/m. Igualmente se tendrá que d/m divide a b/m.

Finalmente, si c es otro entero que divide a a/m y b/m, se tendrá

$$\frac{a}{m} = cj \quad y \quad \frac{b}{m} = ck$$

para algunos enteros j y k.

Multiplicando ambas ecuaciones por m nos da

$$a = mcj \quad y \quad b = mck$$

de donde obtenemos

$$mc \mid a \quad y \quad mc \mid b$$

Usando la definición de Máximo Común Divisor para d, se tiene que d divide a mc, y por lo tanto d/m divide a c.

Así pues, hemos probado 1).

2) Usando 1) se tiene

$$(a, b) = \left(\frac{an}{n}, \frac{bn}{n}\right) = \frac{(an, bn)}{n}$$

luego

$$n(a, b) = (an, bn)$$

3) Usar 1) con $m = (a, b)$.

4) Observar que $(a, b) \mid a$ y $(a, b) \mid b$. Luego $(a, b) \mid ax + b$.
Si c es un entero que divide tanto a b como a $a + bx$, se tendrá

$$c \mid ((a + bx) - bx)$$

y en consecuencia $c \mid a$.

Luego c divide al máximo común divisor entre a y b, el cual es d. Así pues, hemos probado $(b, a + bx) = (a, b) = d$.

♠

Ejemplo:

$$(200, 300) = (2, 3)100 = 100.$$

Ejercicios

1) Usando el algoritmo de Euclides, hallar
a) (122,648)
b) (715,680)
c) (1581,206)
d) (3742, 843)
e) (120, 560)
f) (458, 1290).

2) Demuestre que si $(a, b) = 1$, entonces:

$$(a - b, a + b) = 1, \quad \text{ó} \quad 2.$$

3) Demuestre que si $ax + by = m$, entonces $(a, b) \mid m$.

4) Demuestre que si $(b, c) = 1$, entonces para todo entero positivo a, se tiene $(a, bc) = (a, b)(a, c)$.

5) El Máximo Común Divisor para tres números enteros positivos a, b y c, denotado por (a, b, c) se define como el entero positivo d que satisface:

1. $d \mid a, \quad d \mid b, \quad y \quad d \mid c$

2. Si f es otro entero tal que $f \mid a$, $f \mid b$ y $f \mid c$ entonces $f \mid d$.

Probar que $(a, b, c) = ((a, b), c) = (a, (b, c))$.

6) Hallar el Máximo Común Divisor de
   a) (23,12,18)
   b) (90, 80, 56)
   c) (65, 20, 190).

7) Hallar una solución en números enteros de la ecuación

$$21x + 25y = 1$$

8) Probar que el mínimo común múltiplo entre dos enteros a y b siempre existe.

9) Demostrar la fórmula

$$[a, b] = \frac{ab}{(a, b)}$$

10) Usando la fórmula anterior, calcular
   a) [12,28]
   b) [120,50]
   c) [34,62]
   d) [88, 340].

1.6 Teorema de Factorización Unica

Definición 1.6.1 *Un entero positivo p, distinto de 1, se dice que es* **primo** *si los únicos divisores de p son 1 y p.*

Ejemplo: Los números 2, 3, 19 son primos.

Los números enteros positivos que no son primos, se les llama **compuestos**, como por ejemplo 6. Es decir, todo número compuesto es de la forma

$$m = m_1 m_2,$$

donde $1 < m_1 < m$ y $1 < m_2 < m$.

Los números primos y su distribución dentro de los números enteros, han sido estudiados desde la antigüedad. Ellos han ejercido una atracción fascinante sobre los matemáticos, debido a la forma tan irregular como aparecen en la sucesión de los enteros. Muchos matemáticos han tratado en vano de hallar una fórmula que genere exclusivamente números primos. Así por ejemplo, Pierre Fermat conjeturó que todo número de la forma

$$s(n) = 2^{2^n} + 1$$

era primo. Esto lo comprobó para n= 1,2,3 y 4. Sin embargo en 1732 Leonhard Euler demostró que $s(5)$ no era primo.

Existe una gran cantidad de problemas, aún no resueltos, sobre los números primos. Algunos de ellos serán tratados en las próximas secciones.

El método más elemental para hallar la sucesión de los primos, es el llamado **Criba de Eratóstenes**. Este consiste en colocar los números enteros positivos en orden creciente, formando diez columnas de la siguiente forma

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30

.....

Entonces comenzamos por eliminar de la lista todos los números pares, luego los múltiplos de tres, luego los de cinco, ... y así sucesivamente, hasta agotar todos los números compuestos. Es evidente que los restantes números en la lista serán todos los números primos.

Teorema 1.6.1 *Todo número entero positivo, mayor que uno, puede ser factorizado como un producto de números primos.*

Demostración:

Sea m el número en cuestión. Usaremos inducción sobre m, para probar la proposición "m puede ser factorizado como un producto de primos".

En primer lugar, la proposición es cierta para $m = 2$, pues 2 mismo es un número primo. Supóngase la veracidad de la proposición, para todo número menor que un cierto k, es decir, todo número menor que k y mayor o igual a dos, puede ser factorizado como producto de primos.

Consideremos ahora k. Si k es primo, entonces no hay nada que probar y el resultado será cierto para k. Si por el contrario, k resulta ser compuesto, entonces tenemos

$$k = m_1 m_2$$

donde $2 \leq m_1 < k$ y $2 \leq m_2 < k$.

Podemos entonces aplicar la hipótesis de inducción, tanto a m_1 como a m_2, es decir cada uno de ellos se factoriza como un producto de primos. Luego

$$m_1 = p_1 p_2 \dots p_s$$

$$m_2 = q_1 q_2 \dots q_t$$

donde los p_i, q_j son números primos.

Por lo tanto tenemos

$$k = m_1 m_2 = p_1 p_2 \dots p_s q_1 q_2 \dots q_t$$

esto es, un producto de primos.

♠

Observación: Es posible tener algunos primos repetidos en la factorización de un número compuesto. Por ejemplo $24 = 2.2.2.3$. En todo caso, podemos agrupar aquellos primos iguales usando potenciación. Esto es todo entero positivo n puede ser escrito de la forma

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s} \tag{1.3}$$

donde los p_i son todos primos diferentes y los α_i son mayores o iguales a uno.

La siguiente proposición es fundamental para la demostración del teorema de factorización única.

Proposición 1.6.1 *Sean $p, p_1, p_2, , \ldots p_n$ números primos, tales que $p \mid p_1.p_2 \ldots p_n$. Entonces $p = p_i$ para algún i.*

Demostración:

Usaremos inducción sobre n.

Para $n = 1$, el resultado es cierto. Supongamos que p es distinto de p_1, entonces tenemos

$$(p, p_1) = 1 \quad y \quad p \mid p_1(p_2 p_3 \ldots p_n)$$

Luego por la proposición 2 se obtiene

$$p \mid p_2.p_3 \ldots p_n$$

Usando la hipótesis de inducción, se concluye que $p = p_i$ para algún i.

♠

Teorema 1.6.2 *Todo número entero positivo n, tiene una factorización única de la forma*

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_s^{\alpha_s}$$

Demostración:

Supongamos que n tiene dos factorizaciones distintas

$$n = p_1^{\alpha_1} \ldots p_s^{\alpha_s} = q_1^{\beta_1} \ldots q_t^{\beta_t} \tag{1.4}$$

Probaremos en primer lugar que $s = t$ y posteriormente probaremos que para todo i, con $1 \leq i \leq s$, se tiene

$$p_i = q_j, \quad \text{para algún} \quad j \ \text{ y } \quad \alpha_i = \beta_j.$$

Usaremos inducción sobre n. Si $n = 1$, entonces la tesis del teorema se cumple.

Supongamos que el teorema es cierto para todo entero positivo k, con $k < n$ y probemos el resultado para n.

Sea entonces n como en (1.4). Notemos que p_1 divide al producto de primos $q_1^{\beta_1} \dots q_t^{\beta_t}$, luego por el lema anterior p_1 debe ser igual a alguno de ellos, digamos q_i. Podemos entonces cancelar p_1 en ambos lados de (**??**), con lo cual tendremos que n/p_1 posee dos factorizaciones. Si se aplica entonces la hipótesis de inducción se obtiene el resultado.

♠

Uno de los primeros resultados acerca de los números primos, y que aparece demostrado en *Los Elementos* de Euclides, es el siguiente.

Teorema 1.6.3 *Existen infinitos números primos.*

Demostración:

Supóngase que hay solamente un número finito de primos, digamos $p_1, p_2, \dots, p_n$. Entonces el número

$$x = p_1 p_2 \dots p_n + 1$$

puede ser factorizado como producto de primos.

Sin embargo, ningún primo p_i, de los antes mencionados, puede estar entre los factores de x, pues p_i no divide a x; ¿Por qué?

♠

Ejercicios

1) Hallar la descomposición en factores primos de
   a) 165
   b) 670
   c) 124
   d) 1567
   e) 444.

2) Por medio de la Criba de Eratóstenes, hallar todos los primos menores que 200.

3) Probar que si n no es primo, entonces n tiene un divisor primo, el cual es menor o igual a $\sqrt{n}$.

4) Usando el resultado anterior, implemente un algoritmo de computación para determinar cuándo un número es primo.

5) Determine cuáles de los siguientes números son primos:
   a) 941
   b) 1009
   c) 1123
   d) 1111
   e) 671
   f) 821.

6) Algunos primos son de la forma $4k + 1$, como por ejemplo, 5, 17, 101, ... etc. Probar que hay infinitud de ellos.

7) Demostrar que $2^{524} - 1$ no es primo.

8) Sea

$$a = p_1^{\alpha_1} \dots p_n^{\alpha_n}$$

y

$$b = p_1^{\beta_1} \dots p_n^{\beta_n},$$

entonces probar

$$(a, b) = p_1^{\delta_1} \dots p_n^{\delta_n}$$

donde $\delta_i = min\{\alpha_i, \beta_i\}$.

$$[a, b] = p_1^{\gamma_i} \dots p_n^{\gamma_n}$$

donde $\gamma_i = max\{\alpha_i, \beta_i\}$

9) Use el ejercicio anterior para hallar
   a) $(240, 45)$
   b) $[240, 45]$.
   c) $[1650, 7800]$
   d) $[235, 7655]$

10) Probar que $\sqrt{5}$ es un número irracional.

Capítulo

2

Grupos

2.1 Introducción

La estructura de grupo es una de las más comunes en toda la matemática pues aparece en forma natural en muchas situaciones, donde se puede definir una operación sobre un conjunto. Por ser tan simple en su definición, el concepto de grupo se puede considerar como punto de partida para el estudio de otras estructuras algebraicas más complicadas, como son los cuerpos y los anillos.

Muchos objetos matemáticos provenientes de áreas tan disímiles como la Geometría Analítica, la Combinatoria, el Análisis Complejo, la Topología, etc, tienen incorporados la estructura de grupo, aunque esto pase desapercibido para muchos de nosotros. Existen grupos finitos de cualquier tamaño, grandes o pequeños; de estructura muy simple, como los grupos cíclicos o bastantes complicados, como los grupos de simetrías; grupos infinitos con uno o varios generadores, o bien infinitos sin una base finita.

También se pueden crear nuevos grupos, usando los anteriores, por medio de ciertas operaciones entre ellos. Esto, por supuesto, puede hacer pensar al lector que el estudio de la teoría de grupos es una tarea abrumadora, dada la gran cantidad de grupos que intervienen.

Sin embargo existe una relación muy útil que podemos construir entre dos grupos, lo cual permite comparar la estructura de ambos sin hacer consideraciones acerca de la naturaleza misma de los elementos. Este concepto, que juega un papel central dentro de toda esta teoría, es el de isomorfismo de grupos. Si dos grupos son isomorficos, entonces desde el punto de vista del álgebra son casi iguales: esto es, poseen la misma estructura.

Los grupos aparecieron un poco tarde en la historia de las matemáticas, aproximadamente a mediados del siglo XIX.

El concepto de operación binaria o ley de composición interna aparece por vez primera en la obra del matemático alemán C. F. Gauss en relación a un trabajo sobre composición de formas cuadráticas del tipo:

$$f(x, y) = ax^2 + bxy + cy^2$$

con coeficientes enteros.

Gauss da una definición de equivalencia de formas cuadráticas, y luego define una operación de multiplicación de formas, y posteriormente demuestra que esta multiplicación es compatible con la relación de equivalencia.

También Gauss y algunos de sus predecesores en el campo de la Teoría de Números, como Euler y Lagrange habían estudiado las propiedades de suma y multiplicación de los enteros módulo p, con p primo.

Pero fue el genio de Evariste Galois quien dio inicio a la moderna teoría de grupos, al exponer en sus brillantes trabajos la relación entre las ecuaciones algebraicas y el grupo de permutaciones de las raíces. Galois fue el primero que destacó la importancia de los subgrupos normales y estudió en detalle las propiedades abstractas de los grupos.

La definición general de grupo, fue dada por Cayley en 1854. Pero es a partir de 1880 cuando comienza a desarrollarse la teoría general de los grupos finitos con los trabajos de S. Lie, Felix Klein y Henry Poincaré.

2.2 Definiciones Básicas

Definición 2.2.1 *Sea A un conjunto no vacío. Una* **operación binaria en A** *es una función del producto cartesiano $A \times A$ en A.*

Así pues una operación binaria sobre el conjunto A asigna a cada par de elementos (a, b) en $A \times A$ un tercer elemento en A, el cual se denota con algún símbolo especial, por ejemplo $a * b$.

El símbolo que se utiliza para la operación no reviste mucha importancia en si mismo. Lo pertinente es saber que hay un elemento de A, resultado de aplicar la operación a los elementos a y b, el cual estamos denotando por $a*b$. Podemos usar otras notaciones como ab, $a \cdot b$, $a \triangle b$, ..., etc. siempre que no halla confusión.

El elemento $a * b$ será llamado el "producto de a con b".

Ejemplo 1: Sea $A = \{a, b, c\}$ y definamos la operación $*$ en A de la forma siguiente

$$\begin{aligned}(a,a) &\longrightarrow a\\ (a,b) &\longrightarrow a\\ (a,c) &\longrightarrow a\\ (b,a) &\longrightarrow b\\ (b,b) &\longrightarrow b\\ (b,c) &\longrightarrow b\\ (c,a) &\longrightarrow c\\ (c,b) &\longrightarrow c\\ (c,c) &\longrightarrow c\end{aligned}$$

En realidad se ha podido definir la operación en forma más concisa, haciendo

$$(x,y) \longrightarrow x \quad \forall (x,y) \in A \times A$$

o bien

$$x * y = x \quad \forall x, y \in A$$

Ejemplo 2: Definiremos una nueva operación en A, pero esta vez por intermedio de una tabla. La operación la denotamos por $\odot$. El producto $x \odot y$ aparece en la casilla correspondiente a la columna x y la fila y.

$\odot$	a	b	c
a	a	c	a
b	c	a	b
c	b	b	c

Nótese que por ejemplo el producto de a con c es b, mientras que el producto de c con a es a. Luego para esta operación se tiene:

$$a \odot c \neq c \odot a$$

También se puede observar que:

$$(a \odot c) \odot b = b \odot b = a$$

y

$$a \odot (c \odot b) = a \odot b = c$$

luego

$$a \odot (c \odot b) \neq (a \odot c) \odot b$$

Definición 2.2.2 *Sea A un conjunto en donde esta definida una operación binaria $*$. Diremos que la operación es* **asociativa**, *si y sólo si*

$$x * (y * z) = (x * y) * z \tag{2.1}$$

para todo x, y, z en A.

Ejemplo: Sea $A = \{a, b, c\}$, y $*$ la operación $*$ definida en A, en el ejemplo 1. Esta operación es asociativa.

En efecto, si $x, y, z \in A$, se tendrá entonces:

$$x * (y * z) = x * (y) = x$$
$$(x * y) * z = (x * y) = x$$

luego será cierto que:

$$x * (y * z) = (x * y) * z,$$

para todo x, y, z en A.

Definición 2.2.3 *Sea A un conjunto en donde esta definida una operación binaria $*$, y sea S un subconjunto de A. Diremos que S* **es cerrado** *bajo la operación $*$, si se cumple:*

$$x * y \in S \quad \textit{para todo } x, y \text{ en } S.$$

Nota: Cuando $S = A$ se dice que la operación es cerrada.

Ejemplo 1: Sea $\mathbb{Z}^+$ el conjunto de los números enteros positivos y consideremos la operación suma de números enteros, la cual denotamos por "+", como es costumbre. Entonces, si S es el conjunto de los números pares, se tiene que S es cerrado bajo la suma.

Ejemplo 2: Sea $\mathbb{Z}$ el conjunto de enteros, con la operación resta de enteros "$-$". Si $S = \mathbb{Z}^+$ el conjunto de enteros positivos, entonces S no es cerrado bajo la resta.

Por ejemplo 6 y 9 están en S y sin embargo $6 - 9 = -3$ no está en S.

Definición 2.2.4 *Sea A un conjunto no vacío en donde se define una operación binaria $*$. Diremos que A es un* **semigrupo** *con la operación $*$, si la operación es asociativa y cerrada.*

Denotaremos por $(A, *)$ al semigrupo formado por el conjunto A con la operación $*$. Algunas veces se utiliza simplemente la letra A, para denotar este semigrupo, por abuso de notación.

Ejemplo 1: $(\mathbb{Z}, +)$ es un semigrupo.

Ejemplo 2: $(\mathbb{Z}^+, +)$ es un semigrupo.

Definición 2.2.5 *Sea A un conjunto, con operación binaria $*$. Un elemento $e \in A$ que satisface:*

$$a * e = e * a = a \quad \textit{para todo } a \text{ en } A,$$

se llama **elemento neutro** *de A, para la operación $*$.*

Ejemplo 1: Sea $A = \{a, b, c\}$ y $*$ la operación

$$x * y = x \quad \text{para todo } x, y \text{ en } A.$$

Entonces A no posee elemento neutro.

Ejemplo 2: Sea $\mathbb{Z}$ el conjunto de los enteros con la operación de suma. Entonces el 0 es un elemento neutro, pues

$$n + 0 = 0 + n = n \quad \text{para todo } n \text{ entero.}$$

Ejemplo 3: Sea A un conjunto no vacío y consideremos $P(A)$ el conjunto formado por todos los subconjuntos de A. Entonces podemos definir la operación binaria en $P(A)$, dada por la unión de conjuntos. Luego el conjunto $\emptyset$, es el elemento neutro de $P(A)$, pues

$$B \cup \emptyset = \emptyset \cup B = B \quad \text{para todo } B \text{ subconjunto de } A.$$

Definición 2.2.6 *Sea $(A, *)$ un semigrupo. Entonces si A posee un elemento neutro, diremos que $(A, *)$ es un* **monoide**.

Ejemplo 1: $(\mathbb{Z},+)$ es un monoide.

Ejemplo 2: Si A es cualquier conjunto, entonces $(P(A), \cup)$ es un monoide, donde $\cup$ denota la operación de unión de conjuntos.

2.3 Grupos

Definición 2.3.1 *Un* **grupo** *es un conjunto no vacío G en donde hay definida una operación binaria $\cdot$, llamada producto, la cual satisface:*

1. *$a \cdot b \in G$ para todo $a, b \in G$.*
2. *$a \cdot (b \cdot c) = (a \cdot b) \cdot c$ para todo $a, b, c \in G$ (Ley Asociativa).*

3. *Existe un elemento $e \in G$, llamado elemento neutro o identidad de la operación, el cual satisface:*

$$a \cdot e = e \cdot a = a,$$

para todo $a \in G$.

4. *Para todo a en G, existe un elemento $a^{-1} \in G$, llamado el inverso de a, el cual satisface:*

$$a \cdot a^{-1} = a^{-1} \cdot a = e.$$

Definición 2.3.2 *Si el conjunto G es finito, entonces G se dice* **grupo finito**. *Caso contrario, diremos que G es infinito.*

Definición 2.3.3 *El orden de grupo es el cardinal del conjunto G.*

Notación: Usamos la notación de potencias en G.

$$\begin{aligned} e &= a^0 \\ a &= a^1 \\ a^2 &= a \cdot a \\ &\vdots \\ a^{n+1} &= a^n \cdot a \end{aligned}$$

Definición 2.3.4 *Un grupo G se dice* **abeliano** *o* **conmutativo**, *si*

$$a \cdot b = b \cdot a \quad \text{para todo } a, b \in G.$$

Ejemplo 1: $(\mathbb{Z},+)$ los números enteros con la suma es un grupo abeliano.

Ejemplo 2: Sea $A = \{a,\ b,\ c\}$ y consideremos en este conjunto la operación $*$ definida por la tabla siguiente:

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

Mostraremos que $(A, *)$ es un grupo, para lo cual probaremos que se verifican las cuatro condiciones de la definición.

En primer lugar, la operación es cerrada, pues al multiplicar dos elementos de A se obtiene otro elemento de A.

También observamos que el elemento a sirve de elemento neutro para esta operación, pues $x * a = a * x = x$, para todo x en A.

Además, todo elemento de A posee inverso. En efecto, se tienen las relaciones

$$a * a = a, \quad b * c = c * b = a$$

luego $a^{-1} = a,\ b^{-1} = c,\ c^{-1} = b$.

Solo resta probar la asociatividad de esta operación. Esto no se puede deducir directamente de la tabla y debe hacerse caso por caso. Aceptando que la operación es asociativa, se tiene entonces que $(A, *)$ es un grupo. Finalmente se demuestra que este grupo es abeliano a partir de relaciones:

$$a * b = b * a, \ \ a * c = c * a, \ \ b * c = c * b.$$

Nótese que la tabla de esta operación es simétrica respecto de la diagonal. Esto es otra indicación de que el grupo es abeliano.

Ejemplo 3: Sea $G = Z \times Z$ el producto cartesiano de Z consigo mismo, cuyos elementos son las parejas ordenadas de números enteros (m, n). Podemos definir una operación en este conjunto mediante:

$$(m_1, n_1) \oplus (m_2, n_2) = (m_1 + m_2, n_1 + n_2),$$

donde $+$ denota la suma de números enteros.

Entonces probaremos que G satisface todas las propiedades de la definición de grupo.

Claramente la operación es cerrada, pues la suma de enteros es cerrada y por lo tanto el par $(m_1 + m_2, n_1 + n_2)$ esta en G.

Probaremos que $\oplus$ es asociativa, para lo cual usaremos la asociatividad de los números enteros. En efecto, se tiene

$$\begin{aligned}(m_1, n_1) \oplus [(m_2, n_2) \oplus (m_3, n_3)] &= (m_1, n_1) \oplus [(m_2 + m_3, n_2 + n_3)] \\ &= (m_1 + (m_2 + m_3), n_1 + (n_2 + n_3)) \\ &= ((m_1 + m_2) + m_3), (n_1 + n_2) + n_3) \\ &= ((m_1 + m_2), (n_1 + n_2)) \oplus (m_3, n_3) \\ &= [(m_1, n_1) \oplus (m_2, n_2)] \oplus (m_3, n_3)\end{aligned}$$

También se demuestra que $(0, 0)$ es el elemento neutro para esta suma. Sea (m, n) un elemento cualquiera en G, luego

$$(0, 0) + (m, n) = (m, n) + (0, 0) = (m, n).$$

Finalmente se deduce que todo elemento (m, n) de G posee un inverso, el cual viene dado por $(-m, -n)$ pues

$$(m, n) \oplus (-m, -n) = (m - m, n - n) = (0, 0)$$

$$(-m, -n) \oplus (m, n) = (-m + m, -n + n) = (0, 0)$$

Por lo tanto G es un grupo. Además este grupo es abeliano, pues para todo par de elementos (m_1, n_1) y (m_2, n_2) en G se tiene

$$\begin{aligned}(m_1, n_1) \oplus (m_2, n_2) &= (m_1 + m_2, n_1 + n_2) \\ &= (m_2 + m_1, n_2 + n_1) \\ &= (m_2, n_2) \oplus (m_1, n_1)\end{aligned}$$

Ejemplo 4: Sea S un conjunto finito y $A(S)$ el conjunto de todas las aplicaciones biyectivas de S en si mismo. Entonces definimos una

operación binaria en este conjunto por medio de la composición de aplicaciones. Entonces se puede verificar que $A(S)$ con esta operación es un grupo, basándonos en los siguientes hechos, muy bien conocidos, sobre funciones:

1. La composición de dos aplicaciones biyectivas, es biyectiva.
2. La composición de aplicaciones es asociativa.
3. La aplicación identidad

$$I : A \longrightarrow A$$

$$x \longrightarrow x$$

   es biyectiva
4. Si una aplicación f es biyectiva, entonces su inversa f^{-1} existe y es biyectiva.

Observación Cuando S es un conjunto finito, entonces $A(S)$ es también finito. Además, si S tiene n elementos, entonces $|A(S)| = n!$. (ver problema 9)

Ejemplo 5: Sea $S = \{x_1, x_2, x_3\}$ y G el grupo de aplicaciones biyectivas de S en si mismo. Este grupo se denomina **grupo de permutaciones de** S y se denota por S_3.

Definamos las aplicaciones:

$$\phi : \begin{array}{l} x_1 \longrightarrow x_2 \\ x_2 \longrightarrow x_1 \\ x_3 \longrightarrow x_3 \end{array}$$

$$\psi : \begin{array}{l} x_1 \longrightarrow x_2 \\ x_2 \longrightarrow x_1 \\ x_3 \longrightarrow x_1 \end{array}$$

Sabemos que G tiene 6 elementos. Calcularemos todos los elementos de G y construiremos una tabla para la operación binaria $\cdot$ de composición.

Nota: Usaremos la convención

$$\sigma \cdot \tau = \text{ primero aplicar } \sigma \text{ y luego } \tau$$

También si $s \in S$ y $\sigma \in A(S)$, usaremos la notación $s \cdot \sigma = \sigma(s)$.

Tenemos entonces

$$\phi \cdot \psi : \begin{array}{l} x_1 \longrightarrow x_3 \\ x_2 \longrightarrow x_2 \\ x_3 \longrightarrow x_1 \end{array}$$

$$\psi \cdot \phi : \begin{array}{l} x_1 \longrightarrow x_1 \\ x_2 \longrightarrow x_3 \\ x_3 \longrightarrow x_2 \end{array}$$

Observamos que $\phi \cdot \psi \neq \psi \cdot \phi$ y por lo tanto G no es abeliano.
Calcularemos ahora todas las potencias de los elementos ϕ y ψ

$$\phi^2 : \begin{array}{l} x_1 \longrightarrow x_1 \\ x_2 \longrightarrow x_2 \\ x_3 \longrightarrow x_3 \end{array}$$

luego $\phi^2 = 1$, identidad. Por otra parte:

$$\psi^2 : \begin{array}{l} x_1 \longrightarrow x_3 \\ x_2 \longrightarrow x_1 \\ x_3 \longrightarrow x_2 \end{array}$$

y

$$\psi^3 : \begin{array}{l} x_1 \longrightarrow x_1 \\ x_2 \longrightarrow x_2 \\ x_3 \longrightarrow x_3 \end{array}$$

luego $\psi^3 = 1$, identidad.

Notemos que

$$\psi \cdot \phi = \phi \cdot \psi^2$$

Mediante esta relación, podemos escribir todos los elementos de G en la forma: $\phi^i \cdot \psi^j$, con $0 \leq i$, $0 \leq j$.

Entonces los seis elementos del grupo G son

$$1,\ \psi,\ \psi^2,\ \phi,\ \phi\psi,\ \phi\psi^2.$$

Seguidamente, construiremos una tabla de multiplicación para G.

$\cdot$	1	ψ	ψ^2	ϕ	$\phi\psi$	$\phi\psi^2$
1	1	ψ	ψ^2	ϕ	$\phi\psi$	$\phi\psi^2$
ψ	ψ	ψ^2	1	$\phi\psi$	$\phi\psi^2$	ϕ
ψ^2	ψ^2	1	ψ	$\phi\psi^2$	ϕ	$\phi\psi$
ϕ	ϕ	$\phi\psi^2$	$\phi\psi$	1	ψ^2	ψ
$\phi\psi$	$\phi\psi$	ϕ	$\phi\psi^2$	ψ	1	ψ^2
$\phi\psi^2$	$\phi\psi^2$	$\phi\psi$	ϕ	ψ^2	ψ	1

El grupo G se denomina **grupo simétrico** de grado 3, y lo denotaremos por S_3.

Dejaremos como un ejercicio para el lector, la verificación de cada uno de los productos en la tabla anterior.

Ejemplo 6: Sea n un entero y a un símbolo. Construimos un conjunto G cuyos elementos son los n símbolos

$$a^0 = e,\ a,\ a^2, \ldots, a^{n-1}$$

Definimos un producto en G mediante la siguiente regla de multiplicación:

$$a^i a^j = \begin{cases} a^{i+j}, & \text{si} \quad i+j \leq n \\ a^{i+j-n}, & \text{si} \quad n < i+j \end{cases}$$

Se puede verificar entonces que G con esta operación es un grupo. Este grupo se denota por C_n y se llama **grupo cíclico de orden** n**.**

Ejemplo 7: Sea S el conjunto de los enteros y $A(S)$ el conjunto de las aplicaciones biyectivas de $\mathbb{Z}$ en si mismo. Sea $G \subseteq A(S)$ el conjunto de aquellas aplicaciones que mueven un número finito de elementos.

Esto es, $\sigma \in G$ sí y sólo si

$$A = \{x | \sigma(x) \neq x\}$$

es finito. Entonces G es un grupo (Verificarlo!).

Ejemplo 8: Sea G el conjunto de matrices 2×2 de la forma:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

donde a, b, c, d son números reales y $ad - bc \neq 0$. Podemos dotar a G de una operación binaria, dada por la multiplicación de matrices, la cual se define mediante:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x & y \\ w & z \end{pmatrix} = \begin{pmatrix} ax + bw & ay + bz \\ cx + dw & cy + dz \end{pmatrix}$$

Notemos que

$$\begin{aligned} (ax + bw)(cy + dz) - (cx + dw)(ay + bz) &= acxy + adxz + \\ & \quad bcwy + bdwz - acxy - \\ & \quad bcxz - dawy - bdwz \\ &= xz(ad - bc) \end{aligned}$$

$$\begin{aligned} & +wy(bc-da) \\ = \; & (xz-wy)(ad-bc) \\ \neq \; & 0 \end{aligned}$$

Luego G es cerrado bajo esta operación.

También la matriz

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

actua como la identidad, y además I está en G.

Finalmente si

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G,$$

entonces $ad - bc \neq 0$, luego la matriz

$$B = \begin{pmatrix} \dfrac{d}{ad-bc} & \dfrac{-b}{ad-bc} \\ \dfrac{-c}{ad-bc} & \dfrac{a}{ad-bc} \end{pmatrix}$$

es real y además es un elemento de G, pues

$$\frac{ad-bc}{(ad-bc)^2} = \frac{1}{ad-bc} \neq 0$$

También se puede verificar que

$$A \cdot B = I$$

Luego G es un grupo. Este grupo se llama **grupo lineal de** $\mathbb{R}^2$ y se denota por $L_2(\mathbb{R})$.

Ejemplo 9: Sea G el Conjunto de matrices 2×2 de la forma

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

donde a, b, c y d son números reales y $ad-bc = 1$. Se puede ver entonces que G es un grupo.

Ejercicios

1) Sea $A = \{a, b, c\}$ con la operación $\oplus$ dada por la siguiente tabla

$\oplus$	a	b	c
a	a	b	c
b	b	c	a
c	c	c	a

Hallar un elemento identidad para A.
¿Es $(A, \oplus)$ un semigrupo?
¿Es $(A, \oplus)$ un monoide?

2) Sea A cualquier conjunto y $\cap$, la intersección de conjuntos en $P(A)$. Demuestre que $(P(A), \cap)$ es un monoide.

3) Demuestre que todo grupo de 3 elementos debe ser abeliano.

4) Demuestre que todo grupo G, en donde se tiene la relación: $a^2 = e$, para todo $a \in G$, debe ser abeliano.

5) Demuestre que $A(S)$, el conjunto de todas las aplicaciones biyectivas de S en si mismo es un grupo.

6) Demuestre que la resta de números enteros no es una operación asociativa.

7) Para cada una de las operaciones siguientes, definidas en los números enteros $\mathbb{Z}$, responder las siguientes interrogantes

a) ¿Es asociativa? b) ¿Es cerrada?
c) ¿Hay elemento neutro? d) ¿Es conmutativa?

1) $a * b = a * b + 1$
2) $a * b = \max\{a, b\}$
3) $a * b = \min\{a, b\}$
4) $a * b = 2ab$

5) $a * b = (ab)^2$
6) $a * b = a$

8) Si G es un grupo finito, probar que existe un entero positivo t, tal que $a^t = e$, para todo a en G.

9) Probar que si S es un conjunto con n elementos, entonces $A(S)$ posee $n!$ elementos.

10) Probar que el conjunto de matrices reales 2×2 con determinante no nulo, es un grupo bajo la multiplicación de matrices.

11) Probar la propiedad asociativa para el grupo $L_2(\mathbb{R})$.

12) Probar que el grupo $L_2(\mathbb{R})$ no es abeliano.

13) Sea A el conjunto formado por todas las funciones $f : [0, 1] \longrightarrow \mathbb{R}$. Probar que $(A, +)$ es un grupo, donde $+$ es la operación de suma de funciones.

14) Construya todas las posibles tablas de multiplicación para un grupo de orden 4.

15) Demuestre que el conjunto de los números racionales distintos de cero forman un grupo bajo el producto.

16) Demuestre que el grupo $(Z, +)$ no tiene subgrupos finitos.

17) Demuestre que el grupo $(Q, +)$ no tiene subgrupos finitos.

18) Sea Q^* el conjunto de los números racionales distintos de cero. Probar que $(Q^*, .)$ es un grupo.

19) Hallar un subgrupo finito dentro de $(Q^*, .)$.

20) Probar, mediante el principio de inducción, la existencia y unicidad de las potencias positivas de un elemento a, dentro de un grupo G.

2.4 Simetrías

Una **simetría** de una figura plana es un movimiento rígido del plano que hace coincidir dicha figura consigo misma. Todo movimiento rígido del plano tiene la propiedad de conservar las distancias y por esto se le

da el nombre de **isometría**. El estudio de las simetrías es una de las relaciones más interesantes que se conocen entre algebra y geometría.

Comenzaremos por estudiar el **grupo de simetrías del cuadrado**. Para facilitar el estudio de este grupo, tome un pedazo de papel o cartulina en forma de cuadrado y numere los vértices por ambos lados de acuerdo a la figura

Figura 2.1:

Coloque el cuadrado sobre un sistema de ejes perpendiculares con su centro en el punto de corte de los ejes y lados paralelos a los ejes.

El eje horizontal lo llamamos X y al vertical lo llamamos Y.

Comenzamos ahora nuestro trabajo, considerando todos los posibles movimientos del cuadrado que lo hagan coincidir consigo mismo. Este se puede mover deslizandose sobre el plano y también está permitido levantarlo y voltearlo al revés (Recuerdese que los vértices han sido marcados por ambos lados).

Podemos decir en primer lugar que el cuadrado tiene **simetría rotacional**, pues cada rotación de 90° con eje de rotación en el origen, no altera la figura. Estas rotaciones, por conveniencia, serán realizadas en sentido contrario a las agujas del reloj. Podemos denotarlas por

$$R_1 \quad - \quad \text{Rotación de} \quad 90^\circ$$

R_2 – Rotación de 180°
R_3 – Rotación de 270°
I – Rotación de 360°

Figura 2.2:

También el cuadrado se puede hacer girar 180° sobre un eje que puede ser el eje X, o bien el eje Y, o bien un eje diagonal que pase por dos vértices. Estos movimientos también son simetrías, pues no se altera la figura del cuadrado al ejecutarlos. Estas simetrías , llamadas **simetrías axiales**, producen el mismo efecto que la reflexión sobre un espejo colocado sobre un eje de simetría. Ver la figura.

Figura 2.3:

Tendremos entonces

H	$-$	Reflexión alrededor del eje	X
V	$-$	Reflexión alrededor del eje	Y
D_1	$-$	Reflexión alrededor del eje	L_{13}
D_2	$-$	Reflexión alrededor del eje	L_{24}

Estas 8 simetrías del cuadrado son todas las posibles. Cualquiera otra simetría necesariamente induce una permutación sobre los vértices.

Al mover el cuadrado cada vértice debe ir sobre otro. Para el vértice 1 tenemos 4 posibilidades. Una vez fijado el primer vértice, se tienen dos posibilidades de ubicar el vértice 2. Al estar fijados los vértices 1 y 2, los restantes están determinados, luego hay $4 \times 2 = 8$ posibles maneras de permutar los vértices, lo cual equivale a los 8 tipos de simetrías descritas anteriormente.

Veamos como se pueden multiplicar las simetrías entre si.

El producto de una simetría A_1 por otra simetría A_2, denotado por A_1A_2, consiste en efectuar el movimiento del cuadrado determinado por A_1, seguido del movimiento dado por A_2.

Así por ejemplo, para calcular HV, reflejamos el cuadrado sobre el eje horizontal y seguidamente lo reflejamos sobre el eje vertical. Esto produce el mismo efecto que hacer una rotación del cuadrado de 180° (Ver la figura).

Figura 2.4:

Luego $HV = R_2$.

El producto de dos simetrías da como resultado otra simetría de las ya descritas. Podemos calcular todos los posibles productos para estar seguro de ello.

También el producto de simetrías es asociativo por lo siguiente. Si se tiene A_1, A_2 y A_3 tres simetrías, entonces podemos multiplicarlas de dos maneras distintas. En primer lugar si movemos el cuadrado ejecutando en sucesión A_1 y A_2 obtendremos otra simetría B. Entonces movemos nuevamente el cuadrado para ejecutar A_3. El resultado obtenido será igual a

$$(A_1A_2)A_3$$

Por otro lado, podríamos haber efectuado en sucesión las simetrías A_2 y A_3 para obtener una simetría C. Luego llevamos el cuadrado a la posición original y desde allí efectuamos A_1 seguida de C. El resultado será igual a

$$A_1(A_2A_3)$$

Es fácil ver entonces que

$$(A_1A_2)A_3 = A_1(A_2A_3)$$

Antes de calcular todos los productos de simetrías en una tabla, veamos como se obtienen algunas relaciones interesantes entre ellas.

En primer lugar observamos que todas las rotaciones se obtienen como potencias de R_1

$$\begin{aligned} R_1 &= R_1 \\ R_1^2 &= R_2 \\ R_1^3 &= R_3 \\ R_1^4 &= I \end{aligned} \tag{2.2}$$

También se demuestra que toda reflexión es igual al producto de H por alguna rotación

$$\begin{aligned} H &= H \\ V &= HR_1^2 \\ D_1 &= HR_1 \\ D_2 &= HR_1^3 \end{aligned} \tag{2.3}$$

Para calcular cualquier producto de simetrías, necesitamos la relación

$$R_1 H = D_2 = HR_1^3 \tag{2.4}$$

Vemos que en general este producto no es conmutativo, pues $R_1 H \neq HR_1$.

Teniendo todos estos elementos a la mano, pasamos a construir la tabla de esta operación.

$\cdot$	I	R_1	R_1^2	R_1^3	H	HR_1	HR_1^2	HR_1^3
I	I	R_1	R_1^2	$R_1^3 H$	H	R_1	HR_1^2	HR_1^3
R_1	R_1	R_1^2	R_1^3	I	HR_1	HR_1^2	HR_1^3	H
R_1^2	R_1^2	R_1^3	I	R_1	HR_1^2	HR_1^3	H	HR_1
R_1^3	R_1^3	I	R_1	R_1^2	HR_1^3	H	HR_1	HR_1^2
H	H	HR_1^3	HR_1^2	HR_1	I	R_1^3	R_1^2	R_1
HR_1	HR_1	H	HR_1^3	HR_1^2	R_1	I	R_1^3	R_1^2
HR_1^2	HR_1^2	HR_1	H	HR_1^3	R_1^2	R_1	I	R_1^3
HR_1^3	HR_1^3	HR_1^2	HR_1	H	R_1^3	R_1^2	R_1	I

Podemos extraer muchas conclusiones importantes al observar esta tabla. En primer lugar el elemento I actúa como elemento neutro. También todo elemento posee inverso bajo este producto, pues el elemento I aparece en cada una de las columnas.

Por el momento queda demostrado que el conjunto de todas las simetrías del cuadrado es un grupo con la operación producto de simetrías. Este grupo de orden 8, no es abeliano. De ahora en adelante lo llamaremos **Grupo de simetrías del cuadrado**.

Podemos dar una formulación completamente abstracta de este grupo, sin hacer referencia a los movimientos rígidos de un cuadrado. El lector estará de acuerdo en que el grupo que definiremos a continuación y el anterior tienen la misma tabla de multiplicación y por lo tanto la misma estructura.

Definición 2.4.1 *El* **grupo diédrico de orden 4** *es aquel cuyos elementos son los símbolos $a^i b^j$, con $i = 0, 1$, $j = 0, 1, 2, 3$ y la operación de multiplicación, dada por las relaciones*

$$a^2 = e, \qquad b^4 = e, \qquad ba = ab^3$$

Este grupo se denota por D_4.

Aparte de las simetrías del cuadrado, podemos construir simetrías de otro tipo de figuras planas.

Por ejemplo la figura plana

Figura 2.5:

tiene las siguientes simetrías

$$\begin{array}{lll} H & \text{- reflexión en el eje} & X \\ V & \text{- reflexión en el eje} & Y \\ R & \text{- rotación de} & 180^\circ \end{array}$$

Estos tres elementos satisfacen las relaciones

$$H^2 = V^2 = R^2 = I$$

La tabla de multiplicación es la siguiente

$\cdot$	I	H	V	R
I	I	H	V	R
H	H	I	R	V
V	V	R	I	H
R	R	V	H	I

Este grupo de simetrías, que llamaremos **grupo H**, se puede definir en abstracto usando solamente las relaciones de multiplicación entre sus elementos.

Definición 2.4.2 *El* **grupo** 4 **de Klein** *se define como el conjunto de símbolos* $\{I, a, b, c\}$ *sujeto a las relaciones*

$$a^2 = b^2 = c^2 = I \quad , \quad ab = c \quad , \quad bc = a \quad , \quad ca = b$$

Es claro entonces que el grupo H y el grupo 4 de Klein tienen la misma estructura.

La idea de relacionar grupos de simetría con las propiedades geométricas de las figuras planas se debe al matemático alemán Felix Klein $(1849-1925)$, en su famoso trabajo sobre geometría llamado Programa de Erlangen, el cual fue publicado en 1872.

Capítulo

3

Teorema de Lagrange

3.1 Introducción

En este capítulo estudiaremos uno de los teoremas más importantes de toda la teoría de grupos como lo es el Teorema de Lagrange. Daremos en primer lugar una serie de resultados básicos que se derivan de la definición de grupos. Posteriormente se introduce el concepto de subgrupo y en especial se estudian las propiedades de los grupos ciclícos.

Si H es un subgrupo de un grupo finito G, entonces el Teorema de Lagrange establece que el orden de H es un divisor del orden de G. Este resultado genera una serie de propiedades interesantes de los grupos finitos de tipo estructural. Finalizamos el capítulo con el estudio de las clases laterales de un subgrupo H de G.

3.2 Resultados Preliminares

En esta sección demostramos algunos hechos básicos sobre grupos, que se pueden deducir de la definición 1.3.1.

Lema 3.2.1 *Si G es un grupo entonces*
a) El elemento identidad es único.
b) Todo $a \in G$ tiene un inverso único en G.
c) Para todo $a \in G$, $(a^{-1})^{-1} = a$.
d) Para todo $a, b \in G$, $(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$.

Demostración: *a)* Sean e y f dos elementos identidad en G. Entonces se tiene la ecuación.

$$e = e \cdot f = f,$$

de donde

$$e = f$$

b) Supongamos que un elemento $a \in G$ posee dos inversos x e y.

Luego

$$x \cdot a = a \cdot x = e$$
$$y \cdot a = a \cdot y = e$$

Luego

$$\begin{aligned} y(a \cdot x) &= y \cdot e = y \\ (y \cdot a) \cdot x &= y \\ e \cdot x &= y \\ x &= y \end{aligned}$$

c) Para $a \in G$, se tiene

$$a^{-1} \cdot a = e$$
$$a \cdot a^{-1} = e$$

Luego a es el inverso de a^{-1}, único, y por lo tanto $(a^{-1})^{-1} = a$.

d) Sean $a, b \in G$. Luego

$$\begin{aligned} (a \cdot b)(b^{-1}a^{-1}) &= a \cdot (b \cdot b^{-1}) \cdot a^{-1} \\ &= (a \cdot e) \cdot a^{-1} \\ &= a \cdot a^{-1} \\ &= e \end{aligned}$$

Similarmente

$$\begin{aligned}(b^{-1}a^{-1})(a\cdot b) &= b^{-1}\cdot(a^{-1}\cdot a)\cdot b\\ &= b^{-1}\cdot e\cdot b\\ &= b^{-1}\cdot b\\ &= e\end{aligned}$$

Por lo tanto

$$(a\cdot b)^{-1} = a^{-1}\cdot b^{-1}.$$

♠

Proposición 3.2.1 *Sean a y b en el grupo G. Entonces las ecuaciones*

$$a\cdot x = b \tag{3.1}$$
$$y\cdot a = b, \tag{3.2}$$

poseen solución única: $x = a^{-1}\cdot b$; $y = b\cdot a^{-1}$.

Demostración: Multiplicando (**??**) por a^{-1} a la izquierda tenemos

$$\begin{aligned}a^{-1}\cdot(a\cdot x) &= a^{-1}\cdot b\\ (a^{-1}\cdot a)\cdot x &= a^{-1}\cdot b\\ e\cdot x &= a^{-1}\cdot b\\ x &= a^{-1}\cdot b\end{aligned}$$

Similarmente, multiplicando (**??**) por a^{-1} a la derecha tenemos

$$\begin{aligned}(y \cdot a)a^{-1} &= b \cdot a^{-1} \\ y \cdot (a \cdot a^{-1}) &= b \cdot a^{-1} \\ y \cdot e &= b \cdot a^{-1} \\ y &= b \cdot a^{-1}\end{aligned}$$

♠

Lema 3.2.2 *Sean a, u, w elementos en G. Entonces valen las siguientes* **leyes de cancelación** *en G.*

$$a \cdot u = a \cdot w \quad \text{implica} \quad u = w \tag{3.3}$$
$$u \cdot a = w \cdot a \quad \text{implica} \quad u = w \tag{3.4}$$

Demostración: La ecuación

$$a \cdot u = a \cdot w$$

posee solución única

$$\begin{aligned}u &= a^{-1}(a \cdot w) \\ &= (a^{-1} \cdot a)w \\ &= e \cdot w \\ &= w\end{aligned}$$

Similarmente, la ecuación

$$u \cdot a = w \cdot a$$

posee solución única

$$\begin{aligned} u &= (w \cdot a)(a^{-1}) \\ &= w(a \cdot a^{-1}) \\ &= w \cdot e \\ &= w \end{aligned}$$

Ejercicios

1) Sea m un entero positivo fijo. Diremos que dos enteros a y b son **congruentes módulo m** y lo denotamos por:

$$a \equiv b \; mod \; m,$$

si m divide a $b - a$

Probar que la relación de congruencia módulo m en el conjunto $\mathbb{Z}$ es una relación de equivalencia.

2) Para cada entero a en $\mathbb{Z}$, se define su **clase de congruencia módulo** m, como el conjunto formado por su clase de equivalencia

$$[a] = \{x \in \mathbb{Z} | x \equiv a \; mod \; m\}$$

El conjunto formado por todas estas clases se llaman **Enteros módulo** m y se denota por $\mathbb{Z}_m$.

Probar que $\mathbb{Z}_m$ es un grupo, bajo la operación de suma módulo m, definida por:

$$[a] + [b] = [a + b]$$

¿Cuál es el elemento neutro de este grupo? Construya una tabla para la operación de suma módulo 7.

3) Demuestre que todo grupo de orden ≤ 5 debe ser abeliano.

4) Probar que si G es un grupo abeliano y a, b pertenecen a G, entonces

$$(ab)^n = a^n b^n$$

para todo entero $n \geq 0$.

5) Sea G un conjunto no vacío cerrado con una operación asociativa, tal que

i) Existe un elemento $e \in G$ tal que

$$ae = a$$

para todo $a \in G$.

ii) Para todo $a \in G$ existe un elemento a', tal que

$$a'a = e$$

probar que G es un grupo con esta operación.

6) Sea G un conjunto finito, el cual es cerrado bajo una operación asociativa y tal que valen las dos leyes de cancelación. Es decir, para todos a, b, c en G se tiene

$$ab = ac \Longrightarrow b = c$$

$$ba = ca \Longrightarrow b = c$$

Probar que G es un grupo con esta operación.

7) Hallar los inversos de cada uno de los elementos de S_3.

8) Sea S_7 el grupo de permutaciones de 7 elementos con la composición de aplicaciones, como en S_3. Probar que existe un elemento a, tal que $a^{12} = e$, pero $a^s \neq e$ para $0 < s < 12$.

9) Sea G un grupo. Probar que para cualquier par de enteros m y n se tiene

i) $a^m a^n = a^{m+n}$

ii) $(a^m)^n = a^{mn}$

para todo a en G.

10) Si G es un grupo de orden par, probar que existe un elemento $a \in G$, $a \neq e$ y tal que $a^2 = e$.

11) Hallar todos los elementos de $\mathbb{Z}_{12}$ que satisfacen la ecuación $x^6 = 1$.

12) Sea $G = M_2(\mathbb{R})$ el grupo de matrices invertibles cuadradas de orden 2 sobre $\mathbb{R}$, con la operación producto. Probar que G no es abeliano.

13) Probar que el conjunto de matrices invertibles cuadradas de orden 2 sobre $\mathbb{R}$, con la operación producto y con determinante 1 es un grupo.

14) Demuestre que en los enteros módulo 7, todo elemento $a \neq e$ satisface:

i) $a^7 = e$

ii) $a^s \neq e$, para todo $0 < s < 7$.

15) Sea Q^* el conjunto de los números racionales direrentes de cero. Probar que $(Q^*, .)$ no es un grupo cíclico.

3.3 Subgrupos

Definición 3.3.1 *Sea G un grupo y $H \subseteq G$. Si H es un grupo con la operación definida en G, entonces H se dice* **subgrupo de G.**

Ejemplo: Sea $G = (\mathcal{Q}, +)$ el grupo de los números racionales con la adición y $H = (\mathbb{Z}, +)$ el grupo de los enteros con la adición. Entonces H es subgrupo de G.

Para indicar que H es subgrupo de G, usaremos la notación: $H < G$.

Definición 3.3.2 *Un subgrupo H de G se dice* **subgrupo propio** *si $H < G$ y $H \neq \{e\}$, $H \neq G$.*

Nota: Si G es un grupo, los subgrupos G y $\{e\}$ se llaman **los subgrupos triviales de G.**

Ejemplo 1: Sea G un grupo de orden 3. Entonces G es de la forma $G = \{e, a, a^2\}$. Se puede verificar que G no tiene subgrupos propios.

Ejemplo 2: Sea G el grupo de los enteros módulo 4 con la suma y H formado por los elementos $\bar{0}$ y $\bar{2}$. Entonces H es un subgrupo de G.

Ejemplo 3: Sea V el grupo 4 de Klein, $V = \{e, a, ab\}$ sujeto a las relaciones $a^2 = b^2 = e$. Entonces el conjunto $H = \{e, a\}$ es un subgrupo de G.

Podemos hacer un diagrama de los subgrupos de G, para los dos ejemplos anteriores.

Así tenemos

El siguiente teorema establece un criterio muy útil para determinar cuando un subconjunto H de un grupo G es un subgrupo.

Teorema 3.3.1 *Un subconjunto H de de un grupo G es un subgrupo, si y sólo si*

i) $a \cdot b \in H$ *para todo* $a, b \in H$

ii) $a^{-1} \in H$ *para todo* $a \in H$.

Demostración: Puesto que la operación binaria en G es asociativa, sólo falta verificar que $e \in G$. En efecto, sea $a \in H$, luego $a^{-1} \in H$ (por ii)) y además $a \cdot a^{-1} = e \in H \quad (\text{por } i))$.

Luego H es un grupo, y por lo tanto un subgrupo de G.

♠

Teorema 3.3.2 *Sea G un grupo y $a \in G$. Entonces el conjunto*

$$H = \{a^n \mid n \in \mathbb{Z}\}$$

es un subgrupo de G. Además H es el subgrupo de G más pequeño que contiene a.

Demostración: De acuerdo al teorema anterior, será suficiente con probar:

i) $a^n \cdot a^m \in H$, para $a^n, a^m \in H$
ii) $(a^n)^{-1} \in H$. para $a^n \in H$.

Claramente $a^n \cdot a^m = a^{n+m} = a^z \quad \text{con} \quad z = n + m \in \mathbb{Z}$, y por lo tanto $a^n \cdot a^m \in H$.

También

$$(a^n)^{-1} = a^{-n} \in H$$

Luego $H < G$.

Para probar la segunda afirmación, sea K un subgrupo de G y $a \in K$. Luego $a^0 = e \in K$ por ser K un grupo. También $a^2 \in K$, pues $a \in K$ y K es cerrado bajo la operación en G. De esta forma se concluye $a^n \in K$ para todo $n \geq 0$.

También $a^{-1} \in K$, pues $a \in K$ y su inverso se halla en K. Similarmente $a^{-2} = a^{-1} \cdot a^{-1} \in K$, pues $a^{-1} \in K$ y K es cerrado. Luego $a^{-n} \in K$ para todo $n \geq 0$. Hemos probado entonces que $H \subseteq K$

♠

Definición 3.3.3 *El grupo H, se llama* **subgrupo cíclico** *generado por a. El elemento a se llama el* **generador de** *H. Usaremos la notación:*

$$H =< a > .$$

Definición 3.3.4 *Un grupo G se dice* **cíclico** *si $G =< a >$ para algún $a \in G$.*

Ejemplo 1: Sea G el grupo formado por los enteros con la suma. Entonces $G =< 1 >$.

Ejemplo 2: Sea G el grupo de los enteros módulo 4, luego $G =< \bar{1} >$

Ejemplo 3: Sea $G = S_3$ y $K =< \phi >$, Entonces K es cíclico de orden 2.

3.4 Teorema de Lagrange

En esta sección estudiaremos una condición necesaria necesaria para que un subconjunto de un grupo finito, sea un subgrupo de este.

Teorema 3.4.1 *(Lagrange)*
Sea G un grupo finito y H un subgrupo de G. Entonces el orden de H divide al orden de G.

Demostración: Si $H = \{e\}$ ó $H = G$ no hay nada que probar. Supongamos entonces que $H \neq \{e\}$ y $H \neq G$. Sea

$$H = \{h_1, \ldots, h_r\}$$

donde $r = \circ(H)$.

Luego existe un elemento $a \in G$, tal que $a \notin H$. Entonces tenemos los siguientes elementos en G.

$$h_1, h_2, \ldots, h_r, ah_1, \ldots, ah_r.$$

Afirmamos que hay $2r$ elementos distintos. En efecto:
i)$Si\ ah_i = h_j$, entonces multiplicando por h_i^{-1} a la derecha nos da

$$a = h_j h_i^{-1} \in H$$

Luego $a \in H$, lo cual es una contradicción
ii) Si $ah_i = ah_j$, cancelación por a nos da

$$h_i = h_j$$

lo cual es, nuevamente una contradicción.

Si esos $2r$ elementos son todos elementos de G, entonces

$$\circ(G) = 2r = 2 \circ (H)$$

y entonces $\circ(H)$ divide al orden de G.

Si por el contrario, hay más de $2r$ elementos en G, continuamos el proceso y tendremos que existe un elemento $b \in G$, distinto de los anteriores. Luego tenemos los siguientes elementos en G

$$\begin{array}{cccc} a_0h_1, & \ldots, & a_0h_r \\ a_1h_1, & \ldots, & a_1h_r \\ a_2h_1, & \ldots, & a_2h_r \\ & \vdots & \end{array}$$

donde $a_0 = e$, $a_1 = a$, $a_2 = b$,...etc. y a_i no esta en ninguno de los elementos que forman las filas anteriores a la fila i-ésima. Se puede probar que todos estos elementos que se generan son distintos. En efecto:

i) Si $a_ih_j = a_ih_k$, entonces cancelando se tiene que $h_j = h_k$, lo cual es una contradicción.

ii) Si para $i > l$ se tiene $a_ih_j = a_lh_k$, entonces multiplicando por h_j^{-1} a la derecha se tiene $a_i = a_lh_kh_j^{-1}$. Como H es un grupo , tendremos que $h_kh_j^{-1} \in H$, luego $h_kh_j^{-1} = h_s$, para algún s y por lo tanto $a_i = a_lh_s$. Entonces el elemento a_i pertenece a la l-ésima fila, lo cual es una contradicción.

Puesto que G es un grupo finito, este proceso de formación de filas se detiene despúes de un número finito de pasos, digamos k pasos. Se tendrá entonces que hay $k \circ (H)$ elementos en G. Con esto termina la desmostración.

♠

Definición 3.4.1 *Si G es un grupo y $a \in G$, el* **orden de a** *es el menor entero positivo n tal que*

$$a^n = e.$$

Usamos la notación $\circ(a)$ para indicar el orden de a.

Si ese entero no existe, diremos que a tiene **orden infinito**

Corolario 3.4.1 *Si G es un grupo finito y $a \in G$, entonces $\circ(a)$ es un divisor de $\circ(G)$.*

Demostración: Sea $a \in G$ y consideremos el subgrupo cíclico generado por a, $H =< a >$ el cual consiste en los elementos

$$a^0 = e, a, a^2, \ldots, a^{n-1}$$

donde $a^n = e$.

Es claro entonces que $n = \circ(H)$ y además $n = \circ(a)$.

De acuerdo al teorema de Lagrange, tendremos que

$$\circ(H) | \circ(G)$$

Luego

$$\circ(a) | \circ(G).$$

♠

Corolario 3.4.2 *Si G es un grupo finito y $a \in G$, entonces*

$$a^{\circ(G)} = e.$$

Demostración: Sabemos que $a^{\circ(a)} = e$, y por el corolario anterior

$$\circ(G) = k \circ (a) \quad \text{para algún } \ k.$$

Luego

$$\begin{aligned} a^{\circ(G)} &= a^{\circ(a)\cdot k} \\ &= \left(a^{\circ(a)}\right)^k \\ &= e^k \\ &= e. \end{aligned}$$

Corolario 3.4.3 *Si G es un grupo finito de orden primo p, entonces G es cíclico.*

Demostración: Sea $a \in G$, $a \neq e$. Entonces $H =< a >$ el subgrupo cíclico generado por a tiene orden un divisor de p. Luego hay dos posibilidades:

i) $\circ(H) = p$, lo cual implica $H = G$ y G es cíclico generado por a

ii) $\circ(H) = 1$, y por lo tanto se tendría $a = e$, lo cual es imposible. Luego G es un grupo cíclico.

♠

Ejercicios

1)Probar que $(\mathbb{Z}_6, +)$ es un grupo cíclico. Hallar todos sus generadores.

2) Demuestre que el grupo 4 de Klein no es cíclico.

3) Hallar el orden de cada uno de los elementos del grupo $(\mathbb{Z}_{10}, +)$.

4) Sea p un número primo. Probar que Q_p el conjunto de números racionales de la forma

$$\frac{a}{p^\alpha}$$

donde a es un entero primo relativo con p, y α es un entero positivo, es un subgrupo de $(Q, +)$.

5) Demuestre que si p es un número primo, entonces el grupo $(\mathbb{Z}_p, +)$ tiene p-1 generadores.

6) Demuestre que el grupo de los enteros módulo m, bajo la suma, es un grupo cíclico, con $\overline{1}$ como generador.

7) Sea $G = \mathbb{Z}x\mathbb{Z}$ con la operación de suma de coordenadas. Demuestre que G no es cíclico.

8) (Teorema de Euler). Probar que si a es un entero positivo primo relativo con n, entonces

$$a^{\phi(n)} \equiv 1 \; mod \; n,$$

donde $\phi(n)$ = número de enteros entre 1 y n primos relativos con n.

9) (Teorema de Fermat). Probar si p es un número primo y a es cualquier entero, entonces

$$a^p \equiv a \ mod \ p$$

10) Usando el problema anterior, demuestre que $2^{30} - 1$ es un número compuesto.

11) Hallar el diagrama de subgrupos para los grupos siguientes
a) $(\mathbb{Z}_6,+)$
b) S_3
c) $(\mathbb{Z}_7,+)$

12) Sea m un entero fijo y $\mathbb{Z}_m$ el conjunto de clases de congruencias módulo m. Se define el producto módulo m en $\mathbb{Z}_m$, mediante

$$[a] \cdot [b] = [a \cdot b]$$

Probar que esta operación esta bien definida ¿Es $(\mathbb{Z}_m, \cdot)$ un grupo?

13) Probar que si p es un número primo, entonces el conjunto de los enteros módulo p, no nulos, forman un grupo bajo el producto.

14) Hallar una tabla para el grupo de los enteros módulo 7 bajo el producto.

15) Demuestre que todo grupo cíclico es abeliano

16) Probar que todo subgrupo de un grupo cíclico es cíclico.

17) ¿Cuantos generadores tiene un grupo cíclico de orden n?

18) Sea m un entero positivo dado, no necesariamente primo. Sea U_m el conjunto de clases de congruencias módulo m, no nulas $\overline{x}$, tales que $(x, m) = 1$. Probar que U_m es un grupo bajo la operación de producto módulo m.

19) Hallar explicitamente U_6 y U_{10}.

20) Demuestre que U_{15} tiene un elemento de orden 4.

21) Hallar un generador de U_{10}

22) Dar un ejemplo de un subgrupo cíclico en el grupo de matrices 2×2, de la forma

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \quad \text{con} \quad ad - bc \neq 0$$

23) Sea $G = S_4$, hallar el grupo cíclico H generado por el elemento

$$\psi : \begin{array}{l} x_1 \longrightarrow x_2 \\ x_2 \longrightarrow x_3 \\ x_3 \longrightarrow x_1 \\ x_4 \longrightarrow x_1 \end{array}$$

¿Cual es el orden de este grupo?

24) Sean a y b dos elementos en un grupo G, abeliano tal que

$$(\circ(a), \circ(b)) = 1.$$

Probar que:

$$\circ(ab) = \circ(a) \cdot \circ(b)$$

donde (,) denota el máximo común divisor.

25) Sean a y b dos elementos en grupo abeliano G. Probar que:

$$\circ(ab) = [\circ(a), \circ(b)],$$

donde [,] denota el mínimo común múltiplo.

26) Demuestre que si un elemento a en un grupo G satisface:

$$a^k = e, \quad \text{entonces} \quad \circ(a) | k$$

27) Hallar todos los subgrupos de $(\mathbb{Z}_{10}, +)$.

28) Hallar todos los subgrupos del grupo de simetrías del cuadrado.

3.5 Operaciones con los Subgrupos

Cuando se tiene un grupo G, es posible conocer parte del mismo si se conoce un subgrupo H de G. Si G tiene varios subgrupos diferentes, entonces cada uno de ellos es una pieza dentro de una gran maquinaria: cada una cumple una función específica en G. Cuando se conocen todos los subgrupos de G entonces se tiene un conocimiento total del grupo G, en cierto sentido.

Si queremos mirar como se multiplican dos elementos dentro de G, y estos dos elementos están dentro de un subgrupo H, el cual ha sido determinado de antemano, entonces el problema estará resuelto porque sabemos como se ejecuta la multiplicación dentro de H.

Si por el contrario un elementos está en un subgrupo H, y otro elemento esta fuera de H y dentro otro subgrupo K, entonces el producto de ambos elementos estará en un conjunto L contenido en G. Nos preguntamos: ¿Cómo podríamos garantizar que L sea un subgrupo de G? ¿Cuál es el orden de L?

Definición 3.5.1 *Sea G un grupo y H, K dos subgrupos de G. Entonces la* **intersección** *de H y K, es el conjunto*

$$H \cap K = \{x \in G \mid x \in H, \text{ y } x \in K\}$$

Proposición 3.5.1 *La intersección de dos subgrupos de G es un subgrupo de G.*

Demostración Sean $x,\ y \in H \cap K$. Entonces $xy \in H$, y además $xy \in K$, pues H y K son grupos. Luego $xy \in H \cap K$.

Por otro lado, si $x \in H \cap K$, entonces $x^{-1} \in H$, y $x^{-1} \in K$, pues H y K son grupos. Luego $x^{-1} \in H \cap K$.

Mas generalmente, se tiene

Proposición 3.5.2 *Sea G un grupo y $\{H_i\}$, $i \in I$ una familia de subgrupos de G. Entonces el conjunto*

$$H = \bigcap_{i \in I} H_i$$

es un subgrupo de G.

La **unión de dos subgrupos** no es un grupo en general, por ejemplo, sea $G = (\mathbb{Z}_6, +)$ enteros módulo 6, y

$$H = \{\bar{e}, \bar{2}, \bar{4}\} \quad \text{y} \quad K = \{\bar{e}, \bar{3}\}.$$

Sabemos que H y K son subgrupos de G. Sin embargo

$$H \cup K = \{\bar{e}, \bar{2}, \bar{3}, \bar{4}\}$$

no es un subgrupo, pues

$$\bar{2} + \bar{3} = \bar{5} \notin H \cup K.$$

Definición 3.5.2 *Sea G un grupo y H, K subgrupos de G. Entonces el* **producto de H y K**, *se define por:*

$$HK = \{hk \mid h \in H \text{ y } k \in K\}.$$

Observación El producto de dos subgrupos no es un subgrupo en general. Afortunadamente, existe un criterio muy útil, para determinar cuando esto es cierto.

Teorema 3.5.1 *Sea G un grupo. Entonces HK es un subgrupo de G si y sólo si*

$$HK = KH.$$

Demostración: Sea $HK = KH$ y sean $h_1, h_2 \in K$ y $k_1, k_2 \in K$. Luego debemos probar:

i) $(h_1k_1)(h_2k_2) \in HK$

ii) $(h_1k_1)^{-1} \in HK$

Para probar *i*) notemos que

$$k_1h_2 \in KH = HK,$$

luego existen h_3, k_3 tal que

$$k_1 h_2 = h_3 k_3,$$

por lo tanto

$$\begin{aligned}(h_1k_1)(h_2k_2) &= h_1(k_1h_2)k_2 \\ &= h_1(h_3k_3)k_2 \\ &= (h_1h_3)(k_3k_2) \in HK\end{aligned}$$

Para probar $ii)$ vemos que

$$(h_1k_1)^{-1} = k_1^{-1}h_1^{-1} \in KH = HK$$

Recíprocamente, si HK es un subgrupo de G probaremos que

$$HK = KH$$

En efecto, sea $kh \in KH$. Luego existe el inverso de $hk : h^{-1}k^{-1} \in HK$, y por lo tanto $h = (h^{-1}k^{-1})^{-1} \in HK$.

Luego

$$KH \subseteq HK$$

Para demostrar la inclusión en el otro sentido, sea $x \in HK$, entonces

$$x^{-1} = hk \in HK,$$

luego

$$\begin{aligned}x &= (x^{-1})^{-1} \\ &= (hk)^{-1} \\ &= k^{-1}h^{-1} \in KH\end{aligned}$$

Por lo tanto hemos demostrado

$$HK \subseteq KH$$

♠

Pregunta : ¿Cuantos elementos tiene HK?

Teorema 3.5.2 *Sea G un grupo finito y H, K subgrupos de G. Entonces*

$$|HK| = \frac{\circ(H) \circ (K)}{\circ(H \cap K)}.$$

Demostración: Los elementos de HK son la forma hk con $h \in H$ y $h \in K$. Entonces hay $\circ(H)\ \circ(K)$ elementos de este tipo. Sin embargo puede haber repeticiones, es decir

$$h_1 k_1 = h_2 k_2$$

para algunos $h_1, h_2 \in H$, $k_1, k_2 \in K$.

Pero entonces $h_2^{-1} h_1 = k_2 k_1^{-1}$, y por lo tanto se tiene un elemento $x = h_2^{-1} h_1 = k_2 k_1^{-1}$ en la intersección de H y K.

Es decir cada vez que hay una repetición de dos elementos, se produce un elemento en la intersección $H \cap K$.

Recíprocamente, si $x \in H \cap K$, se tiene

$$hk = hx^{-1}xk = h_1 k_1$$

es decir, x genera un duplicado de hk en el conjunto HK.

Así pues el número de veces que un elemento hk aparece repetido es igual al orden de intersección $\circ(H \cap K)$.

Luego

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

♠

Corolario 3.5.1 *Si H y K son subgrupos de G y*

$$\circ(H) > \sqrt{\circ(G)} \quad \text{y} \quad \circ(K) > \sqrt{\circ(G)}$$

Entonces

$$H \cap K \neq \{e\}$$

Demostración: Como $|HK| \leq \circ(G)$ tenemos

$$\begin{aligned} \circ(G) &\geq |HK| \\ &= \frac{\circ(H) \circ (K)}{\circ(H \cap K)} \\ &> \frac{\sqrt{\circ(G)}\sqrt{\circ(G)}}{\circ(H \cap K)} \\ &= \frac{\circ(G)}{\circ(H \cap K)} \end{aligned}$$

Luego

$$\circ(H \cap K) > 1$$

por lo cual

$$H \cap K \neq \{e\}$$

♠

Como aplicación de esto tenemos lo siguiente

Ejemplo: Sea G un grupo finito, con $\circ(G) = 15$, entonces G tiene a lo sumo un subgrupo de orden 5.

Solución: Si H y K son subgrupos de orden 5, entonces

$$\circ(H) > \sqrt{\circ(G)} \quad \text{y} \circ (K) > \sqrt{\circ(G)},$$

luego por el corolario anterior

$$H \cap K \neq \{e\}.$$

Pero $H \cap K < H$, y por el teorema de Lagrange se tiene $\circ(H \cap K)|5$

Luego la única posibilidad es:

$$\circ(H \cap K) = 5.$$

Por lo tanto

$$H \cap K = H.$$

Usando la misma técnica se prueba $H \cap K = K$. Luego H=K.

Definición 3.5.3 *Sea G un grupo y S un subconjunto de G, diferente del vacío. Entonces el* **grupo generado por** *S viene dado por*

$$< S >= \bigcap \{H \mid \ H \text{ subgrupo de } G \text{ y } S \subseteq H\}$$

Observación Es claro que $< S >$ es un subgrupo de G. Además es el menor subgrupo de G que contiene a S. Esto es simple consecuencia de la definición.

Definición 3.5.4 *Sea G un grupo, y H, K subgrupos de G. Entonces* **el grupo generado por** *H* **y** *K es el conjunto $< H \cup K >$.*

3.6 Clases Laterales

Cuando estudiamos la relación de congruencias módulo m en el conjunto de los números enteros, vimos que esta se define para dos enteros a y b

$$a \equiv b \ mod \ m,$$

si y sólo si m divide a $a - b$.

Es posible definir esta relación en términos de grupos. Si m es un entero positivo, entonces el conjunto de todos los multiplos de m, $H = m\mathbb{Z}$ es un subgrupo del grupo aditivo de $\mathbb{Z}$. Entonces se tiene que

$$a \equiv b \ mod \ m,$$

si y sólo si $a - b \in H$.

En esta sección daremos una generalización del concepto de congruencia módulo m, al considerar dentro de un grupo G la congruencia módulo H, donde H es un subgrupo de G.

Esta relación tiene propiedades muy similares a la congruencia de los números enteros. Una de las ventajas es que nos proporciona una partición del grupo en clases de equivalencias. Bajo ciertas condiciones sobre H, este conjunto de clases de equivalencias módulo H se le podrá dotar de una estructura de grupo.

Definición 3.6.1 *Sea G un grupo y H un subgrupo de G. Si $a \in G$, entonces la* **clase lateral derecha de a en H** *es el conjunto*

$$Ha = \{ha \mid h \in H\}.$$

Ejemplo: Sea $G = S_3$ el grupo simetrico de orden 6. Sea $H = \{I, \phi\}$ entonces las clases laterales derechas son:

$$\begin{aligned} H\psi &= \{\psi, \phi\psi\} \\ H\psi^2 &= \{\psi^2, \phi\psi^2\} \\ H\phi\psi &= \{\phi\psi, \psi\} \\ H\phi\psi^2 &= \{\phi\psi^2, \psi^2\} \\ HI &= \{\psi, \phi\psi\} \\ H\phi &= \{\phi, I\} \end{aligned}$$

Definición 3.6.2 *Sea $a \in G$, entonces la* **clase lateral izquierda de** *a es el conjunto*

$$aH = \{ah \mid h \in H\}.$$

Ejemplo: Las clases laterales izquierdas de H en S_3 son:

$$\begin{aligned} \psi H &= \{\psi, \phi\psi^2\} \\ \psi^2 H &= \{\psi^2, \phi\psi\} \\ \phi\psi H &= \{\phi\psi, \psi^2\} \\ \phi\psi^2 H &= \{\phi\psi^2, \psi\} \\ IH &= \{I, \phi\} \\ \phi H &= \{\phi, I\} \end{aligned}$$

Definición 3.6.3 *Sea G un grupo y H un subgrupo de G. Sean a y b dos elementos de G. Diremos que a* **es congruente a** *b módulo H y lo denotamos*

$$a \equiv b \ mod \ H$$

si y sólo si $ab^{-1} \in H$.

Ejemplo 1: Sea $G = (\mathbb{Z}, +)$ y $H = (3\mathbb{Z}, +)$, entonces

$$a \equiv b \ mod \ H,$$

significa que

$$a - b \in H,$$

luego

$$a - b = 3k, \quad \text{para algún} \ \ k \in \mathbb{Z}$$

Luego se tiene la misma relación de congruencia de números enteros

$$a \equiv b \ mod \ 3$$

Teorema 3.6.1 *Sea G un grupo y $H < G$, entonces la relación de congruencia módulo H, determina una relación de equivalencia en G.*

Demostración:
1) **Reflexiva:** Sea $a \in G$, entonces

$$aa^{-1} = e \in H,$$

luego

$$a \equiv a \ mod \ H$$

2) **Simétrica:** Supongamos que $a \equiv b \ mod \ H$, entonces $ab^{-1} \in H$.

Ahora bien, como H es un grupo, se tiene

$$(ab^{-1})^{-1} = ba^{-1} \in H$$

luego

$$b \equiv a \ mod \ H$$

3) **Transitiva:** Supongamos que $a \equiv b \ mod \ H$ y $b \equiv c \ mod \ H$.

Luego

$$ab^{-1} \in H \quad \text{y} \quad bc^{-1} \in H.$$

Como H es un subgrupo de G, se debe tener

$$ac^{-1} = (ab^{-1})(bc^{-1}) \in H$$

Luego

$$a \equiv c \ mod \ H$$

Teorema 3.6.2 *Para todo $a \in G$, sea*

$$[a] = \{x \in G \mid x \equiv a \ mod \ H\}$$

Entonces

$$[a] = Ha.$$

Demostración: Sea $x \in [a]$, entonces

$$x \equiv a \ mod \ H,$$

luego

$$xa^{-1} \in H$$

por lo tanto existe $h \in H$ tal que $xa^{-1} = h$, lo cual implica $x = ha$. Por lo tanto $x \in Ha$.

Recíprocamente, supongamos que $x \in Ha$. Luego existe $h \in H$, tal que $x = ha$. Luego $xa^{-1} = h$ y por ende $x \equiv a \ mod \ H$. Con esto se prueba que $x \in [a]$, lo cual da fin a la demostración.

♠

Observación Si a es un elemento de G, el conjunto $[a]$ se llama **la clase de congruencia módulo H**. El teorema anterior nos dice entonces, que toda clase lateral es igual a una clase de congruencia.

Seguidamente, probaremos que todas las clases laterales tienen el mismo número de elementos.

Teorema 3.6.3 *Sean a y $b \in G$. Entonces*

$$|Ha| = |Hb|.$$

Demostración: Consideremos la función

$$\begin{aligned} \phi \ : \ & Ha \longrightarrow hb \\ & ha \longrightarrow hb \end{aligned}$$

Entonces probaremos que ϕ es inyectiva.

Sean $h_1, h_2 \in H$. Si suponemos $\phi(h_1 a) = \phi(h_2 a)$, se tiene que $h_1 b = h_2 b$, y luego $h_1 = h_2$.

Claramente ϕ es sobreyectiva y por lo tanto ϕ es biyectiva.

♠

Definición 3.6.4 *Sea G y H un subgrupo de G, entonces el número de clases laterales de H en G se llama el* **índice de H en G** *y lo denotamos por $[G : H]$.*

Corolario 3.6.1 *Sea G un grupo, H un subgrupo de G. Entonces*

$$|G| = [G : H]|H| \tag{3.5}$$

Demostración: Notar que todas las clases laterales derechas de G tiene el mismo número de elementos, en particular H mismo es una clase lateral derecha pues

$$H = He$$

De aquí se deduce

$$\begin{aligned} |G| &= \text{número de clases laterales} \times \text{número de elementos en } H \\ &= [G : H] \cdot |H| \end{aligned}$$

♠

Nota: Si G es finito, entonces se tiene

$$[G : H] = \frac{\circ(G)}{\circ(H)} \tag{3.6}$$

Observación: La fórmula (**??**) nos proporciona otra demostración del teorema de Lagrange.

Ejercicios

1)Sea $G = (\mathbb{Z}_{12}, +)$ y $H =< \overline{3} >$, $K =< \overline{6} >$. Hallar el orden de HK.

2) Sea G un grupo finito. Sean H y K subgrupos de G de ordenes m y n, respectivamente. Probar que $H \cap K = \{e\}$.

3) Sea G un grupo de orden 21 y H y K subgrupos de ordenes 3 y 7 respectivamente. Probar que $HK = KH$.

4) Sea G un grupo, S un n subconjunto no vacío de G, y consideremos

$$S_0 = \{s_1 \dots s_n \mid s_i \in S,\ o\ s_i^{-1} \in S,\ n \in N\}$$

Probar que S_0 es subgrupo de G que contiene S y además $S_0 =< S >$.

5)Sea G el grupo $(\mathbb{Z}, +)$ y $S = \{2, 5\}$. Hallar el grupo generado por S en G.

6) Hallar las clases laterales de $H =< 2 >$ en $(\mathbb{Z}, +)$.

7) Hallar las clases laterales de $H = \{1, -1\}$ en $(\mathcal{Q}, \cdot)$

8) Demuestre que si m y n son enteros primos relativos, entonces el grupo generado por ellos en $(\mathbb{Z}, +)$ es todo $\mathbb{Z}$.

9) Sea m un entero positivo, y $H =< m >$. Hallar el índice de H en $(\mathbb{Z}, +)$.

10) Hallar un subgrupo de índice 2 en $(\mathcal{Q}^*, \cdot)$.

11) Sea $G = S_4$ y

$$\begin{aligned} H &= \{\sigma \in S_4 \mid \sigma(x_1) = x_1\} \\ H &= \{\psi \in S_4 \mid \psi(x_2) = x_2\} \end{aligned}$$

a) Probar que: H y K son subgrupos de S_4
b) Hallar: $\circ(H)$ y $\circ(K)$
c) Hallar: $H \cap K$ y $\circ(H \cap K)$
d) Calcule: $\#HK$
e) Deduzca de d) que HK no es un subgrupo de G.

12) Sea $G = S_4$ y

$$\theta : \begin{array}{l} x_1 \longrightarrow x_3 \\ x_2 \longrightarrow x_1 \\ x_3 \longrightarrow x_2 \\ x_4 \longrightarrow x_4 \end{array} \qquad \psi : \begin{array}{l} x_1 \longrightarrow x_2 \\ x_2 \longrightarrow x_3 \\ x_3 \longrightarrow x_4 \\ x_4 \longrightarrow x_1 \end{array}$$

a) Calcular: $\circ(\theta)$ y $\circ(\psi)$
b) Calcular: $\circ(< \theta\psi >)$

13) Sea G un grupo abeliano y g_1, g_2 elementos de G de orden 3 y 4 respectivamente ¿Cuál es el orden de $g_1 \cdot g_2$?

14) Hacer el diagrama de subgrupos para $\mathbb{Z}_{12}$

15) Demuestre que todo grupo de orden 9 debe ser abeliano.

Ayuda:

i) Considere un elemento $g \in G$ ¿Cual es su orden?

ii) Demuestre que $G = HK$, donde H y K son subgrupos de orden 3, de la forma $H =< g_1 >$, $K =< g_2 >$.

iii) Demuestre que $g_1 g_2 = g_2 g_1$ y por lo tanto todos los elementos de G conmutan.

16) ¿Cuantos grupos abelianos de orden 9 se pueden construir?

17) Sea $G = (\mathbb{C}^*, \cdot)$ el grupo de los números complejos con el producto. Sea $W_n = e^{2\pi i/n}$ y $H_n =< W_n >$

a) Hallar el orden de H_n.

b) Representar H_6 en el plano complejo.

c) Represente el diagrama de subgrupo de H_6

18) Demuestre que un conjunto finito H, en un grupo G, es un grupo si y sólo si H es cerrado bajo la operación establecida en G.

Capítulo

4

Isomorfismos

4.1 Introducción

En el capítulo 1 tuvimos la oportunidad de estudiar una gran cantidad de ejemplos de grupos. Cada uno de ellos estaba formado por elmentos tomados de algún conjunto en particular. Por ejemplo hay grupos cuyos elementos son matrices, otros están formados por números enteros, otros por simetrías de una figura plana, ..., etc.

Podemos estudiar estos grupos en abstracto, considerando únicamente la forma como se multiplican los elementos. Cuando se construye la tabla de multiplicación de un grupo finito se esta haciendo precisamente eso: recojer toda la información posible sobre la operación en el grupo, sin prestar atención a la naturaleza misma de los elementos.

Es posible que dos grupos finitos del mismo orden tengan tablas de multiplicación diferentes: por ejemplo los enteros módulo 4 y el grupo 4 de Klein. En el primer grupo hay un elemento de orden 4 y en el segundo todos los elementos son de orden 2. Diremos entonces que estos grupos no tienen la misma forma, o bien que ellos no son isomorfos.

El concepto de isomorfismo es fundamental en toda la teoría de grupos, pues permite unificar una gran cantidad de grupos bajo una misma estructura en abstracto.

Cuando se consideran todas las posibles imágenes de un grupo G bajo los isomorfismos de grupos, aparece el concepto de grupo normal. Estos subgrupos normales de un grupo G, se definen usando el concepto de clases laterales. Más tarde se establece la conexión entre un grupo normal y el homomorfismo cociente, cuando se estudien los teoremas de Isomorfismo.

Se concluye este capítulo con una exposición del grupo de automorfismos de un grupo G y se dan algunos ejemplos en casos especiales.

4.2 Grupos Normales

Definición 4.2.1 *Sea G un grupo. Un subgrupo N de G se dice* **subgrupo normal** *de G si y sólo si*

$$gng^{-1} \in N, \quad \textit{para todo } g \in G,\ n \in N.$$

Lema 4.2.1 *Sea N subgrupo de G. Entonces N es un subgrupo normal si y sólo si*

$$gNg^{-1} = N, \quad \textit{para todo } g \in G. \tag{4.1}$$

Demostración: Sea N normal. Entonces

$$gng^{-1} \in N, \quad \text{para todo } n.$$

Luego $gNg^{-1} \subset N$. En particular

$$g^{-1}Ng \subset N,$$

luego

$$N = g(g^{-1}Ng)g^{-1} \subset gNg^{-1} \subset N,$$

y por lo tanto $gNg^{-1} = N$.

Recíprocamente, si (**??**) es cierto, entonces N es normal en G.

♠

Observación: Si G es un grupo abeliano entonces todo subgrupo N de G es normal. Por lo tanto la noción de normalidad carece de interés cuando trabajamos con grupos abelianos.

Lema 4.2.2 *Sea G un grupo y $N < G$. Entonces N es subgrupo normal de G, si y sólo si toda clase lateral derecha de G es una clase lateral izquierda.*

Demostración: Sea N normal en G. Consideremos la clase lateral derecha Na. Entonces de acuerdo al lema **??**

$$a^{-1}Na = N$$

de donde $Na = aN$. Luego Na es una clase lateral izquierda.

Por otra parte, si $g \in G$, afirmamos que

$$gNg^{-1} = N$$

En efecto, gN es una clase lateral derecha y de acuerdo a la hipótesis debe ser una clase lateral izquierda. Pero

$$g = ge \in gN$$

y además

$$g = eg \in Ng.$$

Luego la única clase lateral izquierda que contienen a g es Ng, y por lo tanto

$$gN = Ng,$$

y de aquí se obtiene

$$gNg^{-1} = N.$$

♠

Ejemplo 1: Consideremos $G = S_3$, $H = \{e, \phi\}$. Calcularemos las clases laterales izquierdas y derechas.

Solución:

Hay tres clases laterales pues

$$[G : H] = \frac{6}{2} = 3.$$

Las clases laterales derechas e izquierdas vienen dadas por:

$$\begin{array}{rclcrcl} H & = & \{e, \phi\} & & H & = & \{e, \phi\} \\ H\psi & = & \{\psi, \phi\psi\} & & \psi H & = & \{\psi, \psi\phi\} \\ H\psi^2 & = & \{\psi^2\phi\psi^2\} & & \psi^2 H & = & \{\psi^2\psi^2\phi = \phi\psi\} \end{array}$$

Como la clase lateral derecha $H\psi$ no es igual a otra clase lateral izquierda, se sigue que H no es normal.

Ejemplo 2: Sea $G = S_3$ y $N = \{e, \psi, \psi^2\}$. Entonces se puede verificar fácilmente que H es normal en G, pues hay sólo dos clases laterales derechas a saber, N y ϕN, las cuales son iguales a las únicas dos clases laterales izquierdas N y $N\phi$.

4.3 Grupo Cociente

Sea G un grupo y N un subgrupo normal de G. Entonces el conjunto de las clases laterales derechas de N en G, el cual denotamos por G/N, se puede dotar de estructura de grupo.

En primer lugar, definimos una multiplicación en G/N de la forma siguiente:

$$\begin{array}{rcl} G/N \times G/N & \longrightarrow & G/N \\ (Na, Nb) & \longrightarrow & Na \cdot Nb = Nab \end{array} \tag{4.2}$$

Nótese que por ser N normal se tiene que el producto de dos clases laterales derechas es de nuevo una clase lateral derecha, pues

$$Na \cdot Nb = N(aN)b = N \cdot Nab = Nab$$

Se pueden verificar los 4 axiomas de grupo para el conjunto cociente G/N con la operación así definida:

1) Si Na y Nb son dos clases laterales, entonces

$$NaNb = Nab \in G/N.$$

2) Si Na, Nb y Nc están en G/N se tiene

$$\begin{aligned} Na(NbNc) &= Na(Nbc) \\ &= Na(bc) \\ &= N(ab)c \\ &= (NaNb)Nc \end{aligned}$$

3) Si $Na \in G/N$, entonces

$$Na \cdot N = Na = N \cdot Na$$

Luego N es el elemento neutro, para la multiplicación de clases laterales.

4) Si $Na \in G/N$, $Na^{-1} \in G/N$ y

$$\begin{aligned} Na \cdot Na^{-1} &= N(aa^{-1}) = Ne = N \\ Na^{-1} \cdot Na &= N(a^{-1}a) = Ne = N \end{aligned}$$

Teorema 4.3.1 *Sea N normal en G, entonces G/N es un grupo y*

$$\circ(G/N) = \frac{\circ(G)}{\circ(N)}.$$

Demostración: Hemos probado que G/N es un grupo con la operación de multiplicación dada en (**??**)

Por otro lado el orden del grupo cociente G/N es igual al número de clases laterales de G en N, el cual viene dado por el índice de N en G, esto es:

$$|G/N| = [G : N]$$

De acuerdo a la fórmula (**??**), Capítulo 1 se tiene

$$|G/N| = \frac{\circ(G)}{\circ(N)}$$

♠

Ejercicios

1) Demuestre que si H es normal en G y N es un subgrupo normal de G, entones NH es un subgrupo de G.

2) Sea G el grupo de matrices reales 2×2 de la forma

$$A = \begin{vmatrix} a & b \\ c & d \end{vmatrix}$$

con $\triangle_A = ad - bc \neq 0$.

Consideremos el conjunto H de matrices en G, tales que

$$\triangle_h = 1, \quad \text{para toda } h \in H.$$

Probar que H es un subgrupo normal de G.

3) Sea G un grupo y N un subgrupo de G. Probar que N es normal si cumple $[G : N] = 2$.

4) Sea G un grupo, $a \in G$. Definimos el **Normalizador de** a como

$$N(a) = \{x \in G \mid xa = ax\}$$

Demuestre que
a) $N(a)$ es un subgrupo de G.
b) $N(a)$ es normal en G.

5) Sea G un grupo y H subgrupo de G. el **Normalizador de** H es el conjunto

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

Probar que:
a) $N(H)$ es un subgrupo de G.
b) H es un subgrupo de $N(H)$.
c) H es normal en $N(H)$.

6) Sea G un grupo, definimos el **centro de** G como

$$Z(G) = \{x \in G \mid xg = gx, \ \forall g \in G\}$$

Probar que $Z(G)$ es un subgrupo de G, el cual es abeliano.

7) Hallar los centros de los grupos siguientes:
i) S_3, el grupo de simetrías de orden 6.
ii) $M_{2\times 2}(\mathcal{Q})$, grupo de matrices de orden 2×2 sobre los números racionales.

8) Sea G el grupo de enteros módulo 6 con la suma y $H = \{\overline{0}, \overline{2}\}$. Hallar el grupo cociente G/H.

9) Sea $S = \{1, 2, 3, 4\}$ y H el subgrupo de $A(S)$ formado por aquellos elementos σ, tales que $\sigma(1) = 1$ ¿Es H normal en $A(S)$? Hallar el normalizador de H en $A(S)$.

10) Sea H como en 9) y consideremos la biyección

$$\sigma : \begin{array}{ll} 1 & \longrightarrow 1 \\ 2 & \longrightarrow 2 \\ 3 & \longrightarrow 4 \\ 4 & \longrightarrow 3 \end{array}$$

Hallar el nromalizador de σ en H.

11) Demuestre que $Z(A(S)) = \{e\}$.

12) Demuestre que si un elemento $a \in G$, satisface $gag^{-1} = a^s$, para algún s entero, entonces el grupo cíclico $< a >$ es normal en G.

13) Hallar un subgrupo normal $A(S)$, donde $S = \{1, 2, 3, 4\}$.

14) Hallar un subgrupo normal en D_4.

15) Sea G un grupo y U un subconjunto de G. Si $gug^{-1} \in U$ para todo $g \in G$, $u \in U$, probar que $\langle U \rangle$ es normal en G.

16) Sea G un grupo, y U el conjunto

$$U = \{xyx^{-1}y^{-1} \mid x, y \in G\}$$

En este caso escribimos $G' = \langle U \rangle$ y lo llamamos el subgrupo conmutador de G. Probar
a) G' es normal en G.

b) G/G' es abeliano.

c) Si G/N es abeliano, probar que $N \supset G'$

d) Probar que si H es un subgrupo de G y $H \supset G'$, entonces H es normal en G.

4.4 Homomorfismos

Nos proponemos a definir ahora un cierto tipo de aplicación entre dos grupos, el cual sea compatible con las operaciones definidas en cada grupo.

Sea $f : (G, *) \longrightarrow (\overline{G}, \circ)$ una aplicación entre dos grupos. Si a y b son elementos de G, entonces $a * b$ es un elemento de G. Por otra parte $f(a)$ y $f(b)$ son elementos de $\overline{G}$, luego el producto de ellos $f(a) \circ f(b)$ está en $\overline{G}$.

La idea que buscamos es tener una función f con la propiedad de hacer el siguiente diagrama conmutativo

Definición 4.4.1 *Sean $(G, *)$ y $(\overline{G}, \circ)$ dos grupos. Una aplicación*

$$\phi : G \longrightarrow \bar{G},$$

se llama homomorfismo de grupos, si y sólo si

$$\phi(a * b) = \phi(a) \circ \phi(b) \quad \textit{para todo } \ a, b \in G.$$

Observación: Usualmente utilizamos la misma notación para el producto en ambos grupos entonces la condición de homorfismo se escribe

$$\phi(ab) = \phi(a)\phi(b)$$

Ejemplo 1: Si G y $\overline{G}$ son dos grupos y $\overline{e}$ es el elemento neutro de $\overline{G}$, la aplicación

$$\begin{array}{rccc} \phi & : & G & \longrightarrow & \overline{G} \\ & & x & \longrightarrow & \overline{e} \end{array}$$

Se llama **homorfismo nulo**

Ejemplo 2: Sea $(\mathbb{Z}, +)$ los números enteros con la suma y

$$\begin{array}{rccc} \phi & : & (\mathbb{Z}, +) & \longrightarrow & \mathbb{Z}_6 \\ & & x & \longrightarrow & [x] \end{array}$$

se puede verificar que ϕ es un homorfismo de grupos.

Lema 4.4.1 *Sea G un grupo y sea N un subgrupo normal de G. Definamos*

$$\begin{array}{rcl} \phi & : & G \longrightarrow G/N \\ & & \phi(x) = Nx \end{array}$$

entonces ϕ es un homomorfismo sobre.

Este homomorfimo se llama la **proyección canónica sobre** N

Demostración: Sea x, y en G. Entonces

$$\begin{array}{rcl} \phi(xy) & = & Nxy \\ & = & Nx \cdot Ny \\ & = & \phi(x) \cdot \phi(y) \end{array}$$

con esto se demuestra que ϕ es un homorfismo. Además, si $Nx \in G/N$, se tiene que

$$\phi(x) = Nx, \quad \text{con } x \in G.$$

Luego ϕ es sobre.

♠

Dos propiedades muy importantes de los homomorfismos son las siguientes:

Lema 4.4.2 *Sea $\phi : G \longrightarrow \overline{G}$ un homomorfismo de grupos y $e, \bar{e}$ los elementos neutros de G y $\overline{G}$ respectivamente. Entonces*

1) $\phi(e) = \bar{e}$.

2) $\phi(x^{-1}) = [\phi(x)]^{-1}$, para todo $x \in G$.

Demostración:

1) Tenemos que

$$\phi(ee) = \phi(e)\phi(e),$$

por otra parte

$$\phi(ee) = \phi(e)$$

Igualando ambas expresiones

$$\phi(e)\phi(e) = \phi(e)$$

Usando la ley de cancelación en el grupo $\overline{G}$ se obtiene

$$\phi(e) = \bar{e}$$

2) Sea $x \in G$. Entonces

$$\begin{aligned} \bar{e} &= \phi(e) \\ &= \phi(xx^{-1}) \\ &= \phi(x)\phi(x^{-1}) \end{aligned}$$

Luego el inverso de $\phi(x)$ en el grupo $\overline{G}$, viene dado por

$$[\phi(x)]^{-1} = \phi(x^{-1})$$

♠

Definición 4.4.2 *Sea* $\phi : G \longrightarrow \overline{G}$*, entonces el* **Kernel de** ϕ*, o* **núcleo** *es el subconjunto de* G

$$\ker \phi = \{x \in G \mid \phi(x) = e\}.$$

Teorema 4.4.1 *Sea* $\phi : G \longrightarrow \overline{G}$ *un homomorfismo de grupos. Entonces* $\ker \phi$ *es un subgrupo normal de* G*.*

Demostración: En primer lugar demostramos que $\ker \phi$ es un subgrupo de G. Sean $a, b \in \ker \phi$, entonces:

$$\begin{aligned} \phi(ab) &= \phi(a)\phi(b) \\ &= \bar{e}\bar{e} \\ &= \bar{e}, \end{aligned}$$

luego $ab \in \ker \phi$.

Por otro lado, sea $a \in G$, luego se tiene

$$\begin{aligned} \phi(a^{-1}) &= \phi^{-1}(a) \\ &= \bar{e}^{-1} \\ &= \bar{e}, \end{aligned}$$

de donde

$$a^{-1} \in \ker \phi$$

Por lo tanto $\ker \phi$ es un subgrupo de G.

Finalmente para demostrar la normalidad, sea $g \in G$ y $n \in \ker \phi$. Luego

$$\begin{aligned}\phi(g^{-1}ng) &= \phi^{-1}(g)\phi(n)\phi(g)\\ &= \phi^{-1}(g)\bar{e}\phi(g)\\ &= \phi^{-1}(g)\phi(g)\\ &= \bar{e}\end{aligned}$$

Luego hemos demostrado

$$g^{-1}ng \subseteq \ker\phi, \quad \forall n \in \ker\phi$$

Por lo tanto

$$g^{-1}\ker\phi g \subseteq \ker\phi \quad \forall g \in G.$$

Así pues $\ker\phi$ es normal en G.

♠

Definición 4.4.3 *Un homomorfismo de grupo $\phi : G \longrightarrow \overline{G}$ se dice* **isomorfismo** *si y sólo si ϕ es una biyección.*

En tal situación diremos que los grupos G y $\overline{G}$ **son isomorfos** y lo denotamos por

$$G \approx \overline{G}.$$

Proposición 4.4.1 *Sea $\phi : G \longrightarrow \overline{G}$ un isomorfismo, entonces la aplicación inversa $\phi^{-1} : \overline{G} \longrightarrow G$ es también un isomorfismo.*

Demostración: En efecto, sea $y_1, y_2 \in \overline{G}$, luego existen $x_1, x_2 \in G$ tales que

$$y_1 = \phi(x_1), \quad y_2 = \phi(x_2)$$

luego

$$\begin{aligned}\phi^{-1}(y_1y_2) &= \phi^{-1}(\phi(x_1)\phi(x_2))\\ &= \phi^{-1}(\phi(x_1x_2))\\ &= x_1x_2\\ &= \phi^{-1}(y_1)\phi^{-1}(y_2)\end{aligned}$$

♠

Proposición 4.4.2 *Sean G, $\overline{G}$ y $\overline{\overline{G}}$ tres grupos y*

$$\phi : G \longrightarrow \overline{G} \quad \text{y} \quad \psi : \overline{G} \longrightarrow \overline{\overline{G}}$$

isomorfismos, entonces la composición

$$\phi\psi : G \longrightarrow \overline{\overline{G}}$$

es también un isomorfismo.

Demostración: Sean $x, y \in G$, entonces

$$\begin{aligned} \phi\psi(xy) &= \psi(\phi(xy)) \\ &= \psi(\phi(x)\phi(y)) \\ &= \psi(\phi(x))\psi(\phi(y)) \\ &= \phi\psi(x)\phi\psi(y) \end{aligned}$$

Luego $\phi\psi$ es un homomorfismo. Como ϕ y ψ son aplicaciones biyectivas entonces $\phi\psi$ es biyectiva. Por lo tanto $\phi\psi$ es un isomorfismo.

♠

Observación: La relación de isomorfismo es una relación de equivalencia en el conjunto de todos los grupos. Esto puede ser demostrado usando las dos proposiciones anteriores.

Teorema 4.4.2 *(Primer Teorema de Isomorfismo)*
Sea $\phi : G \longrightarrow \overline{G}$ un homorfismo sobre, con $\ker \phi = K$. *Entonces*

$$G/K \approx \overline{G}.$$

Demostración: Consideremos el siguiente diagrama.
donde

$$\begin{array}{rccc} \pi & : & G & \longrightarrow & G/K \\ & & g & \longrightarrow & Kg \end{array}$$

es la aplicación **proyección**.

Definimos

$$\begin{array}{rccc} \psi & : & G/K & \longrightarrow & \overline{G} \\ & & Kg & \longrightarrow & \phi(g) \end{array}$$

1) Probaremos en primer lugar que ψ esta bien definida.

Sean

$$Kg_1 = Kg_2, \quad \text{entonces} \quad g_1 g_2^{-1} \in K$$

luego

$$\phi(g_1 g_2^{-1}) = \bar{e}$$

y de esto se deduce

$$\phi(g_1) = \phi(g_2),$$

lo cual implica

$$\psi(Kg_1) = \psi(Kg_2).$$

2) ψ es un homomorfismo

$$\begin{array}{rcl} \psi(Kg_1 Kg_2) & = & \psi(Kg_1 g_2) \\ & = & \phi(g_1 g_2) \\ & = & \phi(g_1)\phi(g_2) \\ & = & \psi(Kg_1)\psi(Kg_2) \end{array}$$

3) ψ es 1:1

Sea $Kg \in \ker \psi$, luego

$$\psi(Kg) = \phi(g) = \bar{e}$$

Esto implica que $g \in \ker \phi = K$. Luego $Kg = K$, elemento neutro en G/K.

4) ψ es sobre.

Sea $\bar{g} \in \overline{G}$, debemos demostrar que existe $Kg \in G/K$ tal que

$$\psi(Kg) = \bar{g}$$

Ahora bien, como ϕ es sobre, existe $g \in G$ tal que

$$\phi(g) = \bar{g}$$

Luego tenemos

$$\psi(Kg) = \phi(g) = \bar{g}$$

por lo tanto ψ es sobre.

Hemos probado que ψ es un isomorfismo.

♠

Teorema 4.4.3 *(Segundo Teorema de Isomorfismo)*

Sea $\phi : G \longrightarrow \overline{G}$ un homomorfismo de grupos, con $\ker \phi = K$. Bajo estas condiciones tenemos

I) Si $\overline{H}$ un subgrupo de $\overline{G}$ y definamos

$$H = \phi^{-1}(\overline{H}) = \{g \in G \mid \phi(g) \in \overline{H}\}$$

Entonces

i) $K \subseteq H$.

ii) H es un subgrupo de G.

iii) Si $\overline{H}$ es normal en $\overline{G}$, H es normal en G.

II) Si L un subgrupo de G y $\overline{K} \subseteq L$, entonces

$$\overline{L} = \phi(L)$$

es un subgrupo de G *y*

$$L = \phi^{-1}(\overline{L}).$$

Luego existe una correspondencia biyectiva entre los conjuntos

$$\mathcal{A} = \{H \mid H \text{ subgrupo de } G \text{ y } K \subseteq H\}$$

y

$$\mathcal{B} = \{\overline{H} \mid \overline{H} \text{ subgrupo de } \overline{G}\}$$

Demostración I:
i) Sea $\overline{H}$ un subgrupo de $\overline{G}$. Probaremos que $K \subset H$. En efecto, si $g \in K$ se tiene

$$\phi(g) = \bar{e} \in \overline{H},$$

Luego $g \in \phi^{-1}(\overline{H})$, y por lo tanto $K \subseteq H$.

Probaremos que H es un subgrupo de G.

ii) Sean $g_1, g_2 \in H$, luego $\phi(g_1) \in \overline{H}$, $\phi(g_2) \in \overline{H}$ y entonces $\phi(g_1 g_2) = \phi(g_1)\phi(g_2) \in \overline{H}$, pues $\overline{H}$ es un grupo.

Por lo tanto

$$g_1 g_2 \in H$$

También, si $g \in H$, $\phi(g) \in \overline{H}$ y por lo tanto el inverso de este elemento, $[\phi(g)]^{-1}$ pertenece a $\overline{H}$

Luego

$$\phi(g^{-1}) = [\phi(g)]^{-1} \in \overline{H}$$

Por lo tanto $g^{-1} \in H$. Así pues, hemos demostrado que H es un subgrupo de G.

iii) Supongamos que $\overline{H}$ es normal en $\overline{G}$. Sean $h \in H$ y $g \in G$. Entonces

$$\begin{aligned} \phi(ghg^{-1}) &= \phi(g)\phi(h)\phi(g^{-1}) \\ &= \bar{g}\bar{h}(\bar{g})^{-1} \end{aligned}$$

donde $\overline{g} = \phi(g)$, $\overline{h} = \phi(h)$. Se tiene entonces

$$\phi(ghg^{-1}) \in \overline{H}$$

por ser $\overline{H}$ normal en $\overline{G}$. Luego

$$ghg^{-1} \in H$$

y de esto se sigue que H es normal en G.

Demostración II: Sea L un subgrupo de G que contiene a K. Entonces definimos su imagen bajo ϕ

$$\overline{L} = \{\phi(g) \mid g \in L\}$$

entonces es fácil probar que $\overline{L}$ es un subgrupo de $\overline{G}$

Por otro lado, sea $\overline{L}$ un subgrupo de $\overline{G}$ y consideremos $T = \{g \in G \mid \phi(g) \in \overline{L}\}$. Entonces afirmamos que

$$T = L.$$

En efecto, si $g \in T$ se tiene que $\phi(g) \in \overline{L}$, y luego existe $\ell_1 \in L$ tal que $\phi(\ell_1) = \phi(g)$. Entonces

$$\phi(\ell_1)\phi(g^{-1}) = e,$$

por lo tanto

$$\ell_1 g^{-1} \in K \subseteq L$$

Luego existe $\ell_2 \in L$, tal que

$$\ell_1 g^{-1} = \ell_2$$

lo cual implica

$$g = \ell_2^{-1}\ell_1 \in L$$

Hemos demostrado $T \subseteq L$

Por otro lado, si $\ell \in L$, entonces $\phi(\ell) \in \overline{L}$, luego $\ell \in T$. Con esto se prueba que $L \subseteq T$. Esto es

$$T = L$$

♠

Teorema 4.4.4 *(Tercer Teorema de Isomorfismo)*
Sea $\phi : G \longrightarrow \overline{G}$ un homomorfismo sobre, con $\ker\phi = K$. Sea $\overline{N}$ un subgrupo normal de $\overline{G}$ y $N = \{g \in G \mid \phi(g) \in \overline{N}\}$. Entonces

$$G/N \approx \overline{G}/\overline{N}$$

y además

$$G/N \approx \frac{G/K}{N/K}.$$

Demostración: Tenemos el diagrama

Definamos

$$\begin{array}{rccc} \psi & : & G & \longrightarrow & \overline{G}/\overline{N} \\ & & g & \longrightarrow & \overline{N}\phi(g) \end{array}$$

Entonces se puede probar que ψ es un homomorfismo sobreyectivo.

¿Quién es el $\ker\psi$?

Sea $g \in \ker\psi$. Luego

$$\psi(g) = \overline{N}\phi(g) = \overline{N}$$

esto es $\phi(g) \in \overline{N}$, luego $g \in N$, por lo tanto

$$\ker\psi = N$$

Entonces por el primer teorema de los homomorfismos de grupos se concluye

$$G/N \approx \frac{\overline{G}}{\overline{\overline{N}}}$$

Por otro lado, sea la aplicación

$$\begin{array}{rccc} \overline{\phi} & : & G/K & \longrightarrow & \overline{G}/\overline{N} \\ & & Kg & \longrightarrow & \overline{N}\phi(g) \end{array}$$

Entonces $\overline{\phi}$ es un homomorfismo de grupos, el cual es sobre, pues ϕ lo es.

¿Quién es $\ker\overline{\phi}$?

Sea $Kg \in \ker\overline{\phi}$, entonces $\overline{N}\phi(g) = \overline{N}$ y por lo tanto $\phi(g) \in \overline{N}$. Luego $g \in N$ y de aquí se concluye

$$\ker\overline{\phi} = \{Kg \mid g \in N\} = N/K$$

Entonces aplicando nuevamente el primer teorema de los isomorfismos a $\overline{\phi}$, se concluye

$$G/K \Big/ N/K \approx \overline{G}/\overline{N}$$

Ejemplo 1: Sea G el grupo aditivo de los números enteros, $(\mathbb{Z}, +)$ y $10\mathbb{Z}$ el subgrupo de los múltiplos de 10. Como G es abeliano, todos sus subgrupos son normales. Luego se pue formar el grupo cociente $\mathbb{Z}/10\mathbb{Z}$. Veamos como se obtiene dicho grupo, por medio de un homomorfismo.

Consideremos la aplicación

$$\begin{array}{rccc} \phi & : & G & \longrightarrow & \mathbb{Z}_{10} \\ & & x & \longrightarrow & \overline{x} \end{array}$$

donde $\overline{x}$ es la clase de congruencia módulo 10 de x. Entonces se puede verificar que ϕ es un homomorfismo de grupos. Sea $y \in Ker\phi$, luego $\phi(y) = \overline{y} = \overline{0}$, lo cual implica que $y \equiv 0 \ mod\ 10$. y por lo tanto

$y \in 10\mathbb{Z}$. Reciprocamente, si $y \in 10\mathbb{Z}$ se deduce que $y \in Ker\phi$. Por lo tanto concluimos que $Ker\phi = 10\mathbb{Z}$.

Aplicando el primer teorema de los isomorfismos se tendrá:

$$\mathbb{Z}/10\mathbb{Z} \approx \mathbb{Z}_{10}.$$

Sea ahora $\overline{H} =< \overline{2} >$ el subgrupo de $\mathbb{Z}_{10}$ generado por la clase $\overline{2}$. ¿Cuál es la imágen inversa de $\overline{H}$ bajo ϕ? Afirmamos que $\phi^{-1}(\overline{H}) = H$ donde $H = 2\mathbb{Z}$. En efecto, si $x \in H$, entonces $\overline{x}$ es congruente módulo 10 a alguna de las clases $\overline{0},\ \overline{2},\ \overline{4}, \overline{6},\ \overline{8}$. Por otro lado, se debe tener $x = 2i+10k$, para algunos $i,\ k$ enteros y de aquí se deduce que x es par. Luego $x \in 2\mathbb{Z}$. También se demuestra fácilmente que $2\mathbb{Z} \subset \phi{-}1(\overline{H})$. Luego la afirmación es válida.

Entonces, usando el tercer teorema de los isomorfismos concluimos

$$\mathbb{Z}/2\mathbb{Z} \approx \mathbb{Z}/10\mathbb{Z} \Big/ 2\mathbb{Z}/10\mathbb{Z}$$

y además

$$\mathbb{Z}/2\mathbb{Z} \approx \mathbb{Z}_{10}/\overline{H}$$

Ejercicios

1) Demuestre que la relación de isomorfismo es una relación de equivalencia en el conjunto de todos los grupos.

2) Sea $\phi : G \longrightarrow \overline{G}$ un isomorfismo. Probar que si G es cíclico entonces $\overline{G}$ debe ser cíclico.

3) Demuestre que si G_1 y G_2 son dos grupo finitos isomorfos, entonces, $|G_1| = |G_2|$.

4) Sea G el grupo de los números complejos, distintos de cero, bajo el producto. Sea H el conjunto de todos los $Z \in G$ tales que

$$Z^7 = 1$$

a) Demuestre que H es un grupo finito de orden 7.
b) Demuestre: $H \approx (\mathbb{Z}_7, +)$.

5) Sea $\phi : G \longrightarrow \overline{G}$ un isomorfismo de grupos. Entonces probar:
a) $\circ(g) = \circ(\phi(g))$ para todo $g \in G$.
b) G es abeliano si y sólo si $\overline{G}$ lo es.

6) Demuestre que $(\mathbb{Z}, +)$ y $(2\mathbb{Z}, +)$, el grupo aditivo de los enteros pares, son isomormofos.

7) Demuestre que $(\mathbb{Z}, +)$ y $(\mathcal{Q}, +)$ no son isomorfos.

8) Demuestre que los grupos de ordenes 4; $\mathbb{Z}_4$ y V no son isomorfos.

9) Demuestre que el grupo de simetrías del cuadrado y el grupo diédrico son isomorfos.

10) Demuestre que el grupo de rortaciones de un polígono regular de n vértices es isomorfo a $(\mathbb{Z}_n, +)$.

11) ¿Cuántos homomorfismos hay de $\mathbb{Z}$ en $\mathbb{Z}$? ¿ Cuántos isomorfismos hay?

12) ¿Cuántos homomorfismos hay de $(\mathbb{Z}, +)$ en $(\mathbb{Z}_2, +)$?

13) Demuestre que $(\mathbb{Z}, +)$ no es isomorfo a $\mathbb{Z} \times \mathbb{Z}$.

14) Sea G un grupo y $a \in G$. Defina una aplicación $\phi : \mathbb{Z} \longrightarrow G$, que $n \longrightarrow a^n$ ¿Qué posibilidades hay para el $\ker \phi$?

15) Halle un subgrupo de $\mathbb{Z} \times \mathbb{Z}$ isomorfo a $\mathbb{Z}$.

16) Sea $\phi : (\mathcal{Q}, \cdot) \longrightarrow (\mathcal{Q}^+, \cdot)$, $x \longrightarrow |x|$. Demuestre que ϕ es un homomorfismo sobre ¿Cuál es el $\ker \phi$?

17) Demuestre que U_{10} es isomorfo a $(\mathbb{Z}_4, +)$.

18) Demuestre que $(\mathbb{R}, +)$ es isomorfo a $(\mathbb{R}^+, \cdot)$.

19) Sea G un grupo cíclico de orden m. Demuestre que G tiene $\phi(m)$ generadores.

20) Demuestre que S_3 no es isomorfo a $(\mathbb{Z}_6, +)$

21) Demuestre que todo grupo cíclico de orden n es isomorfo a $(\mathbb{Z}_n, +)$.

22) Demuestre que todo grupo cíclico infinito es isomorfo a $(\mathbb{Z}, +)$.

23) Sea $H = (6\mathbb{Z}, +)$ el conjunto de enteros multiplos de 6. Demuestre usando el primer teorema de isomorfismos que

$$\mathbb{Z}/6\mathbb{Z} \approx \mathbb{Z}_6$$

24) Sea G el grupo diédrico, definido por los símbolos $x^i y^j$ sujeto a las relaciones

$$x^2 = e, \quad y^n = e, \quad xy = y^{-1}x.$$

Probar que:
a) El subgrupo $N = \{e, y, y^2, \ldots, y^{n-1}\}$ es normal en G.
b) $G/N \approx W$, donde $W = \{1, -1\}$ subgrupo de los números reales bajo la multiplicación.

25) Sea G el grupo diédrico de orden 4, el cual lo denotamos por D_4. Los elememntos de D_4 son los símbolos $x^i y^j$ con

$$x^2 = e, \quad y^4 = e, \quad xy = y^{-1}x$$

Hallar un subgrupo de S_4 tal que sea isomorfo a D_4.

4.5 Grupos de Automorfismos

Definición 4.5.1 *Sea G un grupo. Una aplicación $\phi : G \longrightarrow G$, la cual es un isomorfismo, se llama un* **automorfismo de** G.

El conjunto de todos los automorfismo de G, se denota por $A(G)$

Teorema 4.5.1 *Sea G un grupo. Entonces $A(G)$ es un grupo.*

Demostración: Sean $\phi_1, \phi_2 \in A(G)$. Entonces

$$\begin{aligned} \phi_1\phi_2(xy) &= \phi_1(xy)\phi_2 \\ &= [\phi_1(x)\phi_1(y)]\phi_2 \\ &= \phi_1\phi_2(x)\phi_1\phi_2(y) \end{aligned}$$

Luego

$$\phi_1\phi_2 \in A(G), \quad \forall x, y \in G$$

Además si $\phi \in A(S)$, ϕ^{-1} existe y es biyectiva. Sean $x_1, x_2 \in G$. Luego

$$\phi^{-1}(x_1) = y_1, \quad \phi^{-1}(x_2) = y_2$$

y

$$\begin{aligned}
\phi(\phi^{-1}(y_1y_2)) &= y_1y_2 \\
&= \phi^{-1}(x_1)\phi^{-1}(x_2) \\
&= \phi^{-1}(\phi(y_1))\phi^{-1}(\phi(\phi(y)) \\
&= \phi(\phi^{-1}(y_1))\phi(\phi^{-1}(y_2)) \\
&= \phi(\phi^{-1}(y_1)\phi^{-1}(y_2))
\end{aligned}$$

Como ϕ es inyectiva, se tiene entonces

$$\phi^{-1}(y_1y_2) = \phi^{-1}(y_1)\phi^{-1}(y_2).$$

Con esto termina la demostración.

♠

El problema que vamos a atacar ahora es el de determinar el conjunto $A(G)$, dado un grupo G.

Ejemplo 1: Si G es abeliano entonces la aplicación

$$\begin{array}{rccc} \phi & : & G & \longrightarrow & G \\ & & x & \longrightarrow & x^{-1} \end{array}$$

es un automorfismo.

Ejemplo 2: Si G es no abeliano entonces para cada $g \in G$, definimos

$$\begin{array}{rccc} T_g & : & G & \longrightarrow & G \\ & & x & \longrightarrow & g^{-1}xg \end{array}$$

Entonces Tg es un automorfismo (verificarlo!) llamado **automorfismo interno de** G.

El conjunto de los automorfismo internos de G, será denotado por $I(G)$

Teorema 4.5.2 *Sea G un grupo cualquiera, entonces*

$$I(G) = \{T_g \mid g \in G\}$$

es un subgrupo del grupo $A(G)$, de automorfismos de G.

Demostración: Sean $T_{g_1}, T_{g_2} \in I(G)$. Luego

$$\begin{aligned} T_{g_1}T_{g_2}(x) &= (g_1^{-1}xg_1)T_{g_2} \\ &= g_2^{-1}g_1^{-1}xg_1g_2 \\ &= (g_1g_2)^{-1}x(g_1g_2) \\ &= T_{g_1g_2}(x) \quad \forall x \in G \end{aligned}$$

Luego

$$Tg_1Tg_2 = Tg_1g_2 \tag{4.3}$$

y por lo tanto $I(G)$ es cerrado bajo el producto. Además si $Tg \in I(G)$

$$TgTg^{-1} = Te = I, \quad \text{por la fórmula (??)}$$

Luego

$$(Tg)^{-1} = Tg^{-1} \in I(G.)$$

♠

Definición 4.5.2 *Sea G un grupo. Un subgrupo H de G se llama* **subgrupo característico**, *si para todo automorfismo T de G, se tiene $T(H) \subset H$.*

Observación Si H es un subgrupo característico de G, entonces H es normal en G. Para ver esto, sea $g \in G$. Entonces el automorfismo interno $T_g : G \longrightarrow G$ satisface $T_g(H) \subset H$. Luego se tiene $ghg^{-1} \in H$, para todo h en H. Por lo tanto H es normal.

El reciproco de este resultado no es cierto en general. Existen subgrupos normales que no son característicos, como se verá en el siguiente ejemplo.

Ejemplo 1: Sea $G = \mathbb{Z} \times \mathbb{Z}$ con la operación de suma de coordenadas. Sea $H = 2\mathbb{Z} \times 3\mathbb{Z}$, el cual es un subgrupo de G, y además es normal. Sin embargo, H no es característico, pues al considerar el automorfismo

$$\begin{array}{rccc} \phi & : & G & \longrightarrow & G \\ & & (a,b) & \longrightarrow & (b,a) \end{array}$$

no se tiene $T(H) \subset H$. Sea G un grupo cualquiera entonces **el centro de** G es el conjunto

$$Z = \{x \in G \mid xg = gx \ \forall g \in G\}$$

Se puede verificar que Z es un subgrupo normal de G.

Teorema 4.5.3 *Sea G un grupo y $I(G)$ el grupo de automorfismos internos. Entonces*

$$I(G) \approx G/Z.$$

Demostración: Sea

$$\begin{array}{rccc} \phi & : & G & \longrightarrow & I(G) \\ & & g & \longrightarrow & T_g \end{array}$$

Entonces ϕ es un homomorfismo sobreyectivo.
En efecto, sean $g_1, g_2 \in G$. Luego

$$\phi(g_1 g_2) = T_{g_1 g_2} = T_{g_1} T_{g_2} \quad \text{por fórmula (??)}$$

Además ϕ es sobre.

Por otro lado, si $g \in Z$ entonces es claro que $T_g = 1$ es la identidad. Luego

$$Z \subseteq \ker \phi$$

Si $g \in \ker g$ entonces

$$Tg(x) = g^{-1}xg = x, \quad \text{para todo } x \in G.$$

Luego

$$xg = gx, \quad \text{para todo } x \in G$$

lo cual implica que

$$\ker \phi \subseteq Z$$

Por lo tanto hemos demostrado que $Ker(\phi) = Z$, y usando el primer teorema de los homomorfismos, se concluye

$$G/\ker \phi \approx I(G)$$

Luego

$$G/Z \approx I(G)$$

♠

A continuación, determinaremos todos los automorfismos de un grupo cíclico G, de orden r.

Teorema 4.5.4 *Sea $G =< g >$ un grupo cíclico de orden r. Entonces $A(G) \approx U_r$, donde U_r es el grupo de enteros módulo r con la multiplicación.*

Demostración: Sea $T \in A(G)$, entonces si g es un generador se tiene

$$T(g^i) = T^i(g) \quad \text{para todo } 1 \leq i$$

Luego para determinar un automorfismo T, basta con determinar la imagen de $T(g)$.

Ahora bien, como $T(g)$ debe tener el mismo orden que g, se tiene que $T(g)$ es un generador de G.

Luego la aplicación

$$\begin{array}{rccc} \psi & : & A(G) & \longrightarrow & U_r \\ & & T_i & \longrightarrow & i \end{array}$$

donde $T_i(g) = g^i$ es un isomorfismo (verificarlo!).

♠

Ejercicios

1) Hallar todos los automorfismos de $\mathbb{Z}_4$.

2) Demuestre que $A(\mathbb{Z}) \approx \mathbb{Z}_2$

3) Demuestre que para $G = S_3$ se tiene $I(G) \approx S_3$

4) Sea G un grupo y G' el subgrupo conmutador. Probar que G' es un grupo característico.

5) Sea G un grupo de orden 9, generado por los elementos a, b, donde $a^3 = b^3 = e$. Hallar todos los automorfismos de G.

Capítulo

5

Permutaciones

5.1 Introducción

Las permutaciones son el ejemplo de grupo finito que más se utiliza dentro de la teoría de grupos. Su importancia se debe a que todo grupo es isomorfo a un grupo de permutaciones, por un lado, y por otro, el grupo de las permutaciones de las raíces de un polinomio, permite determinar la solubilidad de una ecuación algebráica asociada a él, resultado este que se conoce con el nombre de Teoría de Galois.

El problema de la resolución de ecuaciones algebráicas de grado superior a 4, fue atacado por el matemático Noruego Niels Henrik Abel (1802-1829) quien en 1824 publicó una memoria titulada " *Sobre la Resolución de Ecuaciones Algebráicas*", en donde se da la primera prueba de la imposibilidad de resolver en general la ecuación de grado 5, usando radicales.

Dicho en otras palabras, Abel probó que no existe una fórmula general para resolver ecuaciones de grado mayor que 4.

Anteriormente Carl F. Gauss había resuelto un famoso problema, planteado desde la época de los griegos sobre la posibilidad de construir con regla y compás un polígono regular. Este problema se reduce a resolver la ecuación

$$ax^n + b = 0$$

con a y b enteros, usando raíces.

El matemático francés Evarist Galois (1810-1832) inspirandose en ambos trabajos, se planteó el problema aún más general:

Dar un criterio para solubilidad de la ecuación

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 = 0 \tag{5.1}$$

por medio de radicales.

Galois obtuvo un método muy interesante, que ha sido uno de los aportes más grandes a la matemáqtica, y en donde el grupo de permutaciones de las raíces del polinomio en (**??**) nos da toda la información necesaria. Este resultado dice "*La ecuación (**??**) es soluble si y sólo si el grupo de permutaciones de las raíces es soluble*".

Al final de este capítulo se da una demostración completa de la simplicidad de los grupos alternantes A_n para $n \geq 5$, lo cual prueba que estos grupos no son solubles y este resultado es así, equivalente a probar que la ecuación (**??**) no se puede resolver por radicales.

5.2 Teorema de Cayley

En 1854 el matemático inglés Arthur Cayley (1824-1895) escribió un artículo titulado "*Notas sobre la teoría de permutaciones*", donde se demuestra uno de los teoremas más importantes de toda la teoría de grupos.

Dicho teorema establece que todo grupo finito es isomorfo a algún grupo de permutaciones. Esto demuestra el poder unificador de la teoría de grupos, al poder condensar en un sólo grupo abstracto, todos los grupos provenientes de las distintas áreas de matemática.

Teorema 5.2.1 *(Cayley) Sea G un grupo finito. Entonces G es isomorfo a un grupo de H, donde H, es un subgrupo de S_n, para algún n.*

Demostración: Consideremos a G como un conjunto solamente y sea $A(G)$ el grupo de aplicaciones biyectivas de G en si mismo. Para cada $g \in G$ se tiene una aplicación

$$\begin{array}{rccc} \phi_g & : & G & \longrightarrow & G \\ & & x & \longrightarrow & xg \end{array}$$

ϕ_g se llama una **traslación a la derecha inducida por** g. Es fácil verificar entonces que ϕ_g define una biyección y por lo tanto $\phi_g \in A(G)$ para todo g en G.

Luego tenemos una función

$$\begin{array}{rccc} \phi & : & G & \longrightarrow & A(G) \\ & & g & \longrightarrow & \phi_g \end{array}$$

Afirmamos que ϕ es un homomorfismo de grupos. En efecto, sean g_1, g_2 en G. Luego

$$\begin{aligned} \phi(g_1 g_2)(x) &= (g_1 g_2)x \\ &= g_1(g_2 x) \\ &= g_1 \phi_{g_2}(x) \\ &= \phi_{g_1}(\phi_{g_2}(x)) \\ &= \phi_{g_1}\phi_{g_2}(x) \end{aligned}$$

Por lo tanto

$$\phi(g_1 g_2) = \phi_{g_1}\phi_{g_2} = \phi(g_1)\phi(g_2)$$

Además ϕ es inyectiva. Supongamos que $\phi(g) = I$. Luego $\phi_g(x) = x$ para todo x en G, y por lo tanto $\phi_g(e) = e$, lo cual implica $ge = e$, de donde $g = e$.

Si tomamos H la imagen de ϕ, en $A(G)$, entonces se tiene que

$$G \approx H$$

Observación: El teorema de Cayley, si bien es muy importante desde el punto de vista teórico, no tiene mucha aplicación práctica, pues el grupo $A(G)$ es inmenso comparando con G. Por ejemplo, si el orden de G es 20, entonces $A(G)$ tiene orden 20! ¿Cómo hacemos para hallar este pequeño grupo de orden 20 dentro de un grupo de orden 2432902008176640000?

5.3 Descomposición Cíclica

Sea S un conjunto finito de n elementos. Estudiaremos en detalle **el grupo de permutaciones de** S, el cual se denota por $A(S)$.

Sea $S = \{x_1, \ldots, x_n\}$ entonces si θ es una permutación de S podemos representarla en la forma

$$\theta = \begin{pmatrix} x_1 & x_2 & \cdots & x_n \\ x_{i_1} & x_{i_2} & \ldots & x_{i_n} \end{pmatrix},$$

donde $\theta x_1 = x_{i_1}, \theta x_2 = x_{i_2}, \ldots, etc.$

Podemos simplificar esta notación, eliminado las x, para obtener

$$\theta = \begin{pmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \ldots & i_n \end{pmatrix}$$

Así pues una permutación del conjunto S, se puede representar, sin ambigüedad, por una permutación del conjunto $\{1, 2, \ldots, n\}$. El conjunto de estas prmutaciones se denota por S_n y se llama **Grupo Simétrico de grado** n.

Observación: Cuando se tienen dos permutaciones θ y τ en S_n, el producto $\theta\tau$ se interpreta de la forma siguiente:

$$\theta\tau(m) = \tau(\theta(m)),$$

para todo $m \in \{1, 2, \ldots, n\}$.

Es decir, convenimos en "leer" el producto de permutaciones de izquierda a derecha. Otros autores lo hacen en sentido contrario, pero en todo este trabajo usamos siempre la misma convención.

Por ejemplo si θ, τ en S_6 son de la forma

$$\theta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 1 & 4 & 5 & 6 \end{pmatrix}$$

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 1 & 2 & 5 & 6 \end{pmatrix}$$

Entonces

$$\theta\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 1 & 3 & 2 & 5 & 6 \end{pmatrix}$$

$$\tau\theta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 4 & 2 & 3 & 5 & 6 \end{pmatrix}$$

Nótese que

$$\theta\tau \neq \theta\tau.$$

y por lo tanto S_n no es abeliano, para $n > 2$.

Definición 5.3.1 *Sea $\theta \in S_n$ y m un elemento del conjunto*

$$\{1, 2, \ldots, n\}.$$

Diremos que la permutación θ:

1) **Mueve** *a m si $\theta(m) \neq m$*

2) **Fija** *a m si $\theta(m) = m$.*

Observación: El conjunto de los elementos de $\{1, 2, \ldots, n\}$ que son movidos por una permutación σ, se denota por A_σ y se llama **el soporte de la permutación**.

Por ejemplo, si σ y θ son las dos permutaciones dadas con anterioridad, tendremos:

$$A_\sigma = \{1, 2, 3\} \text{ y } A_\theta = \{1, 2, 3, 4\}$$

Definición 5.3.2 *Dos premutaciones σ y θ_1 se dicen* **permutaciones disjuntas**, *si $A_\sigma \cap A_\theta = \phi$.*

Ejemplo: 1 En S_6 consideremos las permutaciones

$$\theta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 1 & 4 & 5 & 6 \end{pmatrix}$$

y

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 6 & 5 & 4 \end{pmatrix}$$

entonces θ y σ son disjuntas.

Teorema 5.3.1 *Sean θ_1 y θ_2 permutaciones disjuntas en S_n. Entonces ellas conmutan, es decir*

$$\theta_1\theta_2 = \theta_2\theta_1.$$

Demostración: Sea $m \in \{1, 2, \ldots, n\}$ y consideremos las tres posibilidades:

1) θ_1 y θ_2 fijan a m.

2) θ_2 mueve a m.

3) θ_1 mueve a m.

1) En este caso se tiene

$$\theta_1\theta_2(m) = m = \theta_2\theta_1(m)$$

luego ellas conmutan.

2) Supongamos $\theta_1(m) = m$ y $\theta_2(m) = k$ con $k \neq m$. Entonces $\theta_1(k) = k$, pues θ_2 mueve a k.

Luego

$$\theta_1\theta_2(m) = \theta_2(m) = k$$
$$\theta_2\theta_1(m) = \theta_1(k) = k$$

es decir

$$\theta_1\theta_2(m) = \theta_2\theta_1(m)$$

3) Si $\theta_1(m) = t$, con $t \neq m$, se tiene que $\theta_2(m) = m$.

Además $\theta_2(t) = t$, pues θ_1 mueve a t. Luego

$$\theta_1\theta_2(m) = \theta_2(t) = t$$
$$\theta_2\theta_1(m) = \theta_1(m) = t$$

esto es

$$\theta_1\theta_2(m) = \theta_2\theta_1(m)$$

Por lo tanto hemos probado que

$$\theta_1\theta_2 = \theta_2\theta_1$$

♠

Definición 5.3.3 *Una permutación $\theta \in S_n$ se llama* **un ciclo**, *si existen elementos s_1, $s_2, \ldots s_k$ en el conjunto $\{1, 2, \ldots, s\}$ tales que*

1. *Se tienen las relaciones $\theta(s_1) = s_2$, $\theta(s_2) = s_3 \ldots \theta(s_{k-1}) = s_k$ y $\theta(s_k) = s_1$.*
2. *La permutación θ deja fijo a todos los elementos de $\{1, 2, \ldots, n\}$ distintos de los s_i.*

Para expresar la permutación anterior, se usa la notación cíclica.

$$\theta = (s_1, s_2, \ldots, s_k)$$

Definición 5.3.4 *El entero k en la definición de arriba, se llama* **la longitud de la permutación**

Ejemplo: 1 La permuatción $\sigma \in S_7$ dada por

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 1 & 3 & 4 & 7 & 6 & 2 \end{pmatrix}$$

es un ciclo, ella se denota por $\sigma = (1,\ 5,\ 7,\ 2)$

Definición 5.3.5 *Sea θ una permutación de S_n y $s \in \{1, 2, \ldots, n\}$, entonces el conjunto*

$$\theta_s = \{s, \theta(s), \theta^2(s), \ldots\}$$

se llama la **órbita de** *s bajo la permutación θ.*

Lema 5.3.1 *Para todo $s \in \{1, 2, \ldots, n\}$ existe un entero positivo k, el cual depende de s. tal que*

$$\theta_s = \{s, \theta(s), \ldots, \theta^{k-1}(s)\}.$$

Demostración: Nótese que el conjunto

$$s, \theta(s), \theta^2(s), \ldots, \theta^n(s), \ldots$$

es finito.

Luego debe haber repeticiones entre estos elementos y por lo tanto existen subíndices i, j con $i < j$ tales que

$$\theta^i(s) = \theta^j(s)$$

es decir,

$$\theta^{i-j}(s) = s$$

Luego si, se toma $t = i - j$ y por lo tanto se cumple

$$\theta^t(s) = s$$

Sea

$$k = \min\{t \mid \theta^t(s)\}$$

Afirmamos que los elementos $s, \theta(s), \ldots, \theta^{k-1}(s)$ son todos distintos. En efecto, si hay una repetición, digamos para $h < \ell$, con $0 \leq h < k$ y $0 \leq \ell < k$

$$\theta^h(s) = \theta^\ell(s)$$

entonces

$$\theta^{\ell-h}(s) = s, \quad \text{y} \;\; 0 \leq \ell - h < k$$

Esto contradice la minimalidad de k y por lo tanto $\theta^h(s)$ y $\theta^\ell(s)$ son distintos.

Por otro lado, si n es cualquier entero positivo, se tiene

$$n = p \cdot k + r, \quad \text{con} \;\; 0 \leq r < k$$

y por lo tanto

$$\begin{aligned} \theta^n(s) &= \theta^{p\cdot k+r}(s) \\ &= \theta^r(\theta^{p\cdot k}(s)) \\ &= \theta^r(s) \end{aligned}$$

Con esto se da fin a la prueba.

♠

Observación: Si θ es una permutación en S_n, entonces la relación en s

$$s_1 \sim s_2 \iff s_1 = \theta^i(s_2),$$

para algún i entero, es de equivalencia.

Además cada clase de equivalencia es una órbita de la permutación. El conjunto $\{1, 2, \ldots, n\}$ queda así dividido en la unión de órbitas disjuntas.

Cada órbita de θ origina la permutación

$$\Big(s, \theta(s), \ldots, \theta^{\ell-1}(s)\Big)$$

Este tipo de permutación se llama un **ciclo**.

Ejemplo: Consideremos la permutación

$$\theta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 4 & 8 & 5 & 9 & 7 & 6 & 1 & 2 \end{pmatrix}$$

Entonces las distintas órbitas son

$$\begin{aligned} \theta_1 &= \{1, 3, 8\} \\ \theta_2 &= \{2, 4, 5, 9\} \\ \theta_6 &= \{6, 7\} \end{aligned}$$

y los ciclos correspondientes vienen dados por:

$$\begin{aligned} c_1 &= (1, 3, 8) \\ c_2 &= (2, 4, 5, 9) \\ c_3 &= (6, 7) \end{aligned}$$

Teorema 5.3.2 *Toda permutación se escribe como un producto de ciclos disjuntos.*

Demostración: Descomponer el conjunto $\{1, 2, \ldots, n\}$ en la unión disjuntas de sus órbitas. Luego formar los ciclos $c_1, \ldots, c_t$.

Afirmamos que

$$\theta = c_1 \cdots c_t$$

En efecto, sea $s \in \{1, 2, \ldots, n\}$. Entonces s aparece en sólo uno de los ciclos, digamos c_i, luego

$$\begin{aligned} c_1 \cdots c_t(s) &= c_1 \cdots c_i(s) \\ &= c_1 \cdots c_{i-1}(\theta(s)) \\ &= \theta(s) \end{aligned}$$

♠

Definición 5.3.6 *Un ciclo de longitud 2 se llama una* **transposición**.

Nota: Si θ es el ciclo $\theta = (s_1, \ldots, s_t)$, entonces se demuestra la fórmula:

$$\theta = (s_1, s_2)(s_1, s_3) \cdots (s_1, s_t) \tag{5.2}$$

Teorema 5.3.3 *Toda permutación se puede escribir como un producto de transposiciones.*

Demostración: Hemos probado que toda permutación se escribe como un producto de ciclos. Si ahora usamos la fórmula (**??**), para descomponer cada ciclo como un producto de transposiciones, se obtiene el resultado deseado.

♠

Ejemplo: La permutación θ del ejemplo anterior, puede ser descompuesta en ciclos:

$$\begin{aligned} \theta &= (1,3,8)(2,4,5,9)(6,7) \\ &= (1,3)(1,8)(2,4)(2,5)(2,9)(6,7) \end{aligned}$$

Ejercicios

1) Sean θ y τ las permutaciones en S_8 dadas por

$$\theta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 7 & 3 & 4 & 2 & 6 & 5 & 1 & 8 \end{pmatrix}$$

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 8 & 3 & 6 & 4 & 5 & 7 & 1 \end{pmatrix}$$

Hallar

a) $\theta\tau$

b) $\tau\theta$

c) $\tau^{-1}\theta^{-1}$

d) $\theta^3\tau^3$

e) $\theta\tau\theta^{-1}$

2) Sea A el conjunto de permutaciones en S_6 que conmutan con la permutación $\theta = (1, 2, 4)$. Probar que A es un subgrupo de S_6. ¿Cuál es el orden de A?

3) Probar que el orden de un ciclo en S_n es igual a su longitud.

4) Probar la fórmula en S_n

$$(1, 2, \ldots, n)^{-1} = (n, n-1, n-2, \ldots, 2, 1)$$

5) Sea $\theta \in S_n$. Sean a, b en $\{1, 2, \ldots, n\}$ y diremos que a y b están relacionados si

$$a = \theta^t(b)$$

para algún $t \in \mathbb{Z}$. Probar que ésta relación es de equivalencia en $\{1, 2, \ldots, n\}$.

6) Calcule el número de órbitas de $\theta = (3, 5, 7)$ en S_9.

7) Sean θ_1 y θ_2 dos ciclos disjuntos de ordenes m y n con $(m, n) = 1$. Probar que el orden de $\theta_1\theta_2$ es mn.

8) Sean $\theta_1, \ldots, \theta_s$ ciclos disjuntos de ordenes $m_1, \ldots, m_s$ ¿Cuál es el orden de $\theta_1 \ldots, \theta_s$?.

9) Sea $G = D_n$ el grupo diédrico de grado n. Hallar la representación de este grupo como un grupo de permutaciones en S_n.

5.4 Grupo Alternante

Definición 5.4.1 *Una permutación θ en S_n se llama* **permutación par** *si se puede descomponer como un número par de transposiciones.*

Si una permutación se descompone como un número impar de transposiciones, entonces diremos que es **impar.**

Una permutación no puede ser par e impar a la vez, como veremos a continuación:

Teorema 5.4.1 *Sea $\theta \in S_n$ una permutación. Entonces θ no puede ser descompuesta como un producto de un número par de transposiciones e impar de transposiciones simultáneamente.*

Demostración: La prueba la dividimos en dos casos:

Caso I: Si $\theta = I$ la permutación identidad. Entonces afirmamos que θ sólo puede ser descompuesta como un número par de transposiciones.

En efecto, si

$$I = \alpha_1 \cdots \alpha_k \tag{5.3}$$

donde cada α_i es una transposición, probaremos que k debe ser par.

Sea s un entero en el conjunto $\{1, 2, \ldots, n\}$ tal que s es movido por algunas de las transposiciones en (**??**) y supongamos que α_j es la primera transposición que mueve a m. Entonces, debe ser $j < k$, pues si la última transposición mueve a m, y ninguna de las anteriores lo hace, el producto en (**??**) no es la identidad.

Sea $\alpha_j = (m, x)$, donde $x \in \{1, 2, \ldots, n\}$. Entonces tenemos dos posibilidades para la siguiente permutación a la derecha α_j, la cual denotamos por α_{j+1}.

1) Si α_{j+1} mueve a m, entonces el producto $\alpha_j\alpha_{j+1}$ se reduce a algunos de los siguientes casos:

$$\alpha_j\alpha_{j+1} = (x, m)(x, m) = I$$
$$\alpha_j\alpha_{j+1} = (x, m)(y, m) = (x, y)(x, m)$$

2) Si α_{j+1} no mueve a m, entonces el producto $\alpha_j\alpha_{j+1}$ se expresa de alguna de las dos formas

$$\alpha_j\alpha_{j+1} = (x,m)(y,z) = (y,z)(x,m)$$
$$\alpha_j\alpha_{j+1} = (x,m)(x,y) = (x,y)(y,m)$$

En conclusión se tiene que α_{j+1} es la primera transposición que mueve a m o bien m desaparece en (**??**), eliminando dos transposiciones. Continuando este proceso se pueden cancelar todas las transposiciones en (**??**), hasta tener la identidad en ambos lados. Luego k debe ser par.

Caso II: Sea θ una permutación cualquiera en S_n y consideremos dos posibles descomposiciones de esta, como producto de transposiciones

$$\theta = \alpha_1 \cdots \alpha_k = \beta_1 \cdots \beta_t$$

Luego

$$\begin{aligned} \theta\theta^{-1} &= \alpha_1 \cdots \alpha_k(\beta_1 \cdots \beta_t)^{-1} \\ &= \alpha_1 \cdots \alpha_k\beta_t^{-1} \cdots \beta_1^{-1} \\ &= \alpha_1 \cdots \alpha_k\beta_t \cdots \beta_1 \end{aligned}$$

pues β_i es una transposición, y por lo tanto

$$\beta_i^{-1} = \beta_i.$$

luego se tiene

$$I = \alpha_1 \cdots \alpha_k\beta_t \cdots \beta_1,$$

y usando el primer caso se concluye que $\alpha + t$ debe ser par. Luego α y t deben ser ambos pares o impares.

Definición 5.4.2 *Una permutación θ en S_n, se dice* **par** *(respectivamente* **impar***) si θ se puede expresar como el producto de un número par (respectivamente impar) de transposiciones.*

El producto de dos permutaciones pares es de nuevo una permutación par. Además si θ es par, su inverso θ^{-1} es también una permutación par.

Luego el conjunto de las permutaciones pares de S_n, es un grupo el cual se denomina **Grupo Alternante de grado n** y se denota por A_n.

Teorema 5.4.2 *El grupo alternante A_n, es un subgrupo normal de S_n y tiene orden*

$$\circ(A_n) = n!/2$$

Demostración: Sea U el grupo formado por 1 y -1 bajo el producto de los números enteros. Consideremos la aplicación

$$\varphi : S_n \longrightarrow U$$

$$\varphi(\theta) = \begin{cases} 1, & \text{si} \quad \theta \text{ es par} \\ -1, & \text{si} \quad \theta \text{ es impar} \end{cases}$$

Entonces se puede verificar fácilmente que φ es un homomorfismo de grupos, el cual es sobre. ¿Quién es el Kernel de φ?

Tenemos que $\ker \varphi$ son exactamente aquellas permutaciones pares, esto es el grupo A_n. Además por el primer teorema de los isomorfismos, obtenemos

$$S_n/\ker \varphi = S_n/A_n \approx U,$$

luego

$$\circ(S_n/A_n) = \circ(U) = 2$$

pero

$$\circ(S_n/A_n) \quad = \quad \frac{\circ(S_n)}{\circ(A_n)} = \frac{n!}{\circ(A_n)}$$

y de esto se concluye

$$\circ(A_n) = \frac{n!}{2}$$

♠

5.5 Simplicidad de A_n $(n \geq 5)$

En esta sección se demuestra uno de los hechos más resaltantes sobre el grupo de permutaciones, como lo es la simplicidad del grupo alternante A_n, para $n \geq 5$.

Este resultado tiene profundas y sorprendentes concecuencias cuando se considera el grupo de permutaciones de las raíces de un polinomio de grado mayor o igual a 5 sobre los racionales. La simplicidad de A_n en este contexto implica la imposibilidad de obtener dichas raíces usando radicales.

Sin embargo no podemos estudiar con detalle esta aplicación. Para la misma se requieren algunos conocimientos de la teoría de cuerpos que no están a nuestro alcance en este momento.

Definición 5.5.1 *Un grupo G se dice* **simple** *si no posee subgrupos normales diferentes de los triviales.*

Lema 5.5.1 *Sean $\varphi = (1,2)$ y $\psi = (1,2,\ldots,n)$. Entonces S_n es generado por estas dos permutaciones.*

Demostración: La prueba se hará en varios pasos:

1) Demostraremos que φ, ψ generan todas los transposiciones

$$(1,2),(1,3),\ldots,(1,n)$$

2) Probaremos que esas transposiciones generan todas las transposiciones.

3) Luego cada $\sigma \in S_n$ al ser generada por un producto de transposiciones, es generada por φ y ψ.

Iniciamos la demostración calculando algunos valores de $\psi^{-n}\varphi\psi^n$.

$$\begin{aligned} \psi^{-1}\varphi\psi(1) &= (n)\varphi\psi \\ &= (n)\psi \\ &= 1 \end{aligned}$$

$$\begin{aligned} \psi^{-1}\varphi\psi(2) &= (1)\varphi\psi \\ &= (2)\psi \\ &= 3 \end{aligned}$$

$$\begin{aligned} \psi^{-1}\varphi\psi(3) &= (2)\varphi\psi \\ &= (1)\psi \\ &= 2 \end{aligned}$$

Si $3 < s \leq n$

$$\begin{aligned} \psi^{-1}\varphi\psi(s) &= (s-1)\varphi\psi \\ &= (s-1)\psi \\ &= s \end{aligned}$$

Luego hemos probado

$$\begin{aligned} \psi^{-1}\varphi\psi(1) &= (2,3) \\ &= (\psi(1), \psi(2)) \end{aligned}$$

En general, probaremos la fórmula

$$\psi^{-k}\varphi\psi^k = (\psi^k(1), \psi^k(2)) \tag{5.4}$$

Es más, si φ es cualquier ciclo $\varphi = (a_1, \ldots, a_s)$. Entonces se tiene

$$\psi^{-k}\varphi\psi^k = (\psi^k(a_1), \ldots \psi^k(a_s)) \tag{5.5}$$

para todo k, $1 \leq k \leq n$.

Para probar (**??**), notemos en primer lugar que

$$\begin{aligned}(\psi^k(1))\psi^{-k}\varphi\psi^k &= (1)\varphi\psi^k \\ &= 2\psi^k \\ &= \psi^k(2),\end{aligned}$$

y además

$$\begin{aligned}(\psi^k(2))\psi^{-k}\varphi\psi^k &= (2)\varphi\psi^k \\ &= 1\psi^k \\ &= \psi^k(1)\end{aligned}$$

Por otro lado, sea $t \neq \psi^k(1), \psi^k(2)$, entonces como ψ^k es biyectiva, existe $x \neq 2, 1$ tal que

$$t = \psi^k(x)$$

luego

$$\begin{aligned}(t)\psi^{-k}\varphi\psi^k &= (\psi^k(x))(\psi^{-k}\varphi\psi^k) \\ &= (x)\varphi\psi^k \\ &= (x)\psi^k \\ &= \psi^k(x) \\ &= t\end{aligned}$$

Luego el elementos t no es movido por esa permutación y por lo tanto

$$\psi^{-k}\varphi\psi^k = (\psi^k(1), \psi^k(2))$$

De esta forma las permutaciones φ, ψ generan todas las transposiciones

$$(1,2)(2,3)(3,4)\cdots(n-1,n)$$

¿Como generamos una permutación del tipo $(1, a)$ con $2 \leq a \leq n$?

Simplemente usamos la fórmula de recurrencia

$$(1, a-1)(a-1, a)(1, a-1) = (1, a). \tag{5.6}$$

2) Si (a, b) es cualquier transposición, entonces

$$(1, a)(1, b)(1, a) = (a, b)$$

Luego (a, b) es generado por φ, ψ.

3) Si θ es cualquier permutación, entonces

$$\theta = \theta_1 \cdots \theta_t$$

donde cada θ_i es una transposición. Con esto se da fin a la prueba.

♠

Lema 5.5.2 *Probar que para $n \geq 3$, el grupo generado por los $3-$ciclos es A_n.*

Demostración: Sea H =subgrupo de S_n generado por los $3-$ciclos. Como cada $3-$ciclo es de la forma:

$$(a, b, c) = (a, b)(a, c),$$

se tiene que

$$H \subseteq A_n$$

Luego si $\theta \in A_n$, entonces θ es producto de un número par de transposiciones.

Si demostramos que el producto de dos transposiciones es un $3-$ciclo o producto de $3-$ciclos estará listo.

Tenemos dos casos a considerar

1) $(a, b)(a, c) = (a, b, c)$.

2) $(a, b)(c, d) = (a, b)(a, c)(a, c)(c, d) = (a, b, c)(c, a, d)$.

Por lo tanto los 3-ciclos generan al grupo alternante A_n.

♠

Lema 5.5.3 *A_n, $n \geq 3$ esta generado por $3-$ciclos de la forma*

$$(1,2,3)(1,2,4)\cdots(1,2,n).$$

Demostración: Basta probar que todo ciclo de la forma (a,b,c) esta generado por un producto de los anteriores o sus inversos.

En primer lugar

$$(1,2,b)^{-1}(1,2,c)(1,2,b) = (\psi(1),\psi(2),\psi(c)) \tag{5.7}$$

donde $\psi = (1,2,b)$

luego

$$\begin{aligned}(1,2,b)^{-1}(1,2,c)(1,2,b) &= (2,b,c)\\ (2,b,c)(2,b,a)(2,b,c)^{-1} &= (\psi(2),\psi(b),\psi(a))\end{aligned}$$

donde $\psi = (2,b,c)$

Luego

$$(1,2,b)^{-1}(1,2,c)(1,2,b) = (b,c,a) = (a,b,c)$$

De esta forma obtenemos el $3-$ciclo buscado.

♠

Lema 5.5.4 *Sea N un subgrupo normal de A_n, $(n \geq 3)$. Si N contiene un $3-$ciclo (a,b,c), entonces*

$$N = A_n.$$

Demostración:

$$\begin{aligned}(1,2,a)^{-1}(a,b,c)(1,2,a) &= (\psi(a),\psi(b),\psi(c))\\ &= (1,b,c) \in N\end{aligned}$$

con $\psi = (1, 2, a)$

Sea $\lambda = (b, 2)(c, k) \in A_n$

$$\begin{aligned} \lambda^{-1}(1, b, c)\lambda &= (\lambda(1), \lambda(b), \lambda(c)) \\ &= (1, 2, k) \in N \end{aligned}$$

Luego N contiene todos los 3−ciclos

$$(1, 2, 3)(1, 2, 4) \cdots (1, 2, n)$$

y por lo tanto

$$N = S_n$$

♠

Teorema 5.5.1 *A_n, $(n \geq s)$ es simple.*

Demostración: Sea $N \neq \{e\}$ un subgrupo normal de A_n. Será suficiente con probar que N contiene 3−ciclo.

Sea $\theta \in N$ tal que θ fija el mayor número de elementos del conjunto $\{1, 2, \ldots, n\}$.

Afirmamos que θ es un 3−ciclo. Si θ no es un 3−ciclo, entonces θ mueve más de 3 elementos, luego podemos suponer

1) $\theta = (1, 2, 3, \ldots)$
o bien

2) $\theta = (1, 2)(3, 4) \cdots$

En el primer caso θ mueve 2 elementos más, digamos 4 y 5, pues si $\theta = (1, 2, 3, 4)$ entonces θ es impar.

Sea $\tau = (3, 4, 5) \in A_n$ y hagamos

$$\theta_1 = \tau\theta\tau^{-1} \in N$$

Si θ es como en 1) entonces

$$\theta_1 = (1, 2, 4, 5, \ldots)$$

Si θ es como en 2) entonces

$$\theta_1 = (1, 2)(4, 5) \cdots$$

Luego

$$\theta_1 \neq \theta$$

y por lo tanto

$$\theta_2 = \tau\theta\tau^{-1}\theta^{-1} \neq e$$

Si θ fija un número s de elementos, con $s > 5$, entonces θ_2 fija dicho número. Además, si θ es como en 1)

$$\begin{aligned} \theta_2(1) &= (1)\tau\theta\tau^{-1}\theta^{-1} \\ &= (1)\theta\tau^{-1}\theta \\ &= (2)\tau^{-1}\theta^{-1} \\ &= 2(\theta^{-1}) \\ &= 1 \end{aligned}$$

Luego θ mueve 1,2,3,4,5 y θ_2 fija 1. Por lo tanto θ_2 tiene más elementos fijos que θ, lo cual es una contradicción.

Si θ es como en 2)

$$\begin{aligned} \theta_2(1) &= (1)\tau\theta\tau^{-1}\theta^{-1} \\ &= (1)\theta\tau^{-1}\theta^{-1} \\ &= (1) \end{aligned}$$

$$\begin{aligned} \theta_2(2) &= (2)\tau\theta\tau^{-1}\theta^{-1} \\ &= (2)\theta\tau^{-1}\theta^{-1} \\ &= (2) \end{aligned}$$

Luego θ fija más elementos que θ lo cual es nuevamente una contradicción.

♠

Ejercicios

1) Determine cuales de las siguientes permutaciones en S_8 son pares y cuales son impares.

a) $(1,2,3)(5,2)$

b) $(4,5,6,7)(1,2)$

c) $(1,2,3,4)(7,8)$

d) $(2,8,7,6,4,5)$

e) $(2,4,5)(3,8,1)$

f) $(1,8,7)(2,5,4,3,6)$

2) Sean θ y τ las permutaciones en S_6 dadas por $\theta = (1,2,3)(4,5)$ $\tau = (1,5,7,4)$

Calcular

a) $\theta^{-1}\tau\theta$

b) $\theta^{-k}\tau\theta^k$, para $2 \leq k \leq 6$.

3) Hallar la descomposición en ciclos de

$$\theta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 10 & 1 & 4 & 6 & 5 & 12 & 11 & 9 & 8 & 2 & 7 & 3 \end{pmatrix}$$

4) Determine si la permutación anterior es par.

5) Demuestre que el producto de dos ciclos disjuntos en S_n es conmutativo.

6) Sea $\theta = (a_1, \ldots, a_t)$ un ciclo de S_n y $\psi \in S_n$. Probar la fórmula

$$\psi^{-1}\theta\psi = (\psi(a_1), \ldots, \psi(a_t)).$$

7) Probar la fórmula (**??**)

8) Probar la fórmula (**??**)

9) Probar la fórmula (**??**)

10) Dos permutaciones θ y τ en S_n se dicen **conjugadas**, si existe otra permutación σ en S_n tal que

$$\theta = \sigma\tau\sigma^{-1}.$$

Halle todos los conjugados de la permutación $(1, 2, 3)$ en S_5.

11) Demuestre que si dos ciclos son conjugados, entonces tiene la misma longitud.

Capítulo

6

Estructura de los Grupos

6.1 Introducción

En nuestro viaje dentro de la teoría de grupos, hemos estudiado muchos ejemplos de grupos interesantes, como los grupos de simetría, los enteros módulo m, las permutaciones,...etc, pudiendo reconocer dentro de cada uno de ellos propiedades particulares que los diferenciaban entre sí; como una planta de helecho se diferencia de una de naranja. Hemos realizado un largo recorrido por este hermoso paraje del álgebra, deteniéndonos en cada árbol del bosque, en cada piedra del camino, en cada río que atravesamos a describir con detalle minucioso lo que ibamos descubriendo. Nos dirigimos ahora hacia una colina desde donde se puede otear todo el camino andado, desde muy arriba, y tener una visión más amplia de las cosas que están abajo en los valles.

Con toda la información que tenemos a la mano, podemos hacer un resumen general de todo lo visto en el recorrido, sintetizando en unas pocas ideas el amplio panorama de la teoría de grupos. Se trata entonces de ordenar todo el material estudiado dentro de una estructura general.

Este enfoque estructural facilita la clasificación de los grupos, permite obtener un conocimiento más profundo de ellos y genera una gran cantidad de nuevos ejemplos.

Existe mucha similitud entre el conjunto de los números enteros y el conjunto de los grupos abelianos finitos, desde el punto de vista estructural, como se verá en este capítulo. Los números primos son los elementos básicos a partir de los cuales se generan todos los demás enteros. En el caso de los grupos abelianos finitos, los grupos cíclicos juegan el mismo papel que los números primos, pues ellos son los bloques con los cuales se construyen los otros grupos.

La clasificación de todos los grupos abelianos finitos es, sin duda alguna, una de las más altas realizaciones de toda el álgebra. El primer

paso en alcanzar esta meta viene dado por el teorema Sylow, el cual permite obtener subgrupos de orden una potencia de un primo p, cuando dicha potencia es un divisor del orden del grupo dado. El teorema de Sylow es una herramienta poderosa que permite desmenuzar un grupo grande en pedazos más pequeõs, los p-grupos, de una manera rápida y eficiente, con tan sólo conocer el orden del grupo.

El proceso de clasificación culmina brillantemente con el teorema de la unicidad de los invariantes para grupos de orden una potencia de un primo p, o p-grupos. Si conocemos todos los invariantes de un p-grupo, entonces se conoce su descomposición como producto directo de grupos cíclicos.

6.2 Producto Directo de Grupos

Sean A y B dos grupos y consideremos a A y B como conjuntos. Sea G el producto cartesiano $A \times B$. Podemos definir una operación binaria en $A \times B$ mediante

$$(a_1, b_1) * (a_2, b_2) = (a_1 a_2, b_1 b_2)$$

donde $a_1 a_2$ indica el producto de a_1 con a_2 en el grupo A_1, y $b_1 b_2$ indica el producto de b_1 con b_2 en el grupo B. Probaremos que G con la operación $*$, de multiplicación por coordenadas, es un grupo.

En primer lugar la operación es cerrada, pues los respectivos productos en A y B son cerrados, con lo cual se demuestra que $(a_1 a_2, b_1 b_2)$ es un elemento de G.

Para demostrar la asociatividad, pongamos

$$\begin{aligned}
(a_1, b_1) * [(a_2, b_2) * (a_3, b_3)] &= (a_1, b_1) * (a_2 a_3, b_2 b_3) \\
&= (a_1(a_2 a_3), b_1(b_2 b_3)) \\
&= ((a_1 a_2)a_3), (b_1 b_2)b_3) \\
&= (a_1 a_2, b_1 b_2) * (a_3, b_3) \\
&= [(a_1, a_2) * (a_2, b_2)] * (a_3, b_3)
\end{aligned}$$

Sea e el elemento neutro de A y f el elemento neutro de B. Entonces el elemento (e, f) está en G. Además, si (a, b) es cualquier elemento de

G se tendrá:

$$(e, f) * (a, b) = (ea, fb) = (a, b)$$
$$(a, b) * (e, f) = (ae, bf) = (a, b)$$

Luego (e, f) es el elemento neutro para la operación $*$.

Finalmente, si $(a, b) \in G$, el elemento (a^{-1}, b^{-1}) estará en G, y se tiene entonces

$$(a, b) * (a^{-1}, b^{-1}) = (aa^{-1}, bb^{-1}) = (e, f)$$

y

$$(a^{-1}, b^{-1}) * (a, b) = (a^{-1}a, b^{-1}b) = (e, f)$$

luego el inverso de (a, b) es (a^{-1}, b^{-1}). En conclusión hemos probado que $(G, *)$ satisface todas las propiedades de la definición de grupo.

Además, si A y B son grupos abelianos, entonces $A \times B$ es un grupo abeliano.

Definición 6.2.1 *Sean A y B dos grupos. El grupo $G = A \times B$, con la operación de multiplicación por coordenadas, se llama* **producto directo externo de A y B.**

Observación: Si los grupos A y B son abelianos, entonces $G = A \times B$ se llama la suma directa de A y B y se denota por $A \oplus B$

El producto directo externo de dos grupos, se puede generalizar a cualquier número de grupos. Sean $G_1, \ldots, G_n$ grupos y sea $G = G_1 \times \cdots \times G_n$ el conjunto de $n-$uplas $(g_1, \ldots, g_n)$ con $g_i \in G_i$, $1 \leq i \leq n$.

Definimos la operación de producto en G, multiplicando componente por componente

$$(g_1, \ldots, g_n) * (h_1, \ldots, h_n) = (g_1h_1, \ldots, g_nh_n)$$

Entonces el grupo G con esta operación se llama el **producto directo externo** de $G_1, \ldots, G_n$

Observación: Si se tiene $G = A \times B$, entonces los conjuntos

$$H = \{(a, f) \mid a \in A\} \quad \text{y} \quad K = \{(e, b) \mid b \in B\}$$

son subgrupos de G y además

$$H \cap K = \{(e, f)\}.$$

Con las mismas notaciones anteriores, se tiene la siguiente

Proposición 6.2.1 *Para todo $g \in A \times B$, existen únicos elementos $g_1 \in H$ y $g_2 \in K$ tales que*

$$g = g_1 g_2.$$

Demostración: Sea $g = (a, b)$, entonces

$$\begin{aligned} g &= (a, b) \\ &= (a, f)(e, b) \\ &= g_1 g_2 \end{aligned}$$

con $g_1 \in H$, $g_2 \in K$.

Supongamos ahora que $g = g_1' g_2'$, con $g_1' \in H$ y $g_2' \in K$. Luego $g = g_1 g_2 = g_1' g_2'$, de donde $(g_1')^{-1} g_1 = g_2 (g_2')^{-1} \in H \cap K$. Por lo tanto $(g_1')^{-1} g_1 = e$, lo cual implica $g_1' = g_1$.

Similarmente se demuestra $g_2' = g_2$.

♠

Este resultado se puede generalizar de la manera siguiente:

Proposición 6.2.2 *Sean $G_1, \ldots, G_n$ grupos, y consideremos el producto directo de ellos, $G = G_1 \times \cdots \times G_n$. Para cada i, sea e_i el elemento neutro del grupo G_i y sea*

$$H_i = \{(e_1, \ldots, e_{i-1}, h, e_{i+1}, \ldots, e_n \mid h \in G_i\}$$

entonces los H_i son subgrupos de G y además

1)) $H_i \cap H_j = e$, para $i \neq j$, donde e es elemento neutro de G.

2)) Todo elemento $g \in G$ se expresa de manera única

$$g = h_1 h_2 \cdots h_n$$

donde los h_i están en H_i.

Definición 6.2.2 *Sea G un grupo y $H_1, \ldots, H_n$ subgrupos normales de G, tales que*

1) $G = H_1 \cdots H_n$

2) Para todo $g \in G$, existen elementos únicos $h_i \in H_i$, $1 \leq i \leq n$, tales que

$$g = h_1 \cdots h_n$$

Entonces G se llama el **producto directo interno** *de $H_1, \ldots, H_n$.*

Observación: Más adelante, probaremos que el producto directo externo es isomorfo al producto directo interno, y por lo tanto, al quedar probado este isomorfismo, hablaremos de producto directo, sin ser específicos.

Antes de llegar a ese resultado, necesitamos la siguiente proposición:

Proposición 6.2.3 *Sea $G = N_1 \cdots, N_s$ producto directo interno. Entonces para todo par de subíndices $i \neq j$ se tiene que*

$$N_i \cap N_j = \{e\},$$

y además se cumple

$$ab = ba$$

para cualquier $a \in N_i$, $b \in N_j$

Demostración: Sea $x \in N_i \cap N_j$, entonces de acuerdo con la definición de producto directo interno, existen elementos $g_1, \ldots, g_s$ con $g_i \in N_i$ tales que

$$x = g_1 \cdots g_s \tag{6.1}$$

Por otro lado, podemos representar a x de dos formas distintas

$$x = e_1 e_2 \cdots e_{i-1} x e_{i+1} \cdots e_n$$
$$x = e_1 e_2 \cdots e_{j-1} x e_{j+1} \cdots e_n$$

donde $e_s = e$, es el elemento neutro de G.

Usando la unicidad de la representación en (**??**) se concluye que $x = e$, de donde

$$N_i \cap N_j = \{e\}$$

Si suponemos que $a \in N_i$ y $b \in N_j$, se tiene que $aba^{-1} \in N_j$, puesto que N_j es normal.

Por estar b^{-1} en N_j, se debe tener $aba^{-1}b^{-1} \in N_j$. Pero por otro lado, usando la normalidad de N_i se sigue que $ba^{-1}b^{-1} \in N_i$, y entonces $aba^{-1}b^{-1} \in N_i$.

Combinando ambos resultados se obtiene

$$aba^{-1}b^{-1} \in N_i \cap N_j = \{e\}$$

De donde

$$ab = ba$$

♠

Teorema 6.2.1 *Sea $G = N_1 \cdots N_s$ producto directo interno y $G' = N_1 \times \cdots \times N_s$ producto directo externo, entonces*

$$G \approx G'.$$

Demostración: Consideremos la aplicación

$$\psi : G' \longrightarrow G$$
$$\psi(g_1, \ldots, g_s) = g_1 \cdots g_s$$

Entonces ψ esta bien definida, pues cada g_i pertenece a G, luego el producto de los g_i esta en G.

Sean $x, y \in G'$ y probemos que

$$\psi(x, y) = \psi(x)\psi(y)$$

Se tiene

$$x = (g_1, \ldots, g_s),\ y = (h_1, \ldots, h_s) \quad \text{con } g_i, h_i \in N_i,$$

para todo $(1 \leq i \leq s)$

Luego, usando la proposición anterior, se deduce

$$\begin{aligned} \psi(x, y) &= \psi(g_1h_1, \ldots, g_sh_s) \\ &= (g_1h_1)(g_2h_2)\cdots(g_sh_s) \\ &= (g_1 \cdots g_s)(h_1 \cdots h_s) \\ &= \psi(x)\psi(y) \end{aligned}$$

Además ψ es sobreyectiva, por la definición de producto interno.

Falta probar la inyectividad de ψ.

Sea $x = (g_1, \ldots, g_s) \in G'$ tal que $\psi(x) = e$, luego se tiene

$$g_1 \cdots g_s = e$$

Usando la unicidad de la representación de

$$g_1 \cdots g_s = e_1 \cdots e_s$$

donde $e_i = e$ para todo $1 \leq i \leq s$, se concluye $g_i = e$, para todo $1 \leq i \leq s$.

Luego

$$x = (e, \ldots, e) = e \ \text{ en } \ G'$$

Por lo tanto hemos probado $\ker \psi = \{e\}$ y se puede concluir entonces que ψ es inyectiva.

♠

Ejemplo: Sea $G = \mathbb{Z}_5 \times \mathbb{Z}_5$, donde $\mathbb{Z}_5$, es el grupo de los enteros módulo 5 bajo la adicción. Luego los elementos de G son:

$$\begin{array}{lllll} e = (0,0) & x_6 = (0,1) & x_{11} = (0,2) & x_{16} = (0,3) & x_{21} = (0,4) \\ x_2 = (1,0) & x_7 = (1,1) & x_{12} = (1,2) & x_{17} = (1,3) & x_{22} = (1,4) \\ x_3 = (2,0) & x_8 = (2,1) & x_{13} = (2,2) & x_{18} = (2,3) & x_{23} = (2,4) \\ x_4 = (3,0) & x_9 = (3,1) & x_{14} = (3,2) & x_{19} = (3,3) & x_{24} = (3,4) \\ x_5 = (4,0) & x_{10} = (4,1) & x_{15} = (4,2) & x_{20} = (4,3) & x_{25} = (4,4) \end{array}$$

Entonces G, lo identificamos con $\mathbb{Z}_5 + \mathbb{Z}_5$, haciendo la identificación

$$(a,b) \longrightarrow a(1,0) + b(0,1)$$

Nótese que todo elemento en G se escribe de manera única en esta forma. Por ejemplo

$$x_{15} = 4(1,0) + 2(0,1)$$

Obsérvese también que el orden de cualquier elemento de G es 5, luego $\mathbb{Z}_5 \times \mathbb{Z}_5$ no es isomorfo a $\mathbb{Z}_{25}$ (¿Por qué?).

Ejercicios

1) Sean $G_1, \ldots, G_n$ grupos tales que $o(G_i) = t_i$. Probar que el orden de $G = G_1 \times \cdots \times G_n$ es igual a $t_1 \cdots t_n$.

2) Sea C_4 el grupo cíclico de orden 4. Probar que $C_4 \oplus C_4$ no es un grupo cíclico. Generalice este resultado.

3) Dar una lista de todos los elementos de $C_4 \oplus C_4$. Halle todos los elementos de orden 2. Halle el diagrama de subgrupos de este grupo.

4) Demuestre que $C_4 \oplus C_2 \oplus C_2$ y $C_4 \oplus C_4$ no son isomorfos.

5) Sea $G = G_1 \times \cdots \times G_n$ y considérense las n aplicaciones

$$\pi_i : G \longrightarrow G_i$$

$$(g_1, \ldots, g_n) \longrightarrow g_i$$

π_i se llama la **i- ésima proyección canónica**.

Probar que para todo i, π_i es un homomorfismo sobreyectivo.

6) Sea $G = G_1 \times \cdots \times G_n$ y considérense las n aplicaciones

$$i_k : G_k \longrightarrow G, \;\; 1 \leq k \leq n,$$

$$g_k \longrightarrow (e_1, \ldots, e_{k-1}, g_k, e_{k+1}, \ldots, e_n)$$

la aplicación i_k se llama la **k - ésima inclusión canónica**. Probar que i_k es un homomorfismo de grupos sobreyectivo, para todo k.

7) Demuestre que si G_1, y G_2 son grupos, entonces

$$G_1 \times G_2 \approx G_2 \times G_1$$

8) Sea $G = G_1 \times G_2$, y $H = \{(a, f) \mid a \in G_1\}$, donde f es la identidad de G_2. Probar que H es normal en G y además

$$G/H \approx G_2.$$

9) Sean C_r y C_s grupos cíclicos de orden r y s, con $(r, s) = 1$. Probar que $C_r \times C_s \approx C_{rs}$.

10) Sea $G = S_3 \times S_3$. Hallar dentro de G un subgrupo de orden 9.

11) Hallar todos los posibles grupos abelianos de orden 16.

12) Sean G_1, G_1', G_2, G_2' grupos, tales que $G_1 \approx G_1'$ y $G_2 \approx G_2'$. Probar que

$$G_1 \times G_2 \approx G_1' \times G_2'.$$

6.3 La Ecuación de la Clase

En esta sección estudiaremos una nueva técnica para contar los elementos dentro de un grupo G, conocida con el nombre de relación de conjugación. Por intermedio de ésta, es posible demostrar un resultado muy interesante sobre grupos finitos debido a Cauchy. Este resultado establece que si un número primo p divide al orden de un grupo finito G, entonces G tiene un subgrupo de orden p.

Definición 6.3.1 *Sea G un grupo y $a, b \in G$. Diremos que* **b es conjugado de a**, *si existe $c \in G$, tal que*

$$b = c^{-1}ac$$

Si b es un conjugado de a, lo denotamos por

$$a \sim b$$

Se puede verificar que la relación "$\sim$" es de equivalencia en el conjunto G. Para cada $a \in G$ se tiene su clase de conjugación:

$$C(a) = \{x \in G, \mid a \sim x\}$$

Si $C(a)$ tiene C_a elementos, se tiene la siguiente fórmula de conteo en G

$$|G| = \sum C_a$$

donde C_a recorre todas las clases de equivalencia. Esta relación se conoce con el nombre de **ecuación de la clase en** G

Definición 6.3.2 *Sea G un grupo y $a \in G$. Definimos el* **Normalizador de** *a como*

$$N(a) = \{x \in G, \mid xa = ax\}.$$

Entonces es fácil probar que $N(a)$ es un subgrupo de G.

Teorema 6.3.1 *Para cada $a \in G$,*

$$C_a = \frac{\circ(G)}{\circ(N(a))}.$$

Demostración: Definimos una función

$$\begin{array}{rccc} \phi & : & C(a) & \longrightarrow & G/N(a) \\ & & T = x^{-1}ax & \longrightarrow & N(a)x \end{array}$$

Probaremos que ϕ es una biyección

1) ϕ está bien definida. Es decir, dos clases de conjugados iguales, pero con distintos representantes, tienen la misma imagen bajo el homomorfismo ϕ

Si $x^{-1}ax = y^{-1}ay$, entonces $yx^{-1}axy^{-1} = a$, lo cual implica

$$(xy^{-1})^{-1}axy^{-1} = a$$

.

Luego debemos tener $xy^{-1} \in N(a)$ y de aqui se deduce que $xN(a) = yN(a)$. Por lo tanto ϕ esta bien definida.

2) ϕ es $1:1$

Supongamos que para $T_1, T_2 \in C(a)$, donde $T_1 = x^{-1}ax$, $T_2 = y^{-1}ay$, se tiene $\phi(T_1) = \phi(T_2)$. Por lo tanto

$$N(a)x = N(a)y$$

Luego $xy^{-1} \in N(a)$, lo cual implica $xy^{-1}a = axy^{-1}$. Por lo tanto $y^{-1}ay = x^{-1}ax$, y de esto se obtiene $T_1 = T_2$.

3) ϕ es sobre (fácil).

♠

Corolario 6.3.1 *Si G es un grupo finito, se tiene*

$$\circ(G) = \sum \frac{\circ(G)}{(\circ(N(a))}$$

donde cada elemento a pertenece a una clase conjugada.

Definición 6.3.3 *Sea G un grupo, entonces* **el centro de** G *es el conjunto*

$$Z(G) = \{g \in G \mid gx = xg,\ \forall x \in G\}.$$

Es fácil verificar que $Z(G)$ es un subgrupo de G.

Observación: Usaremos el símbolo Z o $Z(G)$, indistintamente para indicar este grupo.

Observación: Si $a \in Z(G)$, entonces $N(a) = G$, luego

$$\frac{\circ(G)}{\circ(N(a))} = 1$$

Usando esta observación tenemos el corolario:

Corolario 6.3.2 *Si G es finito*

$$\circ(G) = |Z(G)| + \sum_{a \notin Z(G)} \frac{\circ(G)}{\circ(N(a))}.$$

Corolario 6.3.3 *Si $\circ(G) = p^n$, donde p es un número primo, entonces $Z(G) \neq \{e\}$.*

Demostración: Si $a \notin Z(G)$, entonces $N(a) \neq G$, luego por el teorema de Lagrange

$$\circ(N(a))| \circ (G)$$

y por lo tanto

$$\circ(N(a)) = p^\alpha \quad \text{con } 1 \leq \alpha < n$$

luego

$$p \left| \frac{\circ(G)}{\circ(N(a))} \right. ,$$

para todo $a \notin Z(G)$.

Así

$$p \left| \circ(G) - \sum_{a \notin Z(G)} \frac{\circ(G)}{\circ(N(a))} \right.$$

y por lo tanto

$$p \,|\, \circ(Z(G))$$

Esto es $\circ(Z(G)) > 1$

Corolario 6.3.4 *Si $\circ(G) = p^2$, p primo, entonces G es abeliano.*

Demostración: Por el corolario anterior, sabemos que $Z(G) \neq \{e\}$. Como $Z(G)$ es un subgrupo de G, se debe tener que

$$|Z(G)| = p^2 \quad \text{o} \quad |Z(G)| = p$$

Si $|Z(G)| = p^2$ entonces $Z(G) = G$, y estará listo. Si $|Z(G)| = p$, existe $a \in G$ tal que $a \notin Z(G)$, luego

$$Z(G) \subsetneq N(a) \subseteq G$$

Nuevamente, se debe tener

$$\circ(N(a)) = p^2$$

lo cual implica

$$N(a) = G$$

Esto es una contradicción pues $a \notin Z(G)$. Por lo tanto $Z(G) = G$ y así G es abeliano.

Teorema 6.3.2 *(Cauchy) Sea G un grupo finito y p un número primo tal que $p| \circ (G)$. Entonces G tiene un elemento de orden p.*

Demostración:

1) Supongamos que G es abeliano. Usaremos inducción sobre el orden de G. Si $\circ(G) = 1$ no hay nada que probar.

Supongamos el teorema cierto para subgrupos de orden $< n = \circ(G)$

a) Si $\circ(G) = p$, con p un número primo, entonces G es un grupo cíclico generado por un elemento $g \in G$. Luego $\circ(g) = p$ y g es el elemento buscado.

b) G no tiene subgrupos triviales distintos de $\{e\}$ y G, entonces G es cíclico de orden primo (verificarlo!).

c) Supongamos que G tiene un subgrupo H no trivial, y $\circ(H) < \circ(G)$. Si $p| \circ (H)$ estará listo.

Supongamos que $p \not| \circ (H)$. Luego

$$p \left| \frac{\circ(G)}{\circ(H)} \right.$$

y por lo tanto

$$p| \ \circ \left(\frac{G}{H}\right)$$

Como G/H es abeliano y

$$\circ \left(\frac{G}{H}\right) < \circ(G),$$

aplicamos hipótesis de inducción a G/H. Luego existe un elemento $Hg \in G/H$ de orden p. Luego

$$(Hg)^p = Hg^p = H$$

es decir, $g^p \in H$ y $g \notin H$, luego

$$(g^p)^{\circ(H)} = e$$

Sea $x = g^{\circ(H)}$. Entonces probaremos que $x \neq e$.

En efecto si

$$g^{\circ(H)} = e$$

tenemos que

$$(Hg)^{\circ(H)} = H.$$

Como $\circ(Hg) = p$, se debe tener $p| \circ (H)$, lo cual es imposible.

Así $x \neq e$ y $x^p = e$. Luego

$$\circ(x) = p$$

Con esto termina la demostración del primer caso.

2) G no Abeliano

Nuevamente usamos inducción sobre el orden de G.

Si $\circ(G) = 1$ no hay nada que probar.

Si G tiene un subgrupo H, tal que $p| \circ (H)$ está listo.

Supongamos que p no divide al orden de ningún subgrupo de G. En particular, si $a \notin Z(G)$ entonces $N(a) \neq G$ y por lo tanto $p \not| N(a)$. Luego se tiene la ecuación de la clase

$$\circ(G) = \circ(Z(G)) + \sum_{a \notin Z(G)} \frac{\circ(G)}{\circ(N(a))}$$

Puesto que $p| \circ (G)$ y $p \not| \circ (N(a))$ se tiene que $p| \frac{\circ(G)}{\circ(N(a))}$, si $a \notin Z(G)$. Luego

$$p \left| \circ (G) - \sum_{a \notin Z(G)} \frac{\circ(G)}{\circ(N(a))} \right.$$

y por lo tanto

$$p| \circ (Z(G))$$

Pero hemos supuesto que p no dividía al orden de ningún subgrupo propio de G. Como consecuencia de esto debemos tener $Z(G) = G$, con lo cual G es abeliano. Luego aplicamos el primer caso.

♠

Ejercicios

1) Probar que si G es un grupo, entonces su centro es un grupo abeliano.

2) Sea G un grupo y $a \in G$. Probar que $N(a)$ es un subgrupo de G.

3) Hallar el centro de S_3.

4) En el grupo S_3, calcular $N(\phi)$, donde ϕ es la reflexión de orden 2.

5) Sea G un grupo y $a \in G$. Probar que $a \in Z(G)$ si y sólo si $N(a) = G$.

6) Probar que si G es un grupo, la relación de conjugados, en los elementos de G es de equivalencia.

7) Escribir la ecuación de la clase para el grupo $G = S_3$.

8) Probar que si G es un grupo de orden p^α, entonces G tiene subgrupos de ordenes $1, p, p^2, \ldots, p^{\alpha-1}, p^\alpha$.

9) Sea p un número primo. Probar que existen sólo dos grupos de orden p^2, salvo isomorfismo.

10) Halle todos los conjugados de la rotación R_1 en el grupo de simetrías del cuadrado.

11) Calcule el número de clases conjugadas del grupo diédrico D_4.

12) Halle el centro de D_4.

6.4 Teoremas de Sylow

En esta sección probaremos uno de los teoremas más importantes de toda la teoría de grupos, como lo es el teorema de Sylow. Si G es un grupo cuyo orden es divisible por una potencia de un primo p, entonces el teorema de Sylow garantiza la existencia de un subgrupo de G, cuyo orden es la potencia dada de p.

Para demostrar este teorema necesitamos aplicar una técnica nueva para contar elementos dentro de un conjunto, a partir de un grupo dado, la cual se conoce con el nombre de Acción de Grupos.

Definición 6.4.1 *Sea A un conjunto y G un grupo. Diremos que G actúa sobre A, si existe una función $\phi : G \times A \longrightarrow A$ que satisface*

1. *Para todo $g \in G$, la aplicación*

$$\begin{aligned} \phi_g : A &\longrightarrow A \\ a &\longrightarrow \phi(g, a) \end{aligned}$$

es una permutación del conjunto A.

2. La aplicación

$$G \longrightarrow S(A)$$
$$g \longrightarrow \phi_g$$

es un homomorfismo de grupos.

Observación: De acuerdo con la condición 2 se tienen las siguientes fórmulas de composición.

1. $\phi_a\phi_b = \phi_{ab}$, para todo a y b en G.
2. $\phi_{g^{-1}}\phi_g = \phi_e = Id$, para todo g en G.

Ejemplo: En la demostración del Teorema de Cayley hemos visto cómo un grupo G actúa sobre el conjunto G formado por sus elementos, mediante **Traslaciones a la derecha**. Este tipo de acción viene dada por la función

$$\phi : G \times G \longrightarrow G$$
$$(g, a) \longrightarrow g.a$$

Es fácil verificar que se cumplen las condiciones 1 y 2 de la definición para esta función.

Introducimos a continuación un par de conceptos muy útiles para el conteo de los elementos de un conjunto en donde está definida una acción.

Definición 6.4.2 *Sea G un grupo, el cual actúa sobre un conjunto A. Entonces para todo a en A, se define la* **órbita de** a **bajo** G *como el conjunto*

$$A_a = \{\phi(g, a) \mid g \in G\}$$

Observación: Es fácil verificar que el conjunto de las distintas órbitas de A bajo todos los elementos de G establece una partición del conjunto A.

Definición 6.4.3 *Sea G un grupo, el cual actúa sobre un conjunto A. Entonces para todo $a \in A$ se define el* **estabilizador de a en** *G como el conjunto*

$$Est_a = \{g \in G \mid \phi(g, a) = a\}$$

Observación: Se demuestra que para todo a en A, Est_a es un subgrupo de G.

El siguiente teorema permite calcular el número de elementos dentro de cada órbita.

Teorema 6.4.1 *Sea G un grupo finito, el cual actúa sobre un conjunto A finito. Entonces, para todo $a \in A$ se tiene*

$$|A_a| = [G : Est_a] = \frac{|G|}{|Est_a|}$$

Demostración: Sea $\mathcal{C}_a$ el conjunto de las clases laterales derechas de Est_a en G. Consideremos la aplicación

$$\Psi : \mathcal{C}_a \longrightarrow A_a$$
$$g.Est_a \longrightarrow \phi_g(a)$$

donde $\phi_g(a)$ denota la aplicación de g sobre el elemento a.

En primer lugar probaremos que ϕ está bien definida, para lo cual supongamos que $g_1 Est_a = g_2 Est_a$ para algunos g_1, g_2 en G. Entonces se tiene $g_1 g_2^{-1} \in Esta_a$ si y sólo si $\phi_{g_1^{-1} g_2}(a) = a$.

Luego $\phi_{g_1^{-1}} \phi_{g_2}(a) = a$, si y sólo si $\phi_{g_2}(a) = \phi_{g_1}(a)$. Con esto hemos probado que la función está bien definida. Repitiendo los pasos en sentido inverso, se prueba la inyectividad de ψ. Luego la función es biyectiva y de esto se deduce la tesis del teorema.

♠

Damos inicio ahora a una serie de resultados de combinatoria necesarios para probar la primera parte del Teorema de Sylow.

Sea S un conjunto de n elementos. Entonces el número de formas de escoger k elementos entre los n es dado por:

$$\binom{n}{k} = \frac{n!}{k!(n-k)!} \tag{6.2}$$

Lema 6.4.1 *Sea $n = p^\alpha m$, donde p es primo y $p^r | m$ pero $p^{r+1} \not| \ m$. Entonces*

$$p^r \left| \binom{n}{p^\alpha} \quad pero \quad p^{r+1} \not| \binom{n}{p^\alpha} \right.$$

Demostración: De (**??**) obtenemos

$$\begin{aligned} \binom{p^\alpha m}{p^\alpha} &= \frac{(p^\alpha m)!}{(p^\alpha)!(p^\alpha m - p^\alpha)!} \\ &= \frac{p^\alpha m(p^\alpha m - 1)\cdots(p^\alpha m - p^\alpha + 1)}{p^\alpha(p^\alpha - 1)(p^\alpha - 2)\cdots(p^\alpha - p^\alpha + 1)} \end{aligned} \tag{6.3}$$

Observando la expresión (**??**), vemos que si una potencia de p, digamos p^i divide el numerador, entonces esta potencia también divide al denominador.

En efecto, si $p^i | p^\alpha m - k$, $(k \geq 1)$, entonces $p^i | k$ y por lo tanto

$$p^i | p^\alpha - k.$$

Luego toda potencia de p en el numerador, se cancela con la correspondiente potencia de p en el denominador. Luego la única potencia de p en (**??**) es la que contiene m. De donde se obtiene el resultado.

♠

Teorema 6.4.2 *(Sylow)*
Sea G un grupo finito, p es un número primo y $p^\alpha | \circ(G)$. Entonces G tiene un subgrupo de orden p^α.

Demostración: Sea

$$\circ(G) = p^{\alpha}m,$$

tal que $p^r|m$, y $p^{r+1} \not| m$.

Sea $\mathcal{A} = \{A_1, \ldots, A_s\}$ la familia de subconjuntos de G de tamaño p^{α}. Entonces

$$s = \binom{p^{\alpha}m}{p^{\alpha}}$$

Definimos una relación sobre $\mathcal{A}$, mediante :

A_i, A_j en $\mathcal{A}$ están relacionados, sí y sólo si existe un elemento $g \in G$, tal que $A_i = gA_j$.Es fácil ver que esta relación es de equivalencia.

Afirmamos que existe una clase de equivalencia, digamos $\overline{A}_1$ tal que

$$p^{r+1} \Big| |\overline{A_1}| .$$

Caso contrario p^{r+1} divide a todas las clases de equivalencia y por lo tanto

$$p^{r+1} \mid |\mathcal{A}|$$

entonces

$$p^{r+1} \Big| \binom{p^{\alpha}m}{p^{\alpha}}$$

lo cual es imposible por el lema anterior.

Sea

$$\overline{A_1} = \{A_1, \ldots, A_n\} = \{gA_1 \mid g \in G\}$$

donde $p^{r+1} \not| n$ y sea

$$H = \{g \in G \mid gA_1 = A_1\}$$

entonces H es un subgrupo de G, y además se tiene

$$\circ(H) = \frac{\circ(G)}{n}$$

En efecto, la demostración de **??** se sigue de lo siguiente:

Si para algunos g_1, g_2 en G se tiene que $g_1A_1 = g_2A_1$, entonces $g_2^{-1}g_1A_1 = A_1$.

Luego $g_2^{-1}g_1 \in H$, y por lo tanto las clases laterales g_1H y g_2H son iguales. Por lo tanto, el número de elementos de $\overline{A}_1$, el cual denotamos por n, es igual al número de clases laterales de H en G. Luego

$$n = \frac{\circ(G)}{\circ(H)}$$

de donde

$$\circ(H) = \frac{\circ(G)}{n}$$

Como $\circ(G)/n$ es un entero se tiene que todas las potencias de p que aparecen en n, se cancelan con las respectivas potencias de $\circ(G)$. Como la mayor potencia que divide a n es p^r, se tiene que

$$p^\alpha \,|\circ(H)$$

y por lo tanto

$$\circ(H) \geq p^\alpha \tag{6.4}$$

Por otro lado, $hA_1 = A_1$, para todo $h \in H$. Si tomamos $a_1 \in A_1$ fijo se obtiene

$$ha_1 \in A_1, \quad \forall h \in H$$

Luego

$$\circ(H) \leq \circ(A_1) = p^\alpha \tag{6.5}$$

Usando (**??**) y (**??**) obtenemos

$$\circ(H) = p^\alpha$$

Luego H es el subgrupo buscado y con esto termina la demostración.

♠

Definición 6.4.4 *Sea G un grupo finito de orden $p^\alpha n$, donde p no divide a n. Entonces un subgrupo H de G de orden p^α se llama un* **p-grupo de Sylow** *de G.*

Más adelante veremos otros teoremas de Sylow, que nos darán información sobre el número de p-grupos de Sylow dentro de un grupo G. Antes de llegar a estos teoremas necesitamos una serie de definiciones y resultados sobre grupos conjugados.

Definición 6.4.5 *Sea G un grupo y H subgrupo de G. Para cualquier $a \in G$, el conjunto*

$$aHa^{-1} = \{aha^{-1} \mid h \in H\}$$

se llama **grupo conjugado de H inducido por** a.

La demostración de que dicho conjunto es un subgrupo de G, se deja como ejercicio.

Observación: Es claro que si H' es un conjugado de H, entonces H' y H tienen el mismo orden.

Definición 6.4.6 *Sea G un grupo. Un subgrupo H de G se dice* **invariante** *o* **autoconjugado bajo** *a si y sólo si*

$$aHa^{-1} = H.$$

Observación: Es claro que si $a \in H$, entonces H es invariante bajo a.

Si H es un subgrupo normal de G, entonces H es invariante bajo todos los elementos de G.

Definición 6.4.7 *Sea G un grupo y H, K subgrupos de G. Entonces el conjunto:*

$$N_k(H) = \{k \in K \mid kHk^{-1} = H\}$$

se denomina el **normalizador de H en K.**

Dejamos como ejercicio para el lector, el probar que $N_k(H)$ es un subgrupo de K.

Observación: Si en la definición anterior tenemos $K = G$, entonces denotamos $N_G(H)$ por $N(H)$ y lo llamamos el **Normalizador de** H

Proposición 6.4.1 *Sean H y K subgrupos de G. El número de conjugados de H, inducidos por todos los elementos de K, es igual al índice*

$$[K \ : \ N_K(H)]$$

Demostración: Sea $\mathcal{B}$ el conjunto de todos los conjungados de H, inducidos por los elementos de K y definamos la función

$$\begin{array}{rccc} f & : & K & \longrightarrow & \mathcal{B} \\ & & k & \longrightarrow & kHk^{-1} \end{array}$$

Es claro que f es sobre. Veamos en qué situación dos elementos distintos de K, digamos k_1 y k_2 pueden tener imágenes iguales.

Sea

$$k_1Hk_1^{-1} = k_2Hk_2^{-1}$$

si y sólo si

$$k_1^{-1}k_2H(k_1^{-1}k_2)^{-1} = H$$

si y sólo si

$$k_1^{-1}k_2 \in N_K(H)$$

Luego las imágenes de k_1 y k_2 son iguales si y sólo si estos elementos están en la misma clase lateral de $N_K(H)$ en K. Por lo tanto el número de elementos distintos de $\mathcal{B}$ es igual al número de clases laterales de $N_K(H)$ en K, el cual viene dado por:

$$[K \ : \ N_K(H)]$$

♠

Teorema 6.4.3 *(Sylow)*
Sea G un grupo finito y p un número primo con $p|\circ(G)$. Entonces el número de p-grupos de Sylow de G, el cual denotaremos por h, satisface:

$$h \equiv 1 \ mod \ p \quad y \quad h|\circ(G).$$

Demostración: Sea $\mathcal{D}$ el conjunto de todos los p-grupos de Sylow de G. ($\mathcal{D}$ es diferente del vacío por el primer teorema de Sylow). Sea P un elemento de $\mathcal{D}$. Entonces P actúa sobre $\mathcal{D}$ por conjugación, es decir mediante la acción

$$\begin{aligned} &\phi : P \times \mathcal{D} \longrightarrow \mathcal{D} \\ &(g, P_i) \longrightarrow gP_ig^{-1} \end{aligned}$$

Es claro que esta acción es sobreyectiva, pues si P_i es cualquier elemento de $\mathcal{D}$, se tiene

$$P_i = eP_ie^{-1}$$

donde e es el elemento neutro de P.

Entonces, el número de elementos de $\mathcal{D}$, el cual llamanmos h, se obtiene

$$h = \sum_{Q \in \mathcal{D}} |\mathcal{D}_Q|$$

donde $\mathcal{D}_Q$ es la órbita del elemento Q en $\mathcal{D}$.

Tenemos dos posibilidades para Q.

1) Si $Q = P$, entonces

$$\mathcal{D}_P = \{gPg^{-1} | g \in P\} = P$$

luego esta órbita consiste de un sólo elemento.

2) Si $Q \neq P$, entonces

$$|\mathcal{D}_Q| = \frac{|P|}{|Est_Q|} = \frac{p^\alpha}{|N_P(Q)|} = p^\beta$$

con $\beta \geq 0$.

Como $P \neq Q$, se tendrá $N_P(Q) \neq P$ (Ver los ejercicios) y por lo tanto $\beta > 0$.

En conclusión se tiene que

$$h = 1 + p^{\alpha_1} + p^{\alpha_2} + \cdots + p^{\alpha_n} \tag{6.6}$$

y por lo tanto $h \equiv 1 \ mod \ p$.

En la tercera parte del teorema de Sylow probaremos que todos los p-grupos de Sylow son conjugados entre sí. Entonces si se elige un p-grupo P los restantes p-grupos aparecen en la órbita de P cuando el grupo G actúa sobre $\mathcal{D}$ por conjugación. El tamaño de dicha órbita viene dado por

$$|\mathcal{D}_P| = \frac{|G|}{|Est_P|} = \frac{|G|}{|N(P)|} = [G : N(P)]$$

donde $N(P)$ es el normalizador de P.

♠

Teorema 6.4.4 *(Sylow)*
Sea G un grupo finito y $p| \circ (G)$. Entonces todos los $p-$grupos de Sylow son conjugados.

Demostración:
Sean P un $p-$ subgrupo de Sylow y Q otro $p-$subgrupo de Sylow que no se encuentre entre los conjugados de P.

Entonces calculemos el número total de conjugados de Q, usando la acción del grupo P sobre el conjunto de los conjugados de Q.

En primer lugar, el número de conjugados de Q, por elementos de P (la órbita de Q) viene dado por:

$$[P \ : \ N_P(Q)] = \frac{\circ(P)}{\circ(N_P(Q))} = p^{\beta} \quad \text{con } \beta \geq 0 \tag{6.7}$$

Si asumimos $\beta = 0$, se tendrá

$$\circ(P) = \circ(N_P(Q)))$$

lo cual implica

$$P = N_P(Q)$$

y por lo tanto $P = Q$, lo cual es una contradicción.

Si hay otro conjugado de Q, aparte de los senãlados en (**??**), sea Q_1 otro conjugado y repitamos el proceso. Luego el número total de conjugados de Q (contando todas las órbitas) vendrá dado por

$$h' = p^{\beta_1} + p^{\beta_2} + \cdots p^{\beta_s} \quad \text{con } \beta_i > 0.$$

donde ($\beta = \beta_1$) Por lo tanto $h' \equiv 0 \ mod\ p$, lo cual es imposible por (**??**).

Con esto se da fin a la prueba.

♠

Ejercicios

1) Sea n un entero positivo y k otro entero tal que $k \leq n$. Entonces el **factorial inferior de** n **en** k, el cual denotamos por $(n)_k$ es el número de $k-$uplas que se pueden formar a partir de un conjunto de n elementos.

Si $A = \{1, 2, \ldots, n\}$, entonces $(n)_k$ es el cardinal del conjunto

$$A^k = \{(x_1, \ldots, x_k) \mid x_i \in A \text{ y } x_i \neq x_j, \text{ si } i \neq j\}$$

Probar que $(n)_k = n(n-1)\cdots(n-k+1)$.

2) Si $n = 5$ y $k = 3$, hallar todos los elementos de A^3.

3) Sea $x = (x_1, \ldots, x_k)$ una $k-$upla en A^k. Un **desarreglo de** x es otra $k-$upla y de A^k tal que si $y = (y_1, \ldots, y_k)$, entonces

$$\{x_1, \ldots x_k\} = \{y_1, \ldots, y_k\}$$

Probar que el número de desarreglos posibles de una $k-$upla cualquiera es $k!$.

4) El número de subconjuntos de tamaño k que se puede extraer de un conjunto de n elementos, con $n \geq k$, se llama el **combinatorio de** n **sobre** k y se denota por

$$\binom{n}{k}$$

Demostrar la fórmula

$$\binom{n}{k} = \frac{n!}{(n-k)!k!}$$

5) Probar la fórmula

$$\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}, \quad 1 \leq k \leq n$$

Ayuda: Primero cuente todos los subconjuntos de tamaño k que contienen al 1 y luego aquellos que no contienen al 1.

6) Sea G un grupo finito y $\mathcal{A}$ la familia de todos los subconjuntos de G de tamaño s, con $s < \circ(G)$. Para A_i, A_j en $\mathcal{A}$ se define la relación "$A_i \sim A_j$ si y sólo si existe un $g \in G$ tal que $gA_i = A_j$"

Probar que esta relación define una relación de equivalencia en $\mathcal{A}$.

7) Sea $\mathcal{A}$ como en el ejercicio anterior y $A_0 \in \mathcal{A}$. Diremos que dos elementos g_1 y g_2 en G están relacionados, si y sólo si

$$g_1 A_1 = g_2 A_1$$

Probar que esto define una relación de equivalencia en G.

8) Sea G un grupo, H un subgrupo de G y $a \in G$. Probar que el conjunto

$$aHa^{-1}\{aha^{-1} \mid h \in H\}$$

es un subgrupo de G, cuyo orden es igual al orden de H. Este grupo se dice **grupo conjugado de** H.

9) Sea G un grupo y H, K dos subgrupos de G. Entonces el **Normalizador de** H **en** K se define por

$$N_k(H) = \{k \in K \mid kHk^{-1} = H\}$$

Probar que $N_k(H)$ es un subgrupo de G.

10) Sea G un grupo y H, K dos subgrupos tales que H y K son conjugados y además

$$N_H(K) = H$$

Probar que $K = H$

11) Probar que un grupo finito de orden 21 tiene un solo $p-$grupo de Sylow de orden 3, o bien 1 ó 7 $p-$grupos de Sylow de orden 7.

12) Probar que cualquier subgrupo de orden p^{n-1} en un grupo de orden p^n, con $p-$primo, es normal en G.

13) Sea G un grupo, $Z(G)$ su centro y $G/Z(G)$ cíclico. Probar que G debe ser abeliano.

14) Probar que cualquier grupo de orden 15 es cíclico.

15) Hallar todas las clases de conjugados en S_4 y verificar la ecuación de la clase.

16) Probar que si G es un grupo de orden p^n con p un primo. Entonces G tiene un subgrupo de orden p^α para cualquier $0 \leq \alpha \leq n$. Use la ecuación de la clase.

17) Sea G un grupo finito de orden $3^2 \cdot 5^2$. ¿Cuántos $3-$grupos de Sylow y $5-$grupos de Sylow hay en G?.

18) Sea G un grupo de orden 30

a) Demuestre que los $3-$grupos de Sylow y los $5-$grupos de Sylow son normales.

b) Demuestre que G tiene un subgrupo normal de orden 15.

c) Clasifique todos los grupos de orden 30.

d) ¿Cuántos grupos de orden 30, no isomorfos, existen?

19) Si G es un grupo de orden 231, probar que el $11-$grupo de Sylow está en el centro de G.

20) Sea G un grupo abeliano finito. Probar que G es isomorfo al producto directo de sus grupos de Sylow.

21) Sean A y B grupos. Probar que $A \times B$ es isomorfo a $B \times A$

22) Sean A y B grupos cíclicos de orden m y n, respectivamente. Probar que $A \times B$ es cíclico si sólo si $(m, n) = 1$.

23) Si G es un grupo de orden pq, con p y q primos y $p < q$, entonces si p no divide a $q - 1$, G es un grupo cíclico.

24) Hallar en D_4 todos los conjugados de $H = \{e, h\}$, donde h es una reflexión en el eje x.

25) Sea $G = S_7$ el grupo de permutaciones de 7 elementos, y sean $H = \{\sigma \in G |\ \sigma(1) = 1\}$ y $K = \{\theta \in G |\ \theta(2) = 2\}$. Hallar a) $N_H(K)$ y b)$N_K(H)$.

26) Sea G y H como en el ejercicio anterior, y sea $\tau = (1, 2, 3)$. Hallar el grupo conjugado de H inducido por τ.

27) Sea $G = D_4$ y considérese los grupos $H =< a >$, $K =< b >$, donde $a^2 = e$, $b^2 = e$. Probar que $N_K(H) =< b^2 >$.

28) Probar que la relación de conjugación entre los subgrupos de un grupo G, define una relación de equivalencia.

29) Sea S_3 el grupo simétrico de orden tres y $H =< \phi >$. Hallar todos los conjugados de H.

30) Dar un ejemplo de un grupo de orden n, que no posea subgrupos de orden d, para algún d divisor de n.

6.5 Grupos Abelianos Finitos

Nos ocuparemos en esta sección de la clasificación de todos los grupos abelianos finitos. Usaremos los resultados obtenidos en la sección de producto directo de grupos y los teoremas de Sylow.

Teorema 6.5.1 *Sea G un grupo abeliano, de orden n, y H, K subgrupos de G de órdenes h y k con $n = hk$ y $(h.k) = 1$. Entonces G es isomorfo a el producto directo $H \times K$.*

Demostración: Sabemos que H y K son subgrupos normales de G, luego HK es un subgrupo de G de orden

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

Ahora bien, si $x \in H \cap K$ el orden del elemento x es un divisor de h y k. Pero por hipótesis se tiene que el único divisor común de h y k es 1, pues el $(h, k) = 1$. Luego $x = e$, y esto demuestra que

$$H \cap K = \{e\}$$

Entonces tenemos que

$$\circ(HK) = \circ(H) \circ (K) = hk$$

y por lo tanto $HK = G$

Usando el teorema **??** sección **??**, se concluye la demostración.

♠

Sea G un grupo finito abeliano de orden n, y supongamos que n tiene una factorización en primos distintos

$$n = p_1^{\alpha_1} \cdots p_t^{\alpha_t}$$

Entonces sabemos, por el teorema de Sylow, que G tiene subgrupos de Sylow P_i de orden p^{α_i}, usando esto y el teorema anterior se tiene:

Teorema 6.5.2 *Si G es un grupo abeliano finito de orden n, entonces G es isomorfo al producto directo $P_1 \times P_2 \times \cdots \times P_t$, donde los P_i son los grupos de Sylow de G.*

Ejemplo: Sea G un grupo abeliano de orden 600. Entonces se tiene

$$300 = 2^3 \times 3 \times 5^2.$$

Sean P_1, P_2 y P_3 subgrupos de Sylow de G de ordenes 8, 3 y 25 respectivamente. Luego se tiene el isomorfismo

$$G \approx P_1 \times P_2 \times P_3 \tag{6.8}$$

La estructura anterior todavía no nos da toda la información sobre el grupo G, pues P_1 es un grupo abeliano de orden 8 y debe ser isomorfo a uno de los grupos

$$\mathbb{Z}_8, \quad \mathbb{Z}_4 \oplus \mathbb{Z}_2, \quad \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$$

Sabemos que P_2 es un grupo de orden 3 y por lo tanto isomorfo a $\mathbb{Z}_3$.

Finalmente P_3 es isomorfo a $\mathbb{Z}_{25}$ o bien $\mathbb{Z}_5 \times \mathbb{Z}_5$. Si hacemos todos estas sustituciones para P_1, P_2 y P_3 en la expresión (**??**), nos encontramos con que G es producto directo de grupos cíclicos.

Teorema 6.5.3 *Todo grupo abeliano finito G es suma directa de grupos cíclicos C_i,*

$$G = C_1 \times \cdots \times C_s$$

donde $\circ(G) = \circ(C_1) \cdots \circ (C_s)$.

Demostración: De acuerdo con el teorema anterior, todo grupo G abeliano finito, es producto directo de sus subgrupos de Sylow. Luego el teorema quedará demostrado, si probamos que todo $p-$grupo de orden p^α con p primo, es suma directa de grupos cíclicos.

Esto precisamente lo demostramos a continuación.

♠

Teorema 6.5.4 *Sea G un grupo abeliano de orden p^α, con p primo. Entonces existen subgrupos cíclicos de G, C_i de orden p^{α_i} y tal que $1 \leq i \leq t$*

$$G \approx C_1 \times C_2 \times \cdots \times C_t \tag{6.9}$$

y además

$$\alpha_1 \geq \alpha_2 \geq \cdots \geq \alpha_t.$$

Los α_i se llaman **los invariantes de** G.

Demostración: Si G mismo es cíclico, entonces no hay nada que probar.

Si G no es cíclico, entonces los elementos de G tienen orden una potencia de p. Elegimos a_1 en G, tal que el orden de a_1 es máximo. Luego $\circ(a_1) = p^{\alpha_1}$, para algún $\alpha_1 \geq 1$.

Definimos $C_1 =< a_1 >$, con lo cual el orden del grupo cíclico C_1 es p^{α_1}.

Sea ahora $\overline{G} = G/C_1$ el cual tiene orden una potencia de p. Por el mismo razonamiento, se puede elegir un elemento $\overline{a_2}$ en $\overline{G}$ tal que el orden de $\overline{a_2}$ es maximal entre los ordenes de los elementos de $\overline{G}$.

Luego existe α_2 tal que

$$\circ(\overline{a_2}) = p^{\alpha_2}$$

Como $a_2^{p^{\alpha_1}} = e$, se tiene que

$$p^{\alpha_1} \geq \circ(a_2) \geq \circ(\overline{a_2}) = p^{\alpha_2}$$

Luego

$$\alpha_1 \geq \alpha_2$$

Ahora consideramos dos casos:

Caso I: Si $< a_1 > \cap < a_2 >= \{e\}$, entonces hacemos $C_2 =< a_2 >$ y de esta manera se tiene un producto directo $C_1 \times C_2$ dentro del grupo G, el cual podemos incrementar paso a paso, hasta obtener, después de un número finito de pasos, una descomposición de G de la forma (**??**).

Caso II: Si $< a_1 > \cap < a_2 >\neq \{e\}$, entonces elegiremos otro elemento en lugar de a_2. Tomemos p^{α_2} la menor potencia de p, tal que

$$a_2^{p^{\alpha_2}} \in < a_1 >= C_1$$

Por lo tanto existe un entero positivo i, tal que

$$a_2^{p^{\alpha_2}} = a_1^i,$$

y entonces se obtiene

$$\begin{aligned}\left(a_1^i\right)^{p^{\alpha_1}{}_1-\alpha_2{}_2} &= \left(a_2^{p^{\alpha_2}}\right)^{p^{\alpha_1-\alpha_2}} \\ &= a_2^{p^{\alpha_1}} \\ &= e\end{aligned}$$

Luego p^{α_1} divide a $i(p^{\alpha_1-\alpha_2})$, y por lo tanto

$$p^{\alpha_2}|i.$$

Luego existe j tal que

$$i = jp^{\alpha_2}$$

Tomemos entonces $b_2 = a_1^{-j}a_2$, el cual satisface

$$\begin{aligned}(b_2)^{p^{\alpha_2}} &= a_1^{-jp^{\alpha_2}}a_2^{p^{\alpha_2}} \\ &= a_1^{-i}a_2^{p^{\alpha_2}} \\ &= e\end{aligned}$$

Además, si para algún t, con $1 \leq t < p^{\alpha_2}$ se tiene

$$(b_2)^t = e,$$

entonces

$$a_1^{-jt}a_2^t = e,$$

y por lo tanto $a_2^t \in C_1$, lo cual es una contradicción, pues $t < p^{\alpha_2}$. Con esto queda demostrado que $\circ(b_2) = p^{\alpha_2}$.

Finalmente probaremos que

$$< a_1 > \cap < b_2 > = \{e\}$$

En efecto, si $x \in < a_1 > \cap < b_2 >$, se tendrá $x = b_2^t \in < a_i >$, para algún $t > 0$. Luego

$$b_2^t = (a_1^{-j} a_2)^t = a_1^{-jt} a_2^t$$

lo cual implica que $a_2^t \in < a_1 >$ y por lo tanto p^{α_2} divide a t.

Luego se tendrá

$$x = b_2^t = e$$

Vemos que el elemento b_2, cumple los requisitos buscados y volviendo al caso I, con $C_2 =< b_2 >$, se concluye la demostración.

♠

Ejemplo: Podemos clasificar todos los grupos abelianos de orden 60, usando los teoremas anteriores. Tenemos que $60 = 2^2 \cdot 3 \cdot 5$. Sean C_i grupos cíclicos de orden i, donde $i = 2, 3, 5$. Entonces si $\circ(G) = 60$ se tienen las siguientes posibilidades.

$$G \approx C_2 \times C_2 \times C_3 \times C_5 \cong C_2 \times C_{30}$$

$$G \approx C_4 \times C_3 \times C_5 \cong C_4 \times C_{15} \cong C_{60}$$

Luego existen solamente dos grupo abelianos de orden 60.

Si G es un grupo abeliano de orden p^n, entonces G es isomorfo a un producto directo

$$G \approx C_{p^{n_1}} \times C_{p^{n_2}} \times \cdots \times C_{p^{n_k}}$$

donde $n_1 \geq n_2 \geq \cdots \geq n_k > 0$ y

$$\sum_{i=1}^{k} n_i = n.$$

los enteros $n_1, n_2, \ldots, n_k$ son los invariantes del grupo G.

Nuestro próximo objetivo será probar la unicidad de los invariantes de G.

Definición 6.5.1 *Sea G un grupo abeliano. Entonces para todo $s \geq 1$ se define el conjunto*

$$G(s) = \{g \in G \mid g^s = e\}.$$

Ejemplo: Sea $G = C_4 \times C_2$ Entonces $G(2)$ es el grupo formado por los elementos

$$(0,0), \quad (0,1), \quad (2,1), \quad (2,0),$$

mientras que $G(4) = G$ y $G(1) = \{e\}$. Por otro lado,

Si $s \neq 2, 4, 1 \Longrightarrow G(s) = \{e\}$.

Ejemplo: En el caso particular del grupo multiplicativo de los números complejos se tiene

$$G(n) = \{z \in \mathbb{C} \mid z^n = 1\}, \quad n \geq 1.$$

Este es el grupo de las raíces n-ésimas de la unidad.

Observación: Se demuestra que $G(s)$ es un subgrupo de G, para todo $s \geq 1$.

Proposición 6.5.1 *Sean G_1 y G_2 dos grupos isomorfos. Entonces $G_1(s) = G_2(s)$ para todo s entero.*

Demostración: Sea $f : G_1 \longrightarrow G_2$ el isomorfismo dado entre G_1 y G_2.

Sean e_1 y e_2 los elementos neutros de G_1 y G_2 respectivamente. Si $g^s = e_1$ para algún $s \geq 1$, entonces por las propiedades de isomorfismo se tiene $f(g)^s = e_2$. Luego hemos demostrado

$$f(G_1(s)) \subseteq G_2(s)$$

Por otro lado, si $h \in G_2(s)$, entonces $h_2^s = e$. Como la función f es sobre, existe un $g \in G$, tal que $h = f(g)$ y por lo tanto

$$[f(g)]^s = f(g^s) = e_2$$

Como f es inyectiva, se tiene que $g^s = e_1$. Luego hemos probado $f(G_1(s)) \subseteq G_2(s)$, con lo cual se tiene $f(G_1(s)) = G_2(s)$ y por lo tanto $G_1(s)$ y $G_2(s)$ son isomorfos.

Proposición 6.5.2 *Sea $G = C_{p^{n_1}} \times C_{p^{n_2}} \times \cdots \times C_{p^{n_k}}$, donde p es un primo y cada $C_{p^{n_1}}$ es un grupo cíclico de orden p^{n_i}. Entonces*

$$G(p) = A_1 \times A_2 \times \cdots \times A_k,$$

donde $A_i = \langle x_i \rangle$ y el orden de cada x_i es igual a p.

Demostración: Para cada $1 \leq i \leq k$, sea

$$C_{p^{n_i}} = \langle g_i \rangle,$$

donde g_i es un elemento de G, de orden p^{n_i}.

Sea

$$x_i = g_i^{p^{n_i}-1}$$

para todo $1 \leq i \leq k$.

Entonces $\circ(x_i) = p$. Probaremos que el grupo

$$H = \langle x_1 \rangle \times \langle x_2 \rangle \times \cdots \langle x_k \rangle.$$

es igual a $G(p)$.

Nótese que $h^p = e$ para todo $h \in H$, y por lo tanto $H \subseteq G(p)$.

Por otro lado sea $x \in G(p) - H$. Entonces debemos tener $x^p = e$. Ahora bien, como $x \in G$ se tiene que existen enteros α_i tales que

$$x = (g_1^{\alpha_1}, \ldots, g_k^{\alpha_k}).$$

Como $x \in H$, existen enteros s y t tales que

$$\alpha_i = p^{n_i-1}s + t,$$

con $0 < t < p^{n_i-1}$, para algún i, $1 \leq i \leq k$.

Luego si $x^p = e$, entonces se tiene $(g_i^{\alpha_i})^p = e$, y por lo tanto:

$$g_i^{ps+pt} = e$$

O sea

$$g_i^{pt} = e,$$

con $0 < pt < p^{n_i}$.

Esto contradice la hipótesis de que $\circ(g_i) = p^{n_i}$.

Por lo tanto

$$G(p) = H = \langle x_1 \rangle \times \cdots \times \langle x_k \rangle.$$

Finalmente, daremos el teorema de las unicidad de los invariantes para un grupo abeliano finito de orden una potencia de p.

♠

Teorema 6.5.5 *Sean G_1 y G_2 dos grupos abelianos finitos de orden p^n y supongamos que tienen descomposiciones*

$$\begin{aligned} G_1 &= C_1 \times C_2 \times \cdots \times C_k \\ G_1 &= C_1' \times C_2' \times \cdots \times C_s' \end{aligned} \tag{6.10}$$

donde C_i es grupo cíclico de orden p^{n_i} y C_i' es un grupo cíclico de orden p^{n_i}, con

$$n_1 \geq n_2 \geq \cdots \geq n_k > 0$$

$$h_1 \geq h_2 \geq \cdots \geq h_s > 0.$$

Entonces $G_1 \approx G_2$ si y sólo si tiene los mismos invariantes, esto es $k = s$ y $n_i = h_i$, para todo $1 \leq i \leq k$.

Demostración:
($\Longrightarrow$) Probaremos que si G_1 y G_2 tienen los mismos invariantes, entonces ellos son isomorfos.

Sean

$$G_1 = C_1 \times \cdots \times C_k$$

$$G_2 = D_1 \times \cdots \times D_k$$

donde C_1 y D_1 son grupos cíclicos de orden p^{n_i} y $n_1 \geq n_2 \geq \cdots n_k > 0$.

Entonces para todo $1 \leq i \leq k$, existen elementos $g_i \in G_i$ y $h_i \in D_i$, tales que

$$G_i = \langle g_i \rangle \quad \text{y} D_i = \langle h_i \rangle$$

Consideremos la aplicación

$$\begin{array}{rccc} \phi \ : & G_1 & \longrightarrow & G_2 \\ & (g_1^{\alpha_1}, \ldots, g_k^{\alpha_k}) & \longrightarrow & (h_1^{\alpha_1}, \ldots, k_k^{\alpha_k}) \end{array}$$

Entonces es fácil demostrar que ϕ es isomorfismo de G_1 en G_2.

($\longleftarrow$) Supongamos que G_1 y G_2 dados como en (**??**) son isomorfos. Entonces por la proposición **??** se tiene

$$G_1(p) = G_2(p)$$

De acuerdo con la proposición **??** se tiene que

$$|G_1(p)| = p^k \quad \text{y} \quad |G_2(p)| = p^s$$

luego $s = k$ y por lo tanto G_1 y G_2 tienen el mismo número de invariantes.

Probaremos ahora que los invariantes son iguales, comenzando por el primero. Si suponemos que $n_1 > h_1$, entonces G_1 tiene elementos de orden p^{n_1}, pues el máximo orden de los elementos de G_2 es p^{h_1}. Luego

G_1 y G_2 no pueden ser isomorfos y esto nos lleva a una contradicción. Luego $n_1 = h_1$, lo cual implica que $C_1 \approx C_1'$ en (**??**) .

Si hacemos entonces

$$H = C_2 \times C_3 \times \cdots \times C_k$$

$$K = C_2' \times C_3' \times \cdots \times C_k'$$

es fácil verificar entonces que H es isomorfo a K. Luego podemos aplicar inducción sobre el número de invariantes, se concluye entonces que

$$n_2 = h_2, \ldots, n_k = h_k$$

Con esto queda demostrado que $n_i = h_i$, $1 \leq i \leq k$.

♠

Ejercicios

1) Sea $G = C_{12}$ el grupo cíclico de orden 12. Hallar los subgrupos $G(2)$, $G(4)$ y $G(3)$.

2) Hallar todos los posibles grupos abelianos de orden 200.

3) Demuestre que el número de grupos de orden p^α, no isomorfos, con p un número primo es igual al número de particiones de α.

4) Hallar todos los posibles grupos abelianos de orden 32.

5) Probar que si un grupo finito abeliano G tiene subgrupos de ordenes p y q, con p y q primos diferentes, entonces G tiene un subgrupo de orden pq.

6) Probar que si un grupo finito abeliano tiene orden mn, entonces tiene un subgrupo de orden el mínimo común multiplo de m y n.

7) Sea G un grupo abeliano finito de orden pq con p y q números primos. Probar que todos los subgrupos de G son característicos.

8) Sea G un grupo abeliano finito de orden 5^5 con invariante: $3 > 2 > 0$. ¿Cuántos elementos de orden 5^3 hay en G?

9) Calcule el número de subgrupos de un grupo de orden p^s con invariantes $s - 1 > 1 > 0$.

Capítulo

7

Anillos

7.1 Definiciones Básicas

El concepto de Anillo se obtiene como una generalización de los números enteros, en donde están definidas un par de operaciones, la suma y el producto, relacionadas entre si por una ley de distributividad.

Los anillos pues son estructuras algebraicas más completas que los grupos, pero sin embargo en el estudio de sus propiedades más importantes, nos apoyamos a lo largo de toda la exposición en nuestra experiencia con los grupos. La razon para esto es muy simple, pues todo anillo es un grupo en si mismo.!

Definición 7.1.1 *Un* **anillo** R *es un conjunto no vacío en donde están definidas un par de operaciones llamadas suma y producto, las cuales denotamos por* $+$ *y* $\cdot$ *respectivamente.*

Estas operaciones satisfacen cada una de las propiedades siguientes:

1) Para todo a, $b \in R$, *se tiene que* $a+b$ *y* $a \cdot b$ *están en* R.

2) Para todo a, $b, \in R$ *se tiene que*

$$a + (b + c) = (a + b) + c$$

3) Existe un elemento 0 *en* R, *el cual llamaremos* **cero**, *tal que*

$$a + 0 = 0 + a = a \quad \text{para todo } a \text{ en } R.$$

4) Para todo a *en* R, *existe otro elemento en* R, *denotado por* $-a$, *el cual llamamos el* **opuesto** *de* a *y que verifica*

$$a + (-a) = -a + a = 0$$

5) Para todo a, b *en* R *se tiene*

$$a + b = b + a$$

6) Para todo a, b y c en R se satisface

$$a \cdot (b \cdot c) = (a \cdot b) \cdot c$$

7) Para todo a, b y c en R se satisface

$$\begin{aligned} a \cdot (b + c) &= a \cdot b + a \cdot c \\ (a + b) \cdot c &= a \cdot c + b \cdot c \end{aligned}$$

Observación: De acuerdo a las propiedades 1-5 de la definición, se tiene que todo anillo es un grupo abeliano bajo la suma.

Definición 7.1.2 *Sea R un anillo y supongamos que existe un elemento* $1 \in R$ *tal que*

$$a \cdot 1 = 1 \cdot a = a \quad \textit{para todo } a \textit{ en } R.$$

Entonces el anillo R se dice **anillo unitario** *o* **anillo con unidad**.

Definición 7.1.3 *Sea R un anillo. Si para todos a y b en R se tiene*

$$ab = ba$$

entonces diremos que R es un **anillo conmutativo**.

Definición 7.1.4 *Sea R un anillo, un elemento* $a \in R$ *se dice* **invertible**, *si existe otro elemento* $a^{-1} \in R$ *tal que*

$$a \cdot a^{-1} = a^{-1} \cdot a = 1.$$

Definición 7.1.5 *Un* **anillo de división** *es un anillo con unidad, en donde todos los elementos distintos de cero son invertibles.*

Definición 7.1.6 *Un* **cuerpo** *es un anillo conmutativo con unidad, en donde todos los elementos distintos de cero son invertibles.*

Observación: Existen anillos de división no conmutativos y por ende no cuerpos. Ver problema 13.

Veamos a continuación una serie de ejemplos de anillos

Ejemplo 1: El conjunto $\mathbb{Z}$ de los números enteros, con las operaciones de suma y producto es un anillo conmutativo con unidad.

Ejemplo 2: El conjunto $\mathbb{Z}_m$ de enteros módulo m, con la suma y producto módulo m es un ejemplo de anillo conmutativo con unidad, el cual es finito. La suma y el producto módulo m se definen de la forma siguiente:

Para $[a]$, $[b]$ en $\mathbb{Z}_m$ se tiene

$$[a] + [b] = [a + b]$$

$$[a][b] = [ab]$$

Ejemplo 3: Si p es un número primo, entonces los enteros módulo p, denotado por $\mathbb{Z}_p$, es un cuerpo. Para verificar esto, basta observar que si $[a] \neq [0]$ en $\mathbb{Z}_p$, entonces $p \not| a$ y por lo tanto p y a son primos relativos.

Luego existen enteros x e y tales que

$$a \cdot x + p \cdot y = 1$$

Luego

$$a \cdot x \equiv 1 \ mod \ p.$$

Por lo tanto en $\mathbb{Z}_p$ se tiene que

$$[a] \cdot [x] = [1]$$

de esto se sigue que el elemento $[a]$ es invertible.

Ejemplo 4: Sea $I = [0, 1]$ el intervalo cerrado de números reales y sea R el conjunto de funciones de I en los números reales.

Si f y g son dos funciones, la suma y el producto de ellas se define por:

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

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

Entonces es fácil verificar que R es un anillo con este par de operaciones. Además R posee unidad y R es un anillo conmutativo.

Ejemplo 5: Sea R el conjunto de matrices cuadradas de orden 2×2 con coeficientes reales. Los elementos de R son de la forma:

$$A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$$

donde $a_{ij} \in R$, $1 \leq i \leq 2,\ \ 1 \leq j \leq 2$.

Si A y B son dos elementos de R, entonces la suma y el producto están dadas por:

$$\begin{aligned} A + B &= \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} + \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} \\ &= \begin{pmatrix} a_{11} + b_{11} & a_{12} + b_{12} \\ a_{21} + b_{21} & a_{22} + b_{22} \end{pmatrix} \end{aligned}$$

$$\begin{aligned} A \cdot B &= \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \cdot \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} \\ &= \begin{pmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{pmatrix} \end{aligned}$$

donde

$$c_{ij} = a_{i1}b_{1j} + a_{i2}b_{2j} \text{ para todo } 1 \leq i \leq 2, \quad 1 \leq j \leq 2.$$

Se puede demostrar que R con estas dos operaciones así definidas es un anillo con unidad. Sin embargo R no es conmutativo. Para demostrar esto consideremos el siguiente ejemplo:

Sean

$$A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \quad \text{y} \quad B = \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}$$

Entonces

$$AB = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$$

Mientras que

$$BA = \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}$$

Luego

$$AB \neq BA.$$

Definición 7.1.7 *Sea R un anillo y A un subconjunto de R, el cual es un anillo con las operaciones del anillo R, entonces A se llama un* **subanillo** *de R.*

Ejemplo: El conjunto de los enteros pares $2\mathbb{Z}$, es un subanillo del anillo $\mathbb{Z}$ de los números enteros.

Ejercicios

1) Demuestre que en cualquier anillo R, el conjunto de los elementos invertibles forma un grupo bajo el producto.

2) Pruebe que en un anillo conmutativo con identidad, el elemento unidad es único.

3) Probar que si R es un anillo conmutativo con identidad y a es invertible, entonces $a = (a^{-1})^{-1}$.

4) Sea R el conjunto de parejas ordenadas de números reales. Establecer cuales de las operaciones siguientes determinan una estructura de

a) Anillo.
b) Anillo conmutativo.
c) Anillo conmutativo con unidad.

i) $(a, b) + (c, d) = (a + c, b + d)$
$(a, b) \cdot (c, d) = (ac, bd)$

ii) $(a, b) + (c, d) = (a + c, b + d)$
$(a, b) \cdot (c, d) = (ac + bd, ad + bd)$

iii) $(a, b) + (c, d) = (a, c)$
$(a, b) \cdot (c, d) = (ac, bd)$

iv) $(a, b) + (c, d) = (a + c + 1, b + d)$
$(a, b) \cdot (c, d) = (ad + bc, ac + bd)$

5) Sea R un anillo y $a, b \in R$. Probar la fórmula

$$(a + b)^2 = a^2 + ab + ba + b^2$$

6) Sea R un anillo conmutativo con identidad y n un entero positivo y $a, b \in R$. Probar la fórmula

$$(a + b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k,$$

donde

$$\binom{n}{k} = \frac{n!}{(n-k)!k!}$$

7) **Números Complejos:** Sea R el conjuntos de símbolos de la forma $a + bi$, con a y b números reales, e i la raíz cuadrada de -1, esto es $i^2 = -1$. Convenimos en que dos símbolos $a + bi$ y $c + di$ son iguales si y sólo si $a = c$ y $b = d$. Definimos un par de operaciones en R, mediante

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

Probar que este conjunto R con las operaciones así definidas es un anillo conmutativo con unidad. Este anillo se llama **Anillo de los Complejos**, y lo denotamos por $\mathbb{C}$.

8) **Cuaternios Reales:** Sea R el conjunto de símbolos de la forma $a + bi + cj + dk$, con a, b, c y d números reales, y los símbolos i, j, k definidas por las relaciones:

i) $i^2 = j^2 = k^2 = -1$

ii) $ij = k,\ jk = i,\ ki = j.$

iii) $ji = -k,\ kj = -i,\ ik = -j.$

Convenimos en que dos elementos $a+bi+cj+dk$ y $a'+b'i+c'j+d'k$ son iguales si y sólo si

$$a = a', \quad b = b' \quad c = c', \quad \text{y} \quad d = d'.$$

Definimos la suma de elmentos en R componente por componente, esto es

$$(a+bi+cj+dk)+(a'+b'i+c'j+d'k) = (a+a')+(b+b')i+(c+c')k+(d+d')k$$

La multiplicación de elementos de R se define mediante las leyes de distributividad para expresiones polinómicas y las relaciones $1, 2, 3$. Por ejemplo

$$\begin{aligned}(5 + 3i)(2 + 4k) &= 2 \cdot 5 + 5 \cdot 4k + 3 \cdot 2i + 3 \cdot 4ik \\ &= 10 + 6i - 12j + 20k.\end{aligned}$$

Demostrar que en R, estas operaciones es un anillo de división. Este anillo se denomina anillo de cuaternios reales y se denotan por $\mathcal{Q}$.

9) Sea $(G, *)$ un grupo abeliano y consideremos el conjunto de homomorfismos de G sobre si mismo, denotado por $Hom(G)$. Definimos dos operaciones en este conjunto

$$\begin{aligned}(f+g)(a) &= f(a) * g(a),\\ (f \circ g)(a) &= g(f(a)),\end{aligned}$$

para todo $f, g \in Hom(G)$, y $a \in G$.

Demuestre que $(Hom(G), +, \circ))$ es un anillo.

7.2 Propiedades Elementales de los Anillos

Iniciamos con esta sección el estudio de las propiedades básicas de los anillos. En el transcurso de la misma se daran una serie de definiciones importantes, como lo son: divisor de cero, dominio de integridad y la característica de un anillo. Las mismas serán de utilidad para el resto de este capítulo.

Proposición 7.2.1 *Sea R un anillo, entonces para todos a, $b \in R$, se tiene*

i) $a \cdot 0 = 0 \cdot a = 0$

ii) $a(-b) = (-a)b = -(ab)$

Demostración:
i) Usando la propiedad distributiva (7 de la definición) para R, obtenemos

$$a \cdot 0 = a(0+0) = a \cdot 0 + a \cdot 0$$

Podemos usar a continuación la propiedad de cancelación en el grupo aditivo de R, para concluir

$$a \cdot 0 = 0$$

Similarmente se demuestra que

$$0 \cdot a = 0$$

ii) De acuerdo a *i*) se tiene

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

Por lo tanto el inverso de ab bajo la adición en R (el cual es único) es igual a $a(-b)$ y luego se tiene

$$-(ab) = a(-b)$$

De la misma forma se demuestra que

$$-(ab) = (-a)b$$

y con esto termina la demostración.

♠

Corolario 7.2.1 *Sea R anillo con identidad. Entonces*

i) $(-1)a = -a$ *para todo* $a \in R$

ii) $(-1)(-1) = 1$.

Demostración:

i) Sea $a \in R$, luego podemos usar la proposición anterior para obtener

$$(-1)a = -(1a) = -a$$

ii) Aplicamos la proposición dos veces

$$\begin{aligned}(-1)(-1) &= -(1(-1)) \\ &= -(-(1 \cdot 1) \\ &= 1\end{aligned}$$

Nótese que se hizo uso de la fórmula

$$-(-a) = a, \quad a \in R$$

la cual es cierta en R, por ser un grupo bajo la adición.

♠

Observación: Un anillo R siempre contiene al elemento 0. Si este es el único elemento de R entonces R se llama el **anillo nulo** o el anillo cero.

Si R no es el anillo nulo, y además R contiene una unidad 1, entonces $1 \neq 0$.

En efecto, sea $a \in R$, $a \neq 0$ y supóngase que 1=0, luego

$$\begin{aligned}a &= a1 \\ &= a0 \\ &= 0\end{aligned}$$

lo cual es una contradicción.

Definición 7.2.1 *Sea R un anillo. Un elemento $a \in R$ distinto de cero, se dice* **divisor de cero** *si existe un b en R, distinto de cero, tal que*

$$ab = 0$$

Ejemplo 1: Sea $R = \mathbb{Z}_6$ el anillo de los enteros módulo 6. Luego

$$[2] \neq [0] \quad \text{y} \quad [3] \neq [0],$$

pero

$$\begin{aligned} [2][3] &= [2 \cdot 3] \\ &= [6] \\ &= [0] \end{aligned}$$

por lo tanto [2] y [3] son divisores de cero en este anillo.

Ejemplo 2: Sea $R = \mathbb{Z}$ el anillo de los enteros. Entonces se sabe de las propiedades que definen a los enteros, que $\mathbb{Z}$ no tiene divisores de cero. Para probar esta afirmación, basta usar la ley de cancelación para el producto en $\mathbb{Z}$.

Si $a \neq 0$ y $b \neq 0$ son enteros y además $ab = 0$, se tendrá entonces

$$a0 = 0 = ab$$

de donde

$$b = 0,$$

lo cual es una contradicción.

Definición 7.2.2 *Un anillo conmutativo con identidad que no posee divisores de cero se llama un* **Dominio de Integridad**.

Ejemplo: El anillo $\mathbb{Z}$ de los enteros es un dominio de integridad.

Proposición 7.2.2 *Un anillo conmutativo R, sin divisores de cero, finito es un cuerpo.*

Demostración: Al ser R un dominio de integridad, R es un anillo conmutativo con unidad. Sólo falta probar que todos los elementos de R diferentes de 0 son inversibles.

Consideremos $a \neq 0$ en R, y supongamos

$$R = \{a_1, \ldots, a_n\}$$

Entonces los elementos $aa_1, aa_2, \ldots, aa_n$ son n elementos distintos en R.

En efecto, si suponemos que

$$aa_i = aa_j$$

para algunos $i \neq j$, $1 \leq i \leq n$, $1 \leq j \leq n$, entonces se tendrá:

$$aa_i - aa_j = 0$$

$$a(a_i - a_j) = 0$$

Como R no admite divisores de cero, se debe tener

$$a_i - a_j = 0$$

lo cual implica que $a_i = a_j$, lo cual es una contradicción.

Una vez probado este hecho, el elemento a antes considerado, debe estar entre los aa_i, digamos $a = aa_k$, para algún $1 \leq k \leq n$.

Afirmamos que $a_k = 1$. En efecto, si $a_i \in R$, se tiene que existe un j, $1 \leq j \leq n$, tal que

$$a_i = aa_j$$

Luego

$$\begin{aligned} a_i a_k &= (aa_j)a_k \\ &= (aa_k)a_j \\ &= aa_j \\ &= a_i \end{aligned}$$

Por lo tanto hemos probado que a_k es el elemento unidad de R.

Para concluir, probaremos que el elemento a, elegido al principio es invertible. Siendo a un elemento cualquiera de R distinto de cero, se deduce entonces que todos los elementos de R no nulos son invertibles, y con esto se demuestra que R es un cuerpo.

En efecto, el elemento a_k debe estar entre los elementos $aa_1, \ldots, aa_n$, luego existe j, tal que

$$aa_j = a_k$$

Luego $a_j = a^{-1}$ y a es invertible.

♠

Corolario 7.2.2 *Un Dominio de Integridad finito es un cuerpo.*

Si R es un anillo cualquiera y n es un entero positivo, entonces na es igual a la suma de a $n-$veces. Por otro lado a^n indica el producto de a consigo mismo $n-$veces.

Definición 7.2.3 *Sea R un dominio de integridad. Entonces, el menor entero positivo n (si existe) tal que $na = 0$ para todo $a \in R$ se llama la* **característica** *del anillo. Si no existe dicho entero, entonces se dice que R es de característica 0.*

Ejemplo 1: El anillo $\mathcal{Q}$ de los números racionales con la suma y el producto habituales, es un anillo de característica 0.

Ejemplo 2: El anillo $\mathbb{Z}_7$ de los enteros módulo 7 es de característica 7, pues si $[a] \in \mathbb{Z}_7$, se tiene que

$$7[a] = [7a] = [0]$$

Además no existe un entero positivo menor con dicha propiedad (Verificarlo!).

Teorema 7.2.1 *Si el dominio R es de característica $p > 0$, entonces p debe ser un número primo.*

Demostración: Es claro que $p \cdot 1 = 0$, pues $pa = 0$ para todo a en R.

Por otro lado, si p no es primo, entonces $p = mn$ con $1 < m < p$, $1 < n < p$.

Luego

$$\begin{aligned} p1 &= (mn)1 \\ &= (m1)(n1) \\ &= 0 \end{aligned}$$

Como R es un dominio de integridad, se debe tener $m1 = 0$, o bien $n1 = 0$. Si suponemos $m1 = 0$, entonces para todo $a \in R$ se tendrá

$$\begin{aligned} ma &= m(1a) \\ &= (m1)a \\ &= 0a \\ &= 0 \end{aligned}$$

Luego la característica de R debe ser menor o igual m, lo cual es un absurdo pues $m < p$.

Ejercicios

6) Demuestre que el anillo de matrices cuadradas reales de orden 2×2 no es un dominio de integridad.

8) Si R es un dominio de característica p, probar

$$(a + b)^p = a^p + b^p \quad \text{para todo } a, b \in R.$$

9) Probar que el anillo de funciones $f : [0, 1] \longrightarrow R$ con la suma y producto definidas como en el ejemplo 4, no es un dominio de integridad.

10) Un elemento a en un anillo R se dice nilpotente si $a^n = 0$, para algún n entero positivo. Probar que en un dominio de integridad no hay elementos nilpotentes.

11) Demuestre que un anillo conmutativo D es un dominio de integridad si y sólo si para todos a, b y c en R con $a \neq 0$, la relación $ab = ac$, implica $b = c$.

7.3 Homomorfismos

Los homomorfismos de anillos son aplicaciones entre ellos que preservan las operaciones. Todo homorfismo de anillos es al mismo tiempo un homomorfismo de grupo y esto establece un paralelo entre la teoría de anillos y la teoría de grupos.

Muchas de las definiciones y resultados de esta sección ya han sido estudiadas en los grupos y por lo tanto omitimos algunas demostraciones.

En esta sección se introduce el concepto de ideal, el cual juega el mismo papel que los grupos normales dentro de la teoría de grupos. Mediente el uso de ideales es posible definir los anillos cocientes de forma similar como se hizo para los grupos.

Definición 7.3.1 *Sean R y S dos anillos, un* **homomorfismo de anillos** *entre R y S es una aplicación*

$$\phi : R \longrightarrow S$$

tal que

i) $\phi(r_1 + r_2) = \phi(r_1) + \phi(r_2)$

ii) $\phi(r_1 r_2) = \phi(r_1)\phi(r_2)$
para todo r_1, r_2 en R.

Observación 1: En primer lugar debe tenerse en cuenta que la suma $r_1 + r_2$ en $i)$ se efectua dentro de R, mientras que la suma $\phi(r_1) + \phi(r_2)$

tiene lugar dentro del anillo S. La misma observación es válida para el producto en $ii)$

Observación 2: Obsérvese que de acuerdo a la condición $i)$ todo homomorfismo de anillos es un homomorfismo de grupos y por lo tanto valen todos los resultados sobre homomorfismos, estudiados en el capítulo de grupo.

Ejemplo 1: Sea $\phi : \mathbb{Z} \longrightarrow \mathbb{Z}_m$, la aplicación dada por $\phi(x) = [x]$. Entonces ϕ es un homomorfismo de anillos, pues

$$\begin{aligned} \phi(n+m) &= [n+m] \\ &= [n] + [m] \\ &= \phi(n) + \phi(m) \end{aligned}$$

$$\begin{aligned} \phi(nm) &= [nm] \\ &= [n][m] \\ &= \phi(n)\phi(m) \end{aligned}$$

para todo m, n en $\mathbb{Z}$.

Ejemplo 2: Sea R cualquier anillo y definamos

$$\begin{aligned} \phi \ : \ & R \longrightarrow R \\ & \phi(x) = x \end{aligned}$$

Entonces es fácil verificar que ϕ es un homomorfismo, el cual se llama **homomorfismo identidad**.

Definición 7.3.2 *Sea R y R' dos anillos. Un homomorfismo*

$$\phi : R \longrightarrow R',$$

el cual es biyectivo, se dice que es un **isomorfismo de anillo**.

En tal caso diremos, que los anillos R y R' **son isomorfos** y lo simbolizamos por $R \approx R'$.

Al igual que en los homomorfismos de grupos, se tiene la siguiente propiedad para anillos.

Proposición 7.3.1 *Si $\phi : R \longrightarrow S$ es un homomorfismo de anillos, entonces*

i) $\phi(0) = 0$

ii) $\phi(-a) = -\phi(a)$ *para todo* $a \in R$

Demostración: (Ver el capítulo de grupos).

♠

También se define el **Kernel o núcleo** del homomorfismo, exactamente como se hizo en el caso de grupos.

Definición 7.3.3 *Sea $\phi : R \longrightarrow S$ un homomorfismo de anillos, entonces el* **Kernel** *del homomorfismo ϕ se define por*

$$\ker \phi = \{x \in R \mid \phi(x) = 0\}.$$

Observación: Si a y b son dos elementos en el $\ker \phi$, entonces será cierto, de acuerdo a la definición de homomorfismo, que $a + b$ y ab están en $\ker \phi$. Pero además de esta propiedad, el Kernel posee otra muy interesante y es que al multiplicar un elemento cualquiera del anillo por un elemento en el Kernel, entonces el producto de ambos esta de nuevo en el Kernel. Esta propiedad de "absorber" todos los elementos del anillo por multiplicación, motiva la siguiente:

Definición 7.3.4 *Sea R un anillo. Un subconjunto I de R se dice* **ideal a la derecha**, *si se tiene:*

i) $a + b \in I$ *, para todo* $a, b \in I$

ii) $\gamma a \in I$*, para todo* $\gamma \in R$ *y* $a \in I$*.*

Definición 7.3.5 *Sea R un anillo. Un subconjunto I de R se dice* **ideal a la izquierda**, *si satisface*

i) $a + b \in I$, *para todo* $a, b \in I$

ii) $a\gamma \in I$, *para todo* $\gamma \in R$ *y* $a \in I$.

Combinando ambas definiciones tenemos

Definición 7.3.6 *Sea R un anillo. Un subconjunto I de R se dice* **ideal de** *R, si I es un ideal a la derecha y a la izquierda.*

Observación: Cuando se estudian anillos conmutativos (como es el caso de la mayoría de los anillos), entonces todo ideal lateral, a la derecha o a la izquierda, es un ideal del anillo. Por lo tanto no se hace necesario verificar las dos condiciones simultáneamente.

Ejemplo 1: Sea $\mathbb{Z}$ el anillo de enteros y consideremos $I = 2\mathbb{Z}$, el conjunto de los enteros pares. Entonces se puede verificar que I es un ideal de $\mathbb{Z}$.

Ejemplo 2: Sea R el anillo de funciones de $[0, 1]$ en R y S el conjunto de funciones en R, tales que $f(\frac{1}{2}) = 0$. Luego se prueba fácilmente que S es un ideal del anillo R.

Ejemplo 3: Sea $\phi : R \longrightarrow R'$ un homomorfismo de anillos. Entonces el Kernel de ϕ es un ideal de R.

Si I es cualquier ideal en un anillo R, entonces I es un subgrupo normal del grupo aditivo de R. Luego se puede considerar el conjunto cociente R/I de clases laterales derechas. Este conjunto se le puede dotar de una estructura de anillo, con las operaciones de suma y producto de clases definidas de la forma siguiente

$$(a + I) + (b + I) = a + b + I \tag{7.1}$$
$$(a + I)(b + I) = ab + I \tag{7.2}$$

En estas condiciones se tiene:

Teorema 7.3.1 *Sea R un anillo e I un ideal de R. Entonces el conjunto cociente formado por las clases laterales*

$$R/I = \{a + I \mid a \in R\}$$

es un anillo

Este anillo se denomina **anillo cociente**.

Demostración: Debemos verificar en primer lugar que la suma y el producto de clases están bien definidas.

Sean a, b, a', c' elementos en R y supongamos que

$$a + I = a' + I \tag{7.3}$$
$$b + I = b' + I \tag{7.4}$$

Debemos verificar entonces que

1) $a + b + I = a' + b' + I$

2) $ab + I = a'b' + I$

En efecto, para la primera parte usamos las ecuaciones (**??**) y (**??**) para obtener

$$a - a' \in I \quad \text{y} \quad b - b' \in I.$$

Como I es un ideal, la suma de dos elementos cualesquiera en I estará de nuevo en I. Por lo tanto

$$(a - a') + (b - b') \in I,$$

luego

$$(a + b) - (a' + b') \in I,$$

de donde,

$$a + b + I = a' + b' + I.$$

Para la segunda parte, tomamos s_1 y s_2 en I, tales que

$$a = a' + s_1 \quad \text{y} \quad b = b' + s_2$$

Multiplicando estos dos elementos se obtiene

$$\begin{aligned} ab &= (a' + s_1)(b' + s_2) \\ &= a'b' + s_1b' + bs_2 + s_1s_2 \end{aligned}$$

Como I es un ideal, los elementos s_1b', bs_2 y s_1s_2 están todos en I. Luego

$$ab = a'b' + s$$

donde $s = s_1b' + bs_2 + s_1s_2 \in I$

Por lo tanto se concluye

$$ab + I = a'b' + I$$

La verificación de que R/I es un anillo con las dos operaciones dadas en (**??**) y (**??**), se deja como un ejercicio para el lector. Sin embargo haremos algunas acotaciones importantes es este sentido.

Por ejemplo, el elemento cero R/I, viene dado por

$$0 = 0 + I,$$

donde 0 es el cero en R.

Si R posee identidad 1, entonces el anillo cociente posee identidad, dada por

$$1 = 1 + I.$$

Si R es conmutativo, entonces el anillo cociente también es conmutativo.

Teorema 7.3.2 *Sea R un anillo e I un ideal de R. Entonces la aplicación*

$$\phi : R \longrightarrow R/I, \qquad \gamma \longrightarrow \gamma + I$$

es un homomorfismo de anillos sobreyectivo, con $\ker \phi = I$*, llamado la* **proyección de R sobre I.**

Demostración: La demostración de la condición de homomorfismo ϕ, se deriva de las ecuaciones (**??**) y (**??**). En efecto, si γ_1, γ_2 están en R, se tiene

$$\begin{aligned} \phi(\gamma_1 + \gamma_2) &= (\gamma_1 + \gamma_2) + I \\ &= (\gamma_1 + I) + (\gamma_2 + I) \\ &= \phi(\gamma_1) + \phi(\gamma_2) \end{aligned}$$

$$\begin{aligned} \phi(\gamma_1\gamma_2) &= \gamma_1\gamma_2 + I \\ &= (\gamma_1 + I)(\gamma_2 + I) \\ &= \phi(\gamma_1)\phi(\gamma_2) \end{aligned}$$

Evidentemente, el homomorfismo es sobreyectivo. Veamos a continuación la determinación del $\ker \phi$.

Sea $\gamma \in R$, tal que

$$\phi(\gamma) = \gamma + I = I$$

Luego $\gamma \in I$.

Por otro lado, si $\gamma \in I$ es claro que

$$\phi(\gamma) = I = 0 \quad \in R/I.$$

Luego

$$I = \ker \phi$$

♠

Basándonos en los teoremas de isomorfismos para los grupos, damos a continuación dos teoremas sobre homomorfismos de anillos. Las demostraciones se omiten pues son muy semejantes a las demostraciones dadas en el caso de los grupos.

Teorema 7.3.3 *Sea $\phi : R \longrightarrow S$ un homomorfismo de anillos sobreyectivo. Entonces*

i) Si I es un ideal de R que contiene a $\ker\phi$, entonces el conjunto

$$I' = \{\phi(x) \mid x \in I\}$$

es un ideal de S.

ii) Si L es un ideal de S, entonces el conjunto

$$\phi^{-1}(L) = \{x \in R \mid \phi(x) \in L\}$$

es un ideal de R que contiene a $\ker\phi$.

Teorema 7.3.4 *Sea $\phi : R \longrightarrow S$ un homomorfismo de anillos sobreyectivo con $K = \ker\phi$, y supongamos que I es un ideal de R que contiene a K. Sea L el ideal de S, dado por $L = \phi(I)$. Entonces*

$$R/K \approx S/L$$

Ejercicios

1) Sea U un ideal de anillo R y supongamos que el elemento unidad de R está en U. Probar entonces que $U = R$.

2) Probar que si R es un cuerpo, entonces los únicos ideales son (0) y R.

3) Probar que cualquier homomorfismo de anillos $\phi : R \longrightarrow S$, con R cuerpo, satisface $\phi = 0$ o $\phi =$identidad.

4) Sean I y J ideales de un anillo R. Entonces la suma de I con J se define

$$I + J = \{x + y \mid x \in I,\ y \in J\}$$

El producto de I con J se define por

$$IJ = \left\{ \sum_{i=1}^{n} x_i y_i \mid \text{ donde } x_i \in I,\ y_i \in J,\ 1 \leq i \leq n,\ n \geq 1 \right\}$$

Entonces probar que tanto $I + J$ como IJ son ideales de R.

5) Probar que si $\phi : R \longrightarrow S$ es un homomorfismo de anillos, sobre y $1 \in R$, entonces $\phi(1)$ es la identidad en S. Dar un ejemplo en donde esto no se cumple si se remueve la condición de sobreyectividad.

6) Sea $\phi : R \longrightarrow S$ un homomorfismo de anillos sobre. Probar que si I es un ideal de R, entonces $\phi(I)$ es un ideal de S.

7) Sea R un anillo, U un ideal de R y

$$\gamma(U) = \{x \in R \mid xu = 0,\ \forall u \in U\}$$

Probar que $\gamma(U)$ es un ideal de R. Este ideal se llama el **radical de** U.

8) Demuestre que si $\phi : \mathbb{Z} \longrightarrow \mathbb{Z}$ es un homomorfismo de anillos sobreyectivo, entonces $\phi =$ identidad.

9) Sea R el anillo de matrices cuadradas reales 2×2 y consideremos el subconjunto S, de R de todas aquellas matrices de la forma

$$\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$$

i) Probar que S es un sub-anillo de R.

ii) ¿Es S un ideal de R?.

10) Sea S el anillo de matrices definido arriba y $\mathbb{C}$ el anillo de los complejos. Probar que S es isomorfo a $\mathbb{C}$.

11) Sea $\mathbb{C}$ el anillo de los complejos, probar que la aplicación

$$\begin{array}{rccc} \phi & : & \mathbb{C} & \longrightarrow & \mathbb{C} \\ & & a+bi & \longrightarrow & a-bi \end{array}$$

es un homomorfismo de anillos.

12) Sea R un anillo conmutativo y $a \in R$. Definamos el conjunto

$$Ra = \{ra \mid r \in R\}$$

Probar que Ra es un ideal de R. Este ideal se denomina el **ideal generado por** a.

13) Sea R un anillo conmutativo con 1. Probar que $a \in R$ es invertible si y sólo si $Ra = R$.

14) Probar que si I y J son ideales de un anillo R, entonces $I \cap J$ es también un ideal.

Capítulo

8

Anillos Especiales

8.1 Conceptos Básicos

En este capítulo nos dedicaremos al estudio de algunos anillos especiales que poseen ciertas condiciones adicionales, aparte de las propias de la definición, como por ejemplo los Dominios de Integridad, los Dominios de Factorización Unica y los Dominios Euclideanos.

A todo dominio de integridad se le puede asociar un cuerpo, llamado Cuerpo de Fracciones, en el cual se sumerge de la misma manera como los números enteros se insertan en los números racionales. Veremos como se construye este cuerpo de cocientes y el homomorfismo que permite obtener esta interesante conexión.

Una de las propiedades fundamentales del anillo de los números enteros es que todo entero se expresa de manera única como un producto de números primos. Esta propiedad se generaliza en forma natural a los Dominios de Integridad, originandose así el concepto de Dominio de Factorización Unica.

Existen algunos anillos que gozan de buenas propiedades de factorización y divisibilidad. Entre ellos se encuentran los Dominios Euclideanos, los cuales son a la vez dominios de Factorización Unica. Los ejemplos más conocidos de un Dominio Euclideano son los números enteros y los polinomios, pero también existen otros no tan usados como son los Enteros de Gauss. Haremos un estudio de estos enteros y sus propiedades más relevantes.

En todo este capítulo, cuando se diga anillo, supondremos que se trata de un anillo conmutativo con unidad.

Definición 8.1.1 *Sea R un anillo. Un ideal P de R ($P \neq R$), se dice* **ideal primo**, *si para todo a, b en R tales que $ab \in P$, entonces $a \in P$ ó $b \in P$.*

Ejemplo: Sea $R = \mathbb{Z}$ anillo de los enteros y J el ideal formado por los números pares. Entonces J es un ideal primo de R.

Definición 8.1.2 *Sea R un anillo. Un ideal M de R ($M \neq R$), se llama* **ideal maximal**, *si para todo ideal J tal que*

$$M \subseteq J \subseteq R$$

se tiene

$$M = J \quad ó \quad J = R$$

Proposición 8.1.1 *Sea P un ideal de R. Entonces P es un ideal primo si y sólo si R/P es un dominio de integridad.*

Demostración: $\Longrightarrow$) Sea P un ideal primo de R. Supongamos que existen elementos $a + P$ y $b + P$ en el anillo cociente R/P tal que

$$(a + P)(b + P) = 0$$

Luego

$$ab + P = P$$

y por lo tanto

$$ab \in P$$

Como P es un ideal primo, se tendrá

$$a \in P \quad ó \quad b \in P$$

Luego

$$a + P = 0 \quad ó \quad b + P = 0$$

Por lo tanto R/P, es un anillo conmutativo con unidad, el cual no tiene divisores de cero y luego es un Dominio de Integridad.

$\Longleftarrow$) Por otro lado supongase que R/P es un domino de integridad. Si P no es primo, existen elementos a y b en R tal que

$$a \notin P, \;\; b \notin P \quad \text{y} \quad ab \in P$$

Luego

$$a + P \neq 0 \quad \text{y} \quad b + P \neq 0$$

pero

$$(a + P)(b + P) = ab + P = 0$$

Esto implica que $a + P$ es un divisor de cero, lo cual es una contradicción. Luego $a \in P$ o $b \in P$.

Además $P \neq R$, pues $R/P \neq (0)$. En conclusión, el ideal P es primo.

♠

Proposición 8.1.2 *Sea M un ideal de un anillo R. Entonces M es maximal si y sólo si R/M es un cuerpo.*

Demostración: $\Longrightarrow$) Sabemos que R/M es un anillo conmutativo con unidad, pues R lo es. Solo falta probar que todo elemento de R/M distinto de cero es inversible, para que R/M sea un cuerpo.

Sea $a + M \neq 0$ en R/M. Luego construimos el ideal J de la forma siguiente:

$$J = Ra + M$$

Se tiene entonces que $M \subsetneq J$, pues $a \notin M$ y por ser M un ideal maximal, se deduce de la definición que

$$Ra + M = R \tag{8.1}$$

Como $1 \in R$ se tiene de (**??**)

$$ra + m = 1 \tag{8.2}$$

para algunos elementos $r \in R$ y $m \in M$. Por lo tanto, usando (**??**) se concluye

$$(r + M)(a + M) = 1 + M$$

Luego hemos probado que $r + M$ es el inverso de $a + M$.

$\Longleftarrow$) Supongase ahora que R/M sea un cuerpo. Sea I un ideal de R tal que

$$M \subseteq I \subseteq R$$

Si suponemos que $I \neq R$, entonces el ideal I/M es un ideal propio de R/M. Pero los únicos ideales de R/M son (0) y él mismo, pues R/M es un cuerpo. Luego

$$I/M = (0)$$

de donde

$$I = M$$

Por lo tanto M es un ideal maximal.

♠

Se sabe que todo cuerpo es un dominio de integridad, luego podemos combinar los dos teoremas anteriores para obtener:

Corolario 8.1.1 *Sea R un anillo. Entonces todo ideal Maximal es un ideal primo.*

Ejemplo 1: Sea I un ideal de $\mathbb{Z}$. Entonces I es un subgrupo del grupo aditivo de $\mathbb{Z}$, y por lo tanto es de la forma $I = (m)$ para algún $m \in \mathbb{Z}$. Si I es un ideal primo, entonces el elemento m debe ser un número primo. Caso contrario se tiene

$$m = n_1 n_2$$

con $1 < n_1 < m,\ \ 1 < n_2 < m$

Luego el producto de n_1 y n_2 está en el ideal I, pero $n_1 \notin I$ y $n_2 \notin I$. Por otro lado si p es un número primo, afirmamos que el ideal $P = (p)$ es un ideal primo. En efecto si para algunos n_1, n_2 se tiene

$$n_1 n_2 \in P,$$

se deduce que

$$n_1 n_2 = kp \quad \text{para algún} \quad k \in \mathbb{Z}$$

Luego

$$p | n_1 n_2$$

y por lo tanto

$$p | n_1 \quad \text{ó} \quad p | n_2$$

Si suponemos que $p|n_1$ se tiene

$$n_1 = sp \tag{8.3}$$

para algún s entero, y de (**??**) se deduce que $n_1 \in P$. Igualmente, si suponemos que $p|n_2$ se llega a que $n_2 \in P$. Por lo tanto el ideal P es primo.

En conclusión hemos demostrado que los únicos ideales primos de $\mathbb{Z}$ son de la forma: $P = (p)$ con p un número primo. Mostraremos que dichos ideales son también maximales.

En efecto, sea p un número primo, $P = (p)$ y J otro ideal tal que

$$P \subseteq J \subseteq \mathbb{Z}$$

Luego si suponemos que $P \neq J$, existe un elemento n, el cual está en J pero no en P. Por lo tanto $p \not| n$ y así se tendrá que p y n son un par de enteros primos relativos. Luego existen enteros x e y tales que

$$px + ny = 1$$

Ahora bien, de acuerdo a las propiedades de ideal de J se tendrá

$$px \in P \subseteq J$$

y

$$ny \in J$$

Luego

$$1 = px + ny \in J,$$

de donde

$$J = \mathbb{Z}$$

Luego hemos probado que todo ideal primo de $\mathbb{Z}$ es maximal.

Observación: Existen anillos que poseen ideales primos los cuales no son maximales. Sin embargo en el caso de los números enteros sí se tiene esta propiedad.

Ejemplo 2: Sea $R = \mathbb{Z} + \mathbb{Z}$ conjunto de parejas ordenadas de números enteros, con las operaciones:

Suma: $(a, b) + (c, d) = (a + c, b + d)$

Producto: $(a, b)(c, d) = (ac, bd)$

Entonces es fácil verificar que R es un anillo conmutativo con unidad.

Sean

$$I = \{(0, y) \mid y \in \mathbb{Z}\}$$

$$M = \{(2x, y) \mid x, y \in \mathbb{Z}\}$$

Entonces es fácil verificar que tanto I como M son ideales propios de R.

Además el ideal I es primo, pues si se tiene

$$(a, b)(c, d) \in I$$

entonces

$$ac = 0$$

Como $\mathbb{Z}$ es dominio de integridad, se tiene

$$a = 0 \quad \text{ó} \quad c = 0,$$

de donde

$$(a, b) \in I \quad \text{ó} \quad (c, d) \in I$$

Sin embargo I no es un ideal maximal, pues se tiene

$$I \subseteq M \subseteq R$$

y

$$M \neq I \ , \ M \neq R.$$

8.2 Cuerpo de Cocientes de un Dominio de Integridad

Si D es un Dominio de Integridad, no todos los elementos de D poseen un inverso bajo la multiplicación, como es el caso del anillo de los enteros.

Podemos entonces construir un cuerpo que contenga a D, de la misma forma como se construyen las fracciones de números enteros, el cual contiene a $\mathbb{Z}$ como un subanillo.

Esta construcción es muy similar a la construcción de los números racionales a partir de los enteros. Cuando se tiene una fracción $\frac{a}{b}$, entonces puede existir otra representación $\frac{e}{d}$ de la misma fracción. En tal caso se tiene que

$$\frac{a}{b} = \frac{c}{d}, \quad \text{si y sólo si} \quad ad = bc.$$

Esta condición de igualdad de fracciones, será el punto de partida de nuestra exposición.

Sea D un Dominio de Integridad y A el subconjunto del producto cartesiano $D \times D$, formados por pares de la forma (a, b), tal que $b \neq 0$.

Entonces definimos una relación A, mediante

$$(a, b) \sim (c, d) \quad \text{si y sólo si} \quad ad = bc$$

Proposición 8.2.1 *La relación " $\sim$ " es una relación de equivalencia.*

Demostración:

1) **Reflexiva:** Sea $(a, b) \in A$, entonces claramente

$$(a, b) \sim (a, b)$$

pues

$$ab = ba$$

2) **Simétrica:** Sea $(a, b) \sim (c, d)$. Entonces

$$ad = bc,$$

y como D es conmutativo, se obtiene

$$cb = da,$$

luego

$$(c, d) \sim (a, b)$$

3) **Transitiva:** Sea $(a, b) \sim (c, d)$ y $(c, d) \sim (e, f)$. Luego

$$ad = bc,$$

y

$$cf = de$$

Multiplicando la primera ecuación por f, la segunda por b y luego restando ambas nos produce

$$adf - bde = 0$$

o sea

$$d(af - be) = 0$$

De la última ecuación se deduce

$$af - be = 0,$$

pues $d \neq 0$ y D es un dominio de integridad.

Por lo tanto

$$(a, b) \sim (e, f)$$

Con esto termina la demostración

♠

Una vez hecho esto, consideremos el conjunto cociente de todas las clases de equivalencia de esta relación y denotemoslo por F. Así pues

$$F = \{[a, b] \mid (a, b) \in A\}$$

donde $[a, b]$ denota la clase de equivalencia del elemento (a, b) en A.

Seguidamente, definimos en F un par de operaciones

Suma: $[a, b] + [c, d] = [ad + bc, bd]$

Producto: $[a, b][c, d] = [ac, bd]$

Notemos en primer lugar que $bd \neq 0$, puesto tanto b como d son no nulos y D es un dominio de integridad, y por lo tanto la suma y el producto de clases es una operación cerrada.

Probaremos que estas operaciones están bien definidas. Esto es, supongase que para algunos elementos $a, b, c, d, a', b', c', d'$ en D con $bd \neq 0$ y $b'd' \neq 0$, se tiene

$$[a, b] = [a', b']$$

$$[c, d] = [c', d']$$

Luego debemos tener

$$ab' = ba' \quad \text{y} \quad cd' = dc' \tag{8.4}$$

Por lo tanto

$$[a, b] + [c, d] = [ad + bc, bd]$$

$$[a', b'] + [c', d'] = [a'd' + b'c', b'd']$$

Debemos probar entonces

$$[ad + bc, bd] = [a'd' + b'c', b'd']$$

o lo que es lo mismo

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

si y sólo si

$$adb'd' + bcb'd' = a'd'bd + b'c'bd \tag{8.5}$$

Entonces si partiendo de las relaciones en (**??**), llegamos a probar la ecuación (**??**), la suma estará bien definida.

Para demostrar la igualdad (**??**) comenzaremos por desarrollar el lado izquierdo, hasta obtener el término de la derecha. Luego

$$\begin{aligned} adb'd' + bcb'd' &= ab'(dd') + cd'(bb') \\ &= ba'(dd') + dc'(bb') \\ &= a'd'bd + b'c'bd \end{aligned}$$

Con esto queda demostrado (**??**).

Para el producto, la demostración es bastante similar. En efecto, supóngase que (**??**) es cierto y entonces se desea probar

$$[a, b][c, d] = [a', b'][c', d']$$

o lo que es equivalente a

$$[ac, bd] = [a'c', b'd']$$

Si y sólo si

$$ac(b'd') = bd(a'c') \tag{8.6}$$

Desarrollando el lado izquierdo de (**??**) y usando (**??**) se tiene

$$\begin{aligned} ac(b'd') &= ab'(cd') \\ &= (ba')(dc') \\ &= bd(a'c') \end{aligned}$$

Luego (**??**) se cumple, y por lo tanto el producto está bien definido.

Dejaremos como ejercicio para el lector la verificación de las propiedades de anillo de F, con este par de operaciones, en donde los elementos $[0, a]$ y $[a, a]$ actúan como elemento cero e identidad, donde a es cualquier elemento no nulo de D.

Para ver esto último, sea $[e, f] \in F$. Luego

$$\begin{aligned} [e, f] + [0, a] &= [ea + 0f, fa] \\ &= [ea, fa] \\ &= [e, f] \end{aligned}$$

$$\begin{aligned} [e, f][a, a] &= [ea, fa] \\ &= [e, f] \end{aligned}$$

Finalmente, probaremos que todo elemento no nulo $[a, b]$ de F, posee un inverso multiplicativo. En efecto, como $a \neq 0$, entonces $[b, a] \in F$ y además

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

Luego $[a, b]^{-1} = [b, a] \in F$. Resumiremos todos estos resultados en el siguiente teorema

Teorema 8.2.1 *Sea D un dominio de integridad cualquiera, entonces el conjunto*

$$F = \{[a,b] \mid a,b \in D \quad y \quad b \neq 0\}$$

es un cuerpo, el cual se denomina **Cuerpo de Cocientes de D**.

Teorema 8.2.2 *Sea D un dominio de integridad y F su cuerpo de fracciones. Entonces la aplicación*

$$\begin{array}{rccc} \phi & : & D & \longrightarrow & F \\ & & a & \longrightarrow & [a,1] \end{array}$$

es un homomorfismo inyectivo, el cual se denomina la **Inmersión Canónica** *de D en F.*

Demostración: Sean $a,b \in D$. Luego

$$\begin{array}{rcl} \phi(a+b) & = & [a+b,1] \\ & = & [a1+1b, 1\cdot 1] \\ & = & [a,1]+[b,1] \\ & = & \phi(a)+\phi(b) \end{array}$$

También

$$\begin{array}{rcl} \phi(ab) & = & [ab,1] \\ & = & [a,1][b,1] \end{array}$$

Además, probaremos que ϕ es $1:1$, para lo cual sean $a,b \in D$, tales que

$$\phi(a) = \phi(b)$$

Luego

$$[a, 1] = [b, 1]$$

de donde

$$a = b$$

Con esto se concluye la demostración.

♠

Ejercicios

1) Probar que si D es un dominio de integridad, entonces el ideal (0) es primo.

2) Sea R un anillo conmutativo con unidad, en donde los únicos ideales son (0) y R. Probar que R debe ser un cuerpo.

3) Probar la propiedad conmutativa para la suma y el producto en F.

4) Demuestre que si D es un dominio de integridad y K es un cuerpo que contiene a D, entonces K contiene a F.

5) Probar que todo cuerpo de característica 0, contiene una copia homomorfica del cuerpo $\mathcal{Q}$.

6) Probar que $\mathcal{Q}$ es el menor cuerpo que contiene a los números enteros.

7) Sean D y D' dos dominios de integridad y

$$\varphi : D \longrightarrow D'$$

un homomorfismo inyectivo. Probar que existe un homomorfismo inyectivo entre el cuerpo de cocientes de D y el cuerpo de cocientes de D'.

8) Probar que en todo dominio de integridad D se verifican las leyes de cancelación para el producto. Esto es,

$$\text{si} \quad a, b, c \quad \text{están en} \quad D \quad \text{y} \quad a \neq 0,$$

entonces

$$ab = ac \Longrightarrow b = c$$

$$ba = ca \Longrightarrow b = c$$

9) Probar que en todo anillo conmutativo con unidad, cualquier ideal está contenido en un ideal maximal.

10) Sean I, J dos ideales primos en $\mathbb{Z}$, tales que

$$I \cap J = (0).$$

Probar que

$$I + J = \mathbb{Z}$$

11) Sea D un dominio de integridad con cuerpo de cocientes K y sea $[a, b] \in K$. Entonces demostrar

i) $[af, bf] = [a, b] \quad \forall\ f \in K,\ f \neq 0.$
ii) $[a, b] + [c, b] = [a + c, b]$.
iii) $-[a, b] = [-a, b]$.

12) Sea D un cuerpo y K su cuerpo de fracciones. Demuestre que K es isomorfo a D.

13) Probar que $R = \mathbb{Z} \oplus \mathbb{Z}$ con las operaciones

$$(a, b) + (c, d) = (a + c), b + d)$$

$$(a, b)(c, d) = (ac, bd)$$

es un anillo conmutativo con unidad.

14) Sea R como en el ejercicio anterior. Probar que el conjunto

$$I = \{(0, y) \mid y \in \mathbb{Z}\}$$

es un ideal de R.

15) Sean $X = [3, 2]$ e $Y = [-5, 4]$ en el cuerpo cociente de $\mathbb{Z}$. Calcular

a) $X + Y$
b) XY
c) X^{-1}
d) Y^{-1}

8.3 Dominios de Factorización Unica

Definición 8.3.1 *Sea R un anillo y J un ideal de R. Entonces J se dice* **ideal principal** *si existe un elemento $a \in J$, tal que $J = (a)$.*

También se dice que J esta **generado** por el elemento a.

Definición 8.3.2 *Un dominio de integridad en donde todos los ideales son principales, se denomina* **dominio de ideales principales**.

Ejemplo: El anillo de los enteros $\mathbb{Z}$ es un dominio de ideales principales. Si I es un ideal de $\mathbb{Z}$, entonces I es un subgrupo del grupo abeliano $\mathbb{Z}$ con la suma, y por lo tanto I es de la forma (m) para algún $m \in \mathbb{Z}$.

Definición 8.3.3 *Sean a y b elementos en un anillo R, con $a \neq 0$. Diremos que a* **divide a** *b, si existe un elemento c en R, tal que $b = ac$.*

Usaremos el símbolo $a|b$ para indicar que el elemento a divide a b, como se hace para los números enteros.

Observación: Podemos definir en R una relación, mediante

$$a \sim b \quad \text{si y sólo si} \quad a|b$$

Entonces se puede verificar que esta relación es reflexiva y transitiva, pero no es simétrica en general.

Proposición 8.3.1 *Sean a y b elementos en un anillo R. Entonces si*

$$a|b \quad y \quad a|c,$$

se tiene

$$a|bx + cy$$

para todo par de elementos x, y en R.

Demostración: Fácil.

Definición 8.3.4 *Sea R un anillo. Un elemento $u \in R$, se dice* **unidad** *si existe v en R, tal que*

$$uv = 1$$

Observación: Es importante destacar la diferencia entre un elemento unidad de un anillo y la unidad del anillo, el cual siempre será denotado por el símbolo 1. El elemento 1 actua como elemento neutro para el producto, mientras que una unidad u no necesariamente satisface $ua = 1$ para todo a en el anillo. Obviamente, el 1 es una unidad en todo anillo.

Definición 8.3.5 *Un elemento a en un anillo R se dice* **elemento irreducible***, si a no es unidad y cada vez que se tenga una factorización del tipo*

$$a = bc$$

entonces b ó c es una unidad en el anillo.

Ejemplo: Se puede demostrar fácilmente que los elementos irreducibles del anillo $\mathbb{Z}$ de los enteros, son precisamente los números primos.

Proposición 8.3.2 *Sea D un dominio de integridad. Entonces si para algún par de elementos a y b en R se tiene que $a|b$ y $b|a$, se debe cumplir $a = ub$, donde u es una unidad.*

Demostración: Si $a|b$, existe un elemento c en R, tal que $b = ac$. Igualmente, si $b|a$ existe un elemento e en R, tal que $a = be$.

Combinando ambos resultados obtenemos

$$b = bec$$

de donde

$$b(1 - ec) = 0$$

Como $b \neq 0$ y D es un dominio de integridad, se deduce $ec = 1$, lo cual implica que e es una unidad.

♠

Definición 8.3.6 *Dos elementos a y b en un anillo R, se dicen* **asociados**, *si existe una unidad u en R, tal que*

$$a = bu$$

Observación: Si D es un dominio de integridad, entonces la relación de asociados en D es una relación de equivalencia.

Definición 8.3.7 *Un dominio de integridad D se dice* **Dominio de Factorización Unica** *si todo elemento $a \in D$, el cual no es 0 ni unidad, puede ser factorizado como un producto finito de elementos irreducibles, esto es*

$$a = p_1 \cdots p_s$$

donde los p_i son irreducibles.

Además si a tiene otra factorización distinta como producto de irreducibles, digamos

$$a = q_1 \cdots q_t$$

donde los q_j son irreducibles, entonces $s = t$ y cada p_i es asociado de algún q_j.

Más adelante probaremos que todo Dominio de Ideales Principales, es un Dominio de Factorización Unica. Antes, daremos un lema muy interesante el cual establece una condición de cadena en ideales, para cualquier Dominio de Ideales Principales.

Definición 8.3.8 *Sea R un anillo, entonces una* **cadena ascendentee de ideales** *es una familia de ideales de R, $\{I_i\}, i \geq 1$, tales que*

$$I_1 \subseteq I_2 \subseteq \cdots \subseteq I_i \subseteq I_{i+1} \subseteq \ldots$$

Lema 8.3.1 *Toda cadena ascendente de ideales $\{I\}_{i\geq 1}$ está acotada superiormente por un ideal J de R. Es decir*

$$I_i \subseteq J, \quad \forall i \geq 1$$

Demostración: Tomemos

$$J = \bigcup_{i\geq 1} I_i$$

Es claro que J contiene a todos los I_i. Afirmamos que J es un ideal de R.

En efecto, sean $a, b \in J$ y $r \in R$. Debemos probar entonces

1) $a \pm b \in J$

2) $ra \in J$

Si $a, b \in J$, entonces existen i_1, i_2, tales que

$$a \in I_{i_1} \quad \text{y} \quad b \in I_{i_2}$$

Sin pérdida de generalidad, podemos suponer que $i_1 > i_2$, de donde se tendrá entonces $a \in I_{i_1}$, $b \in I_{i_1}$ y como I_{i_1} es un ideal se tiene

$$a \pm b \in I_{i_1} \subseteq J$$

$$ra \in I_{i_1} \subseteq J$$

Luego se cumplen las condiciones 1) y 2) y con esto finaliza la prueba.

♠

Lema 8.3.2 *Sea D un dominio de ideales principales. Entonces toda cadena ascendente de ideales*

$$I_1 \subseteq I_2 \subseteq \cdots \subseteq I_n \subseteq \ldots$$

es estacionaria.

Es decir, existe un entero positivo k tal que

$$I_n = I_k, \quad \forall n \geq k$$

Demostración: Sea

$$I = \bigcup_{i \geq 1} I_i$$

Entonces de acuerdo al lema amterior, I es un ideal de D, el cual contiene a todos los I_n. Luego el ideal I es principal, pues D es un dominio de ideales principales, y por lo tanto existe un elemento a en D tal que $I = (a)$.

Como I es una unión de conjuntos y $a \in I$, existe un miembro de la familia, digamos I_k tal que $a \in I_k$.

Luego si $n \geq k$ se tendrá

$$I = (a) \subseteq I_k \subseteq I_n \subseteq I$$

Por lo tanto

$$I_n = I_k$$

♠

Teorema 8.3.1 *Todo Dominio de Ideales Principales es un Dominio de Factorización Unica.*

Demostración: Sea D un dominio de ideales principales y a un elemento de D, el cual no es cero, ni es una unidad.

Si a es irreducible, entonces a es un producto de elementos irreducibles.

Supongase que a no es irreducible. Entonces existen un par de elementos a_1 y a_2 (no unidades) tales que

$$a = a_1 a_2$$

Si tanto a_1 como a_2 son irreducibles, entonces el teorema es cierto. Supongase que a_1 no es irreducible y hagamos $a_0 = a$. Luego se tiene una cadena de dos ideales

$$(a_0) \subsetneq (a_1)$$

Continuando de esta manera se tiene una cadena ascendente de ideales, estrictamente contenidos, de la forma

$$(a_0) \subsetneq (a_1) \subsetneq \cdots \subsetneq (a_n) \subsetneq \cdots$$

Como D es un dominio de ideales principales, existe un k, tal que

$$(a_n) = (a_k), \quad \forall n \geq k.$$

Entonces el elemento a_k es un irreducible, pues si suponemos

$$a_k = bc$$

Se tendrá $a_{k+1} = b$, digamos y por lo tanto la igualdad

$$(b) = (a_{k+1}) = (a_k)$$

implica que b y a_k son asociados. Luego c es unidad.

Además, a_k es un factor irreducible de a y por lo tanto se tiene

$$a = a_k e$$

Aplicando el mismo razonamiento al elemento e, se concluye que a es un producto de irreducibles. Además este proceso se termina después de un número finito de pasos, pues si los irreducibles $p_1, p_2, p_3, \ldots, p_n, \ldots$

aparecen en la factorización de a, se tendrá una cadena ascendente de ideales

$$(a) \subseteq (p_2 \dots p_n \dots) \subseteq (p_3 \dots p_n \dots) \subseteq \dots$$

la cual se detiene en algún momento.

Así pues queda probada la primera parte de la definición de Dominio de Factorización Unica.

Para probar la segunda parte, necesitamos algunos resultados previos sobre divisibilidad.

Proposición 8.3.3 *Sea a un elemnto irreducible en un Dominio de Ideales Principales D. Entonces el ideal (a) es maximal.*

Demostración: Sea I un ideal de D y supongamos

$$(a) \subseteq I \subseteq D.$$

El ideal I es un ideal principal y por lo tanto existe un elemento x en D, tal que $I = (x)$.

Luego

$$a \in (a) \subseteq (x),$$

y luego existe un elemento $y \in D$, tal que

$$a = xy$$

Como a es irreducible, se tiene que x o y es unidad. Si x es una unidad, entonces

$$(x) = I = D.$$

Si y es una unidad, se debe tener que a y x son asociados, luego

$$(x) = (a)$$

y por lo tanto

$$I = (a).$$

En conclusión se tiene que (a) es un ideal maximal.

♠

Proposición 8.3.4 *Sea D un Dominio de Ideales Principlales y a un elemento en D tal que $a|bc$, entonces si a es irreducible se tiene que $a|b$ ó $a|c$*

Demostración: De acuerdo a la proposición anterior se tiene que el ideal (a) es maximal y por lo tanto primo. Luego si $a|bc$ implica que $bc \in (a)$, y por lo tanto

$$b \in (a) \quad \text{o} \quad c \in (a)$$

esto es

$$a|b \quad \text{o} \quad a|c$$

♠

Proposición 8.3.5 *(Segunda parte del teorema)*

Sea D un dominio de Ideales Principales y a un elemento en D el cual se factoriza de dos maneras como productos irreducibles

$$a = p_1 \cdots p_s = q_1 \cdots q_t \tag{8.7}$$

entonces $s = t$ y cada p_i es un asociado de algún q_j

Demostración: Comenzamos por considerar el elemento p_1 en el lado izquierdo en (**??**) el cual es irreducible y divide al producto $q_1 \cdots q_t$. Por la proposición anterior se deduce que p_1 divide a alguno de los q_i, digamos $p_1|q_j$, para algún $1 \leq j \leq t$. Luego de acuerdo al ejercicio 6 se

debe tener que p_1 y q_j son asociados, esto es existe una unidad u_1 tal que

$$p_1 = u_1 q_j$$

Podemos entonces cancelar este elemento en (**??**) para tener una expresión

$$p_2 \cdots p_s = u_1 q_1 \cdots q_{i-1} q_{i+1} \cdots q_t \tag{8.8}$$

Continuando de esta manera, podemos cancelar todos los p_i en el lado derecho de (**??**), después de un número finito de pasos, hasta obtener una expresión de la forma

$$1 = u q_{i_1} \cdots q_{i_k} \tag{8.9}$$

con $k = t - s$ y u una unidad.

Como los q_i son irreducibles, no son unidades y por lo tanto en (**??**) se debe tener $k = 0$ o sea $t = s$.

♠

Concluiremos esta sección, dando una propiedad muy importante de los Dominios de Ideales Principales como lo es la existencia de Máximo Común Divisor entre dos elementos.

Definición 8.3.9 *Sea R un anillo y a, b dos elementos en R. Un elemento $d \in R$ se dice* **Máximo Común Divisor** *entre a y b, si*

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

ii) Si c es un elemento de R, tal que

$$c|a \quad y \quad c|b$$

entonces $c|d$.

Usamos la notación $d = (a, b)$ para indicar el Máximo Común Divisor entre a y b.

Teorema 8.3.2 *Sea D un Dominio de Ideales Principales. Entonces el Máximo Común Divisor entre dos elementos a y b cualesquiera siempre existe, además existen elementos x e y en D tales que*

$$(a, b) = ax + by$$

Demostración: Sea I el ideal de D generado por a y b (ver problema 10) esto es

$$I = Da + Db$$

Los elementos de I son de la forma $r_1a + r_2b$ con r_1, r_2 en D. Como D es un Dominio de Ideales Principales, el ideal I es principal y por lo tanto existe un elemento d en D, tal que $I = (d)$.

Afirmamos que d es el Máximo Común Divisor entre a y b. En efecto, como $a \in I$ y $b \in I$, se tiene que $d|a$ y $d|b$.

Por otra parte, $d \in I$ y por lo tanto d es de la forma

$$d = ax + by$$

para algunos x, y en D.

Si c es un elemento en D, tal que

$$c|a \quad \text{y} \quad c|b$$

entonces

$$c|ax + by,$$

y por lo tanto

$$c|d$$

♠

Ejemplo: En el anillo $\mathbb{Z}$, todo par de números enteros a y b posee un Máximo Común Divisor, el cual se puede hallar usando la descomposición en factores primos de ambos elementos.

Por ejemplo si se quiere calcular el Máximo Común Divisor entre 18 y 30, se descomponen ambos números como producto de primos

$$18 = 2 \cdot 3^2$$

$$30 = 2 \cdot 3 \cdot 5$$

Luego $(18, 30) = 2 \cdot 3 = 6$

Definición 8.3.10 *Un elemento p en un anillo R se dice que es* **primo** *si p no es cero ni unidad y cada vez que p divide al producto de dos elementos a y b, entonces p divide a a o p divide a b.*

Ejemplo: En el anillo de los enteros $\mathbb{Z}$, todo elemento primo es irreducible y viceversa. Esto puede ser verificado fácilmente por el lector y lo dejamos como ejercicio.

Proposición 8.3.6 *Sea D un Dominio de Integridad. Entonces todo elemento primo en D es irreducible.*

Demostración: Sea p un elemento primo en D y supongase que existen b y c en D, tales que

$$p = bc \tag{8.10}$$

Luego se tiene $p|bc$ y como p es primo, por hipótesis, p debe dividir a alguno de los dos elementos, digamos $p|b$.

Por lo tanto $b = pe$ para algún e en D, y sustituyendo en (**??**) nos da

$$p = bc = p(ec)$$

luego

$$p(1 - ec) = 0$$

De esto se deduce $1 = ec$, pues D es un Dominio de Integridad y $p \neq 0$, con lo cual c es una unidad.

Igualmente, la suposición $p|c$ nos lleva a concluir que b es unidad. Luego p es irreducible.

Observación: En un Dominio de Factorización Unica, los conceptos de elemento primo y elemento irreducible coinciden (ver problema 12). Pero en general esto no es cierto.

Ejemplo: Un Dominio de Integridad que no es Dominio de Factorización Unica.

Sea R el anillo de números complejos, definido por

$$R = \{a + b\sqrt{-5} | a, b \in \mathbb{Z}\}$$

Para cada elemento

$$x = a + b\sqrt{-5} \quad \text{de} \quad R,$$

se define su **norma** mediante

$$N(x) = (a + b\sqrt{-5})(a - b\sqrt{-5}) = a^2 + 5b^2$$

Se demuestra entonces que la norma así definida satisface las propiedades

i) $N(x) = 0$ si y soló si $x = 0$.

ii) $N(x, y) = N(x)N(y)$, para todo x, y en R.

Se demuestra que R es un dominio de integridad y que las únicas unidades de R son 1 y -1. (Ver problemas 13-16).

En este anillo un elemento puede tener dos factorizaciones distintas como producto de elementos irrreducibles. Por ejemplo

$$6 = 3 \cdot 2 = (1 + \sqrt{-5})(1 - \sqrt{-5}) \tag{8.11}$$

Mostraremos que $3, 2, (1 + \sqrt{-5})$ y $(1 - \sqrt{-5})$ son irreducibles, y además no son asociados entre si. Con esto quedará probado que R no es un Dominio de Factorización Unica.

Comenzaremos por probar que 3 es irreducible. En efecto si $3 = xy$ para algunos x, y en R, se tendrá entonces

$$9 = N(3) = N(x)N(y)$$

Luego los posibles valores para $N(x)$ son $1, 3$ y 9. Si $N(x) = 1$, entonces x es una unidad y estará probado que 3 es irreducible. Si $N(x) = 9$ se demuestra entonces que $N(y) = 1$ y por lo tanto y es una unidad. Entonces también en este caso estaremos probando que 3 es irreducible.

Veamos que la posibilidad $N(x) = 3$ nos lleva a una contradicción.

En efecto, haciendo $x = a + b\sqrt{-5}$, tendremos

$$3 = N(x) = a^2 + b^2 5$$

lo cual no se puede resolver para a y b números enteros.

De la misma forma se demuestra que 2 es irreducible.

Para probar que $1 + \sqrt{-5}$ es irreducible, supongamos nuevamente que $1 + \sqrt{-5} = xy$, para algunos x e y en R. Entonces

$$6 = N(1 + \sqrt{-5}) = N(x)N(y)$$

Luego las posibilidades para $N(x)$ son $1, 2, 3$ y 6. Si $N(x) = 1$ ó 6, entonces x o y es una unidad.

Sea

$$x = a + b\sqrt{-5}$$

luego si

$$N(x) = 2 \quad \text{ó} \quad 3$$

se tiene

$$3 = N(x) = a^2 + 5b^2$$

o bien

$$2 = N(x) = a^2 + 5b^2$$

lo cual es imposible para a y b enteros.

Luego hemos demostrado que $1+\sqrt{-5}$ es irreducible. La demostración de que $1-\sqrt{-5}$ es irreducible sigue los mismos pasos de la demostración anterior.

Finalmente notemos que ninguno de los elementos

$$2, 3, (1+\sqrt{-5}) \ , \ (1-\sqrt{-5}) \tag{8.12}$$

son asociados.

En efecto, los elementos $2, 3$ y $(1+\sqrt{-5})$ tienen normas distintas y por lo tanto no puede haber asociados entre ellos. Sin embargo $(1+\sqrt{-5})$ y $(1-\sqrt{-5})$ poseen la misma norma y debemos tratar este caso aparte. Si existe una unidad u en R tal

$$(1+\sqrt{-5}) = u(1-\sqrt{-5})$$

se tendrá

$$1+\sqrt{-5} = 1-\sqrt{-5} \quad \text{ó} \quad 1+\sqrt{-5} = -1+\sqrt{-5}$$

pues las únicas unidades de R son ± 1. Vemos que hemos llegado a una contradicción. Por lo tanto ninguno de los cuatro elementos dados en (**??**) son asociados entre ellos.

♠

Ejemplo: Un elemento irreducible no primo

Sea R el anillo del ejemplo anterior, en donde hemos probado que 2 es irreducible. Sin embargo probaremos que 2 no es primo.

De acuerdo a la relación (**??**) se tiene que 2 divide al producto $(1+\sqrt{-5})(1-\sqrt{-5})$. Probaremos que 2 no divide a ninguno de los factores, con lo cual se demuestra que 2 no es primo.

Supongase que 2 divida a $(1+\sqrt{-5})$, entonces se tiene

$$2 = x(1+\sqrt{-5})$$

Tomando normas se tiene

$$4 = 6N(x)$$

lo cual es imposible pues $N(x)$ es un entero mayor o igual que 1. De la misma manera se demuestra que 2 no divide a $1 - \sqrt{5}$.

Ejercicios

1) Demuestre que si dos elementos a y b en un dominio D son asociados, entonces $(a) = (b)$ y viceversa.

2) Sea R un anillo y a, b, c elementos en R. Probar que si

$$a|b \quad \text{y} \quad b|c$$

entonces

$$a|c$$

3) Probar que todo número primo en el anillo $\mathbb{Z}$ de los enteros es irreducible.

4) Probar que si I es un ideal de un anillo R, tal que I contiene una unidad, entonces $I = R$.

5) Expresar los números 1521 y 670 como un producto de irreducibles en $\mathbb{Z}$.

6) Probar que si a y b son dos elementos irreducibles tales que $a|b$, entonces a y b son asociados.

7) Probar que si u y v son unidades, entonces uv es una unidad.

8) Demuestre que el conjunto de las unidades forman un grupo bajo la multiplicación.

9) Hallar el conjunto de las unidades del anillo $\mathbb{Z}_{10}$.

10) Sean $x_1, \cdots, x_n$ elementos en un anillo R. Entonces definimos el conjunto

$$(x_1, \cdots, x_n) = \{r_1x_1 + \cdots + r_nx_n \mid r_i \in R\}$$

Probar que este conjunto es un ideal de R, el cual se llama **ideal generado por** $x_1, \cdots, x_n$.

11) Probar que en el anillo $\mathbb{Z}$ de los enteros, todo elemento primo es irreducible.

12) Demuestre que si D es Dominio de Factorización Unica, entonces todo elemento irreducible es primo.

13) Sea $R = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\} \subseteq C$ con las operaciones de suma y multiplicación de números complejos. Probar que R es un anillo conmutativo con unidad.

14) La norma en el anillo R del ejemplo anterior, se define por

$$N(a + b\sqrt{-5}) = (a + b\sqrt{-5})(a - b\sqrt{-5}) = a^2 + 5b^2$$

Probar que esta norma satisface las propiedades

i) $N(x) \geq 0$ para todo $x \in R$
ii) $N(x) = 0$ si y sólo si $x = 0$
iii) $N(xy) = N(x)N(y)$ para todo x, y en R.

15) Probar que el anillo R del problema 13 es un Dominio de Integridad.

16) Probar que las unidades u del anillo R están caracterizadas por la condición $N(u) = 1$. Determine todas las unidades de este anillo.

17) Dos elementos x e y en un anillo R se dicen primos relativos si $(x, y) = 1$. Probar que si x e y son primos relativos, entonces

$$Rx + Ry = R.$$

18) Probar que si p es un número primo y $p \not| a$ entonces $(p, a) = 1$.

19) Demuestre que existen infinitos números primos.

20) Demuestre que existen infinitos primos de la forma $4n + 1$.

21) Probar que la relación de asociados en un anillo R, define una relación de equivalencia.

22) Sean a y b enteros positivos, los cuales se factorizan como producto de primos

$$a = p_1^{\alpha_1} \cdots p_t^{\alpha_t} \qquad \alpha_i \geq 0$$

$$b = p_1^{\beta_1} \cdots p_t^{\beta_t} \qquad \beta_i \geq 0$$

Probar que

$$(a, b) = p_1^{\gamma_1} \cdots p_t^{\gamma_t}$$

donde $\gamma_i = \min\{\alpha_i, \alpha_i\}, \quad 1 \leq i \leq t.$

8.4 Dominios Euclideanos

Definición 8.4.1 *Un Dominio de Integridad D se dice* **Dominio Euclideano**, *si existe una función*

$$d : D\backslash\{0\} \longrightarrow \mathbb{Z}^+$$

tal que

i) Para a y b en D, no nulos, se tiene

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

ii) Para a y b en D, no nulos, existen elementos q y r en D tales que

$$a = qb + r$$

con $r = 0$ o $d(r) < d(b)$.

Ejemplo: El anillo de los enteros $\mathbb{Z}$ con la función $d(x) = |x|$ es un Dominio Euclideano. La propiedad $i)$ es consecuencia inmediata de la definición de valor absoluto para números enteros y la propiedad $ii)$ es precisamente el algoritmo de división para los enteros.

Teorema 8.4.1 *Sea D un Dominio Euclideano. Entonces D es un Dominio de Ideales Principales.*

Demostración: Sea I un ideal de D. Entonces debemos probar que I es un ideal principal.

Si $I = (0)$, entonces es claro que I es principal. Sea $I \neq (0)$. Luego existe un elemento $a \in I$ tal que

$$d(a) = \min\{d(x) | x \in I\} \tag{8.13}$$

Sea $x \in I$. Entonces por ser D un Dominio Euclideano, existen elementos q y r en D tales que

$$x = qa + r \tag{8.14}$$

con $r = 0$ o $d(r) < d(a)$.

Veamos que la condición $d(r) < d(a)$ nos lleva a una contradicción. En efecto, de (**??**) tenemos que $r = x - qa$ y por lo tanto $r \in I$. Luego $d(r) \geq d(a)$, por (**??**), y entonces la posibilidad $d(r) < d(a)$ queda descartada. La única alternativa posible es $r = 0$ en (**??**), lo cual nos da: $x = qa$. Esto es $I \subseteq (a)$.

La otra inclusión es evidente y en consecuencia el ideal I es principal generado por a.

♠

Corolario 8.4.1 *Todo Dominio Euclideano es un Dominio de Factorización Unica.*

Demostración: Consecuencia del Teorema anterior y del teorema **??**.

♠

Si D es un Dominio Euclideano, entonces D tiene una unidad 1 y los elementos unidades están caracterizados de la forma siguiente

Proposición 8.4.1 *Sea u un elemento en un Dominio Euclideano D, entonces u es una unidad si y sólo si $d(u) = d(1)$.*

Demostración: Supongamos que u es una unidad, y sea v en D tal que

$$uv = 1$$

Entonces

$$d(1) = d(uv) \geq d(u) \geq 1$$

Luego $d(u) = 1$

Por otro lado, si $d(u) = 1$, sean q y r tales que

$$1 = uq + r$$

con $r = 0$ o $d(r) < d(u)$.

Como $d(r) \geq 1$, por definición de la función d debemos tener $r = 0$. Luego $uq = 1$ y así vemos que u es una unidad.

♠

En un Dominio Euclideano D, dado cualquier par de elementos a y b, entonces el Máximo Común Divisor entre ellos siempre existe, pues D es un Dominio de Ideales principales. Afortunadamente, en los Dominios Euclideanos se puede calcular el Máximo Común Divisor mediante un algoritmo, llamado método de Euclides, el cual depende de las propiedades de la función d.

Teorema 8.4.2 *(Método de Euclides para calcular el Máximo Común Divisor) Sean a y b dos elementos en un Dominio Euclideano D y consideremos las divisiones sucesivas*

$$\begin{aligned} b &= aq_0 + r_1 \quad , \quad d(r_1) < d(a) \\ a &= r_1 q_1 + r_2 \quad , \quad d(r_2) < d(r_1) \\ r_1 &= r_2 q_2 + r_3 \quad , \quad d(r_2) < d(r_2) \\ &\vdots \\ r_i &= r_{i+1} q_{i+1} + r_{i+2} \quad , \quad d(r_{i+2}) < d(r_{i+1}) \\ &\vdots \end{aligned} \tag{8.15}$$

Entonces existe un $n \geq 0$ *tal que*

$$r_n = r_{n+1} q_{n+1}$$

y además se cumple $r_{n+1} = (a, b)$.

Demostración: La sucesión de elementos $\{r_i\}_{i \geq 1}$ satisface

$$d(r_1) > d(r_2) > \cdots > d(r_I) >$$

Por ser una sucesión de números positivos, la cual es decreciente, debe ser finito y por lo tanto se debe tener, para algún $n \geq 0$

$$r_{n+2} = 0 \quad , \quad r_{n+1} \neq 0$$

Es decir, r_{n+1} es el último resto distinto de cero en (**??**). Afirmamos que r_{n+1} es el Máximo Común Divisor entre a y b.

En primer lugar, se tienen las relaciones

$$\begin{aligned} r_n &= r_{n+1} q_{n+1} \\ r_{n-1} &= r_n q_n + r_{n+1} \\ &\vdots \\ r_1 &= r_2 q_2 + r_3 \\ a &= r_1 q_1 + r_2 \\ b &= aq_0 + r_1 \end{aligned} \tag{8.16}$$

De la ecuación (**??**) se deduce que $r_{n+1}|r_n$

Luego $r_{n+1}|r_nq_n+r_{n+1}$ y por lo tanto $r_{n+1}|r_{n-1}$. Continuando de esta manera, se llega a demostrar que r_{n+1} divide a todos los r_i restantes, $1 \leq i \leq n$. Luego $r_{n+1}|r_1q_1 + r_2$ y por lo tanto $r_{n+1}|a$. También $r_{n+1}|aq_0 + r_1$, lo cual implica que $r_{n+1}|b$.

Finalmente, sea c un elemento de D, tal que $c|a$ y $c|b$. Entonces usando (**??**), tendremos

$$c|b - aq_0$$

y por lo tanto $c|r_1$.

Continuando este proceso en el sistema de ecuaciones en (**??**), se llega a demostrar que $c|r_i$ para todo $1 \leq i \leq n$ y por lo tanto $c|r_{n+1}$.

Luego r_{n+1} satisface las dos condiciones de Máximo Común Divisor entre a y b.

♠

Este algoritmo se puede utilizar para hallar el Máximo Común Divisor entre dos números a y b.

Ejemplo 1: Hallar $(345, 20)$

Tenemos entonces

$$\begin{aligned} 345 &= 20 \times 17 + 5 \\ 20 &= 5 \cdot 4 \end{aligned}$$

luego $(345, 20) = 5$

Cerramos esta sección con el estudio de un Dominio Euclideano muy especial, el cual fue descubierto por el matemático alemán Carl Friedrich Gauss $(1777 - 1855)$, en relación al problema de determinar que números enteros positivos se pueden expresar como suma de dos cuadrados.

Ejemplo 2: (Enteros de Gauss) Sea A el conjunto de números complejos de la forma

$$A = \{x + iy \mid x, y \in \mathbb{Z}\}$$

Dejaremos como ejercicio para el lector, el probar que A es un Dominio de Integridad. Probaremos que A es un Dominio Euclideano con la función

$$d(x + iy) = x^2 + y^2 \tag{8.17}$$

para todo $x + iy \in A$.

Notemos en primer lugar que la función

$$d : A \longrightarrow \mathbb{Z}^+$$

está bien definida, pues si $x+yi \in A$, entonces x e y son números enteros y por lo tanto $d(x + iy)$ es un entero positivo. Además si $a = x + iy$ entonces

$$d(a) = (x + iy)(x - iy) = a\overline{a}$$

donde $\overline{a}$ denota el conjugado de a.

Luego d tiene la propiedad de una norma

$$d(ab) = d(a)d(b)$$

En efecto:

$$\begin{aligned} d(ab) &= (ab)\overline{(ab)} \\ &= (ab)(\overline{a}\overline{b}) \\ &= d(a)d(b) \end{aligned}$$

Por lo tanto la función d satisface la propiedad $i)$ de la definición de un Dominio Euclideano:

$$d(ab) \geq d(a)$$

para todos a y b en A con $a \neq 0$ y $b \neq 0$.

Probaremos que A satisface la condición $ii)$ de la definición.

Sean a y b en A con $a \neq 0$. Entonces se tiene el número complejo $\frac{a}{b} = \alpha + \beta i$, donde $\alpha, \beta \in \mathcal{Q}$. Luego existen enteros x e y tales que

$$|x - \alpha| \leq \frac{1}{2} \quad \text{y} \quad |\beta - y| \leq \frac{1}{2}$$

Si tomamos $q = x + iy$, se tiene que

$$a = qb + (a - qb) \tag{8.18}$$

y además se cumple

$$d\left(\frac{a}{b} - q\right) = (\alpha - x)^2 + (\beta - y)^2 < \frac{1}{2}$$

Luego hacemos $r = a - qb$ y $r = 0$, o bien

$$\begin{aligned} d(r) &= d(a - qb) \\ &= d(b)d\left(\frac{a}{b} - q\right) \\ &\leq \frac{1}{2}d(b) < d(b) \end{aligned}$$

En conclusión, hemos demostrado que A es un Dominio Euclideano.

Ejercicios

1) Mostrar que todo cuerpo F es un Dominio Euclideano.

2) Sea D un Dominio Euclideano. Mostrar que para cada par de elementos a y b, los elementos q y r en la definición, no son necesariamente únicos. Usar un contraejemplo.

3) Probar que todo elemento a en un Dominio Euclideano satisface

$$d(1) \leq d(a)$$

4) Probar que para todo x en un Dominio Euclideano se tiene

$$d(x) = d(-x)$$

5) Probar que si a y b no son unidades de un Dominio Euclideano D, entonces

$$d(a) < d(ab)$$

6) Usando el método de Euclides, calcular
   a) $(1560, 68)$
   b) $(752, 541)$
   c) $(1110, 720)$
   d) $(212, 2703)$

7) Expresar el Máximo Común Divisor entre a y b como una combinación $d = ax + by$ para los siguientes pares de enteros

   a) $(120, 45)$
   b) $(615, 814)$
   c) $(1714, 48)$
   d) $(248, 623)$

8) Probar que el conjunto A de los Enteros de Gauss definido por

$$A = \{x + iy \mid x, y \in \mathbb{Z}\}$$

es un Dominio de Integridad.

9) Sea $x = 3 + 2i$ e $y = -1 + 4i$ en A. Hallar

   a) $x + y$
   b) xy
   c) x/y
   d) $d(x)$,$d(y)$

e) $d(xy)$

10) Hallar todas las unidades en el anillo A de los Enteros de Gauss.

11) Probar que si x es un número racional, entonces existe un entero z tal que $|x - z| \leq \frac{1}{2}$.

12) Hallar el cociente y el resto de la división de $a = 10 + 2i$ entre $b = 2 - i$.

13) Probar que si a y b son elementos de un Dominio Euclideano D, tales que $d(a) = d(b)$, entonces se tiene $(a) = (b)$.

14) Demuestre que 2 no es un elemento irreducible en los Enteros de Gauss.

Capítulo

9

Anillo de Polinomios

9.1 Introducción

Hemos dejado el estudio de los polinomios para el final, pues este ejemplo nos permitirá repasar todas las definiciones y propiedades de anillos, estudiadas en capítulos anteriores. Realmente los polinomios es uno de los ejemplos de anillos, más estudiados desde la antigüedad por estar estrechamente relacionado con la solución de ecuaciones en una o varias incógnitas.

Muchas de las propiedades básicas de los polinomios como lo son las operaciones de suma, producto y división, el cálculo de raíces y la factorización, ya las hemos estudiado en la escuela secundaria, de un modo operacional.

En este capítulo, los polinomios serán estudiados desde el punto de vista de su estructura de anillo. Este nuevo enfoque aclarará muchos de los conceptos ya estudiados en cursos anteriores al, considerarlos dentro de propiedades más generales de anillos, y al mismo tiempo abrirá nuevos caminos que nos conduciran a resultados bastante vigorosos, resando las técnicas desarrolladas en el Capítulo 6.

Definición 9.1.1 *Sea A un anillo. Un* **polinomio** *en la indeterminada x es una suma formal*

$$f(x) = \sum_{i=1}^{\infty} a_i x^i$$

donde $a_i \in A$, para todo $i \geq 0$, y $a_i = 0$ para todo i, excepto para un número finito de ellos.

Observación: Podemos dar otra definición de lo que es un polinomio, sin hacer referencia a la variable x.

Definición 9.1.2 *Sea A un anillo. Un* **polinomio** *sobre A es una sucesión infinita $(a_0, a_1, \ldots, a_n, \ldots)$ donde $a_i \in A$; para todo i y $a_i = 0$ para casi todos los i.*

Una sucesión $(a_0, a_1, \ldots, a_n, \ldots)$ donde casi todos los a_i son iguales a cero, se denomina una **sucesión casi nula**.

La definición (**??**) es más formal que la definición (**??**) pues no hace uso de la variable x. Sin embargo el símbolo x se ha utilizado para expresar los polinomios desde hace mucho tiempo y aún se usa en la actualidad. Para mantenernos en esta tradición usaremos la definición (**??**) de polinomios. Si hacemos $x = (0, 1, 0, 0, \ldots)$, y entonces la variable x es un polinomio en si misma, y deja de ser un objeto misterioso. Nosotros seguiremos denotando los polinomios a la manera clásica

$$f(x) = a_n x^n + \cdots + a_1 x + a_0$$

donde se sobre entiende que $a_i = 0$ para $i > n$.

El conjunto de los polinomios sobre el anillo A, será denotado por $A[x]$.

Definición 9.1.3 *Sea $f(x) = a_n x^n + \cdots + a_1 x + a_0$ un polinomio en $A[x]$. Entonces los a_i se llaman los* **coeficientes** *del polinomio.*

Definición 9.1.4 *El polinomio que tiene todos sus coeficientes iguales a 0, se llama* **polinomio nulo o polinomio cero** *y se denota por 0.*

Definición 9.1.5 *El polinomio que tiene todos sus coeficientes a_i iguales a cero, para $i \geq 1$ se llama* **polinomio constante**.

Definición 9.1.6 *Dados dos polinomios $f(x) = a_n x^n + \cdots + a_1 x + a_0$ y $g(x) = b_m x^m + \cdots + b_1 x + b_0$, diremos que son iguales y lo denotamos por $f(x) = g(x)$, si y sólo si*

$$a_i = b_i \qquad \forall i \geq 0$$

En el conjunto de polinomios $A[x]$ se pueden definir un par de operaciones

Suma de Polinomios

$$(a_n x^n + \cdots + a_1 x + a_0) + (b_m x^m + \cdots + b_1 x + b_0)$$

$$= \quad C_k x^k + \cdots + C_1 x + C_0 \tag{9.1}$$

donde $C_i = a_i + b_i, \quad a \leq i \leq k$

Producto de Polinomios

$$(a_n x^n + \cdots + a_1 x + a_0)(b_m x^m + \cdots + b_1 x + b_0)$$

$$= \quad C_k x^k + \cdots + C_1 x + C_0 \tag{9.2}$$

donde $C_s = \sum_{i+j=s} a_i b_j$, para todo $0 \leq s \leq k$.

Ejemplo: Sean $f(x) = 2x^2 + 3x - 1$ y $g(x) = x^3 + 1$ dos polinomios en $\mathbb{Z}[x]$. Entonces para poder sumar f y g es necesario introducir coeficientes nulos en ambos polinomios, de la manera siguiente

$$\begin{aligned} f(x) &= 0x^3 + 2x^2 + 3x - 1 \\ &= a_3 x^3 + a_2 x^2 + a_1 x + a_0 \\ g(x) &= x^3 + 0x^2 + 0x + 1 \\ &= b_3 x^3 + b_2 x^2 + b_1 x + b_0 \end{aligned}$$

luego sumamos los polinomios, de acuerdo a la definición, es decir, sumamos los coeficiente de potencias de x iguales

$$\begin{aligned} f(x) + g(x) &= (0+1)x^3 + (2+0)x^2 + (3+0)x + (1-1) \\ &= x^3 + 2x^2 + 3x \end{aligned}$$

Para multiplicar los polinomios, construimos los elementos C_i en la expresión (**??**). Luego

$$\begin{aligned} C_0 &= a_0b_0 \\ &= (-1)(1) \\ &= -1 \end{aligned}$$

$$\begin{aligned} C_1 &= a_0b_1 + a_1b_0 \\ &= (-1)0 + 3(1) \\ &= 3 \end{aligned}$$

$$\begin{aligned} C_2 &= a_0b_2 + a_1b_1 + a_2b_0 \\ &= (-1)(0) + 3(0) + (2)(1) \\ &= 2 \end{aligned}$$

$$\begin{aligned} C_3 &= a_0b_3 + a_1b_2 + a_2b_1 + a_3b_0 \\ &= (-1)(1) + 3(0) + 2(0) + (0)1 \\ &= -1 \end{aligned}$$

$$\begin{aligned} C_4 &= a_1b_3 + a_2b_2 + a_3b_1 \\ &= 3(1) + (2)(0) + (0)(0) \\ &= 3 \end{aligned}$$

$$\begin{aligned} C_5 &= a_2b_3 + a_3b_2 \\ &= 2(1) + (0)(0) \\ &= 2 \end{aligned}$$

$$\begin{aligned} C_6 &= a_3b_3 \\ &= (0)(1) \\ &= 0 \end{aligned}$$

Luego el resultado de multiplicar $f(x)$ y $g(x)$ viene expresado por

$$f(x)g(x) = 2x^5 + 3x^4 - x^3 + 2x^2 + 3x + 1$$

Observación: Se recomienda al estudiante hacer la multiplicación por el método tradicional, y luego comparar ambos resultados.

A continuación definimos una función que asocia a cada polinomio no nulo $f(x)$ un entero no negativo.

Definición 9.1.7 *Sea $f(x) = a_s x^s + \cdots + a_1 x + a_0$ en $A[x]$, no nulo. Entonces el* **grado de** $f(x)$*, denotado por $g(f(x))$, es el mayor entero no negativo n, tal que $a_n \neq 0$.*

Observación 1: Si el grado de $f(x)$ es n, entonces $a_k = 0$, para todo $k > n$ y escribimos

$$f(x) = a_n x^n + \cdots + a_1 x + a_0,$$

es decir, no se colocan aquellos términos $a_x x^i$ con $i > n$, pues son todos nulos.

El término a_n se llama **coeficiente principal de** $f(x)$.

Definición 9.1.8 *Un polinomio de la forma $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ se llama* **mónico**.

Observación 2: Si $f(x)$ es un polinomio constante no nulo, entonces $g(f(x)) = 0$.

Observación 3: El grado del polinomio 0 lo definimos mediante el símbolo especial $-\infty$, de acuerdo a las siguientes reglas

i) $-\infty < n$, para todo $n \in \mathbb{Z}$

ii) $-\infty + (-\infty) = -\infty$

iii) $-\infty + n = -\infty$, para todo $n \in \mathbb{Z}$

Proposición 9.1.1 *Sea A un Dominio de Integridad. Sean $f(x)$ y $h(x)$ dos polinomios no nulos en $A[x]$, de grados n y m respectivamente. Entonces*

i) $g(f(x)+h(x)) \leq \max\{n,m\}$

ii) $g(f(x)h(x)) = n+m$

Demostración: i) Supongamos que $n > m$. Entonces el coeficiente principal de $f(x)+h(x)$ es igual al coeficiente principal de $f(x)$ y por lo tanto

$$g(f(x)+h(x)) = g(f(x)) = n = \max\{n,m\}$$

Si suponemos que $n = m$, entonces pueden ocurrir dos casos

I) La suma de los coeficientes principales de f y h es cero. Luego $g(f(x)+h(x)) < n$.

II) La suma de los coeficientes principales de f y h es distinta de cero. En este caso $g(f(x)+h(x)) = n$.

Luego en cualquiera de los dos casos obtenemos la desigualdad deseada.

ii) Para calcular el grado del producto, sean

$$f(x) = a_n x^n + \cdots + a_1 x + a_0$$

y

$$h(x) = b_m x^m + \cdots + b_1 x + b_0$$

entonces hacemos la multiplicación.

$$f(x)h(x) = C_s x^s + \cdots + C_1 x + C_0$$

Afirmamos que $C_{n+m} \neq 0$. En efecto, se tiene $C_{n+m} = a_n b_m \neq 0$, pues tanto a_n como b_m son no nulos. Por otra parte si $s > n+m$ se tiene

$$C_s = \sum_{i+j=s} a_i b_j$$

Luego cada término $a_i b_j$ en dicha suma es igual a cero, pues se debe tener $i > n$ ó bien $j > m$, lo cual implica $a_i = 0$ ó bien $b_j = 0$.

Por lo tanto $C_s = 0$ para $s > n + m$, y así hemos probado que el grado de $f(x)g(x)$ es $m + n$.

♠

Teorema 9.1.1 *El conjunto $A[x]$ de polinomios sobre un anillo A, es un anillo con las operaciones de suma y producto de polinomios. Si A es un anillo conmutativo con unidad, entonces $A[x]$ es un anillo conmutativo con unidad.*

Demostración: Es claro que $A[x]$ es un grupo abeliano con la suma de polinomios. El elemento neutro para la suma es el polinomio nulo. Si $p(x) = a_n x^n + \cdots a_1 x + a_0$, entonces el opuesto de $p(x)$ es

$$-p(x) = (-a_n)x^n + \cdots + (-a_1)x - a_0.$$

Con respecto al producto, se demuestra que esta operación es asociativa y satisface las leyes distributivas.

Además, si A es conmutativo sean $f(x)$ y $h(x)$ dos polinomios en $A[x]$, luego

$$f(x) = a_n x^n + \cdots + a_1 x + a_0$$

y

$$h(x) = b_m x^m + \cdots + b_1 x + b_0$$

Entonces se tiene

$$\begin{aligned} f(x)h(x) &= C_s x^s + \cdots + C_1 x + C_0 \\ h(x)f(x) &= d_s x^s + \cdots + d_1 x + d_0 \end{aligned}$$

con $s = m + n$.

Pero todo $0 \leq i \leq s$, obtenemos

$$\begin{aligned} C_i &= \sum_{k+j=i} a_k b_j \\ &= \sum_{j+k=i} b_j a_k \\ &= d_i \end{aligned}$$

Luego $f(x)h(x) = h(x)f(x)$ por tener todos sus coeficientes iguales.

Si A tiene unidad 1, entonces el polinomio constante $f(x) = 1$ es el polinomio unidad para el producto.

♠

Proposición 9.1.2 *Si el anillo A es un Dominio de Integridad, entonces el anillo $A[x]$ es un Dominio de Integridad.*

Demostración: Es claro que $A[x]$ es un anillo conmutativo con unidad, de acuerdo al teorema anterior.

Por otro lado, sean $f(x)$ y $h(x)$ son dos polinomios en $A[x]$, tal que $f(x)h(x) = 0$.

Si $f(x) \neq 0$ y $h(x) \neq 0$ se tiene entonces

$$\begin{aligned} g(f(x)) &\leq g(f(x)h(x)) \\ &= g(0) \\ &= -\infty \end{aligned}$$

de donde

$$g(f(x)) = -\infty$$

y por lo tanto $f(x) = 0$, lo cual es una contradicción. Luego $f(x) = 0$ ó $h(x) = 0$.

♠

Observación: Sabemos que todo Dominio de Integridad posee un cuerpo de cocientes. Por lo tanto $A[x]$ tiene su cuerpo de cocientes, el cual se llama **cuerpo de funciones racionales en** x y sus elementos son cocientes de polinomios en $A[x]$.

9.2 El Algoritmo de División

En esta sección consideramos el anillo de polinomios sobre un cuerpo K, el cual será denotado por $K[x]$. Probaremos que este anillo tienen la propiedad de ser euclideano y por lo tanto valen todas las propiedades de los Dominios Euclideanos descritas en el capítulo 6.

Proposición 9.2.1 *Sean $f(x)$ y $h(x)$ polinomios no nulos en $K[x]$. Entonces $g(f(x)) \leq g(f(x)h(x))$.*

Demostración: De acuerdo a la proposición (**??**) se tiene

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

luego

$$g(f(x)) \leq g(f(x)h(x)).$$

♠

Teorema 9.2.1 *(Algoritmo de División) Sean $f(x)$ y $h(x)$ dos polinomios en $K[x]$, con $h(x) \neq 0$. Luego existen polinomios $q(x)$ y $r(x)$ en $K[x]$, tales que*

$$f(x) = h(x)q(x) + r(x)$$

con

$$r(x) = 0 \quad ó \quad g(r(x) < g(h(x))$$

Demostración: Si $f(x) = 0$, tomamos entonces $q(x) = 0$ y $r(x) = 0$.

Si $g(f(x)) < g(h(x))$, tomamos $q(x) = 0$ y $r(x) = f(x)$.

Supongamos entonces que $g(f(x)) \geq g(h(x))$ y pongamos

$$f(x) = a_n x^n + \cdots + a_1 x + a_0$$

y

$$g(x) = b_m x^m + \cdots + b_1 x + b_0$$

con $n \geq m$.

Podemos entonces usar inducción sobre n para obtener el resultado. Si $n = 0$, entonces

$$f(x) = a_0, \quad h(x) = b_0 \quad \text{y}$$

$$f(x) = a_0 b_0^{-1} h(x) + 0$$

luego tomando $q(x) = a_0 b_0^{-1}$ y $r(x) = 0$ se obtiene el resultado.

Supóngase que el teorema es cierto para todo polinomio de grado k, con $k < n$. Luego

$$f(x) - a_n b_m^{-1} x^{n-m} h(x)$$

es un polinomio de grado menor que n y por la hipótesis de inducción existen $q'(x)$ y $r'(x)$ tales que

$$f(x) - a_n b_m^{-1} x^{n-m} h(x) = h(x) q'(x) + r'(x)$$

con $r'(x) = 0$ ó $g(r'(x)) < g(h(x))$

Por lo tanto, tenemos

$$f(x) = h(x) \left[q'(x) + a_n b_m^{-1} x^{n-m} \right] + r'(x)$$

Si tomamos $q(x) = q'(x) + a_n b^{-1} m x^{n-m}$ y $r(x) = r'(x)$ se tiene el resultado deseado

♠

Observación: Los polinomios $q(x)$ y $r(x)$ se llaman respectivamente **cociente** y **resto** de la división de $f(x)$ entre $h(x)$.

Si definimos la función $d : K[x] \longrightarrow \mathbb{Z}^+$ por $d(f(x)) = g(f(x))$, entonces se tiene

Corolario 9.2.1 *El anillo de polinomios $K[x]$ es un* **Dominio de Euclideano**.

Definición 9.2.1 *Sea K un cuerpo y $f(x)$, $h(x)$ en $K[x]$. Diremos que el polinomio $f(x)$ es divisible entre $h(x)$, si existe otro polinomio $c(x)$ en $K[x]$, tal que*

$$f(x) = h(x)c(x)$$

Definición 9.2.2 *Sea $f(x)$ un polinomio en $K[x]$. Diremos que $f(x)$ es un* **polinomio irreducible** *en $K[x]$, o irreducible sobre K, si cada vez que*

$$f(x) = h(x)q(x),$$

entonces $h(x)$ o $q(x)$ es una constante.

Observación: Como consecuencia directa del corolario anterior se tiene que $K[x]$ es un Dominio de Ideales Principales y por lo tanto un Dominio de Factorización Unica. Luego se tienen los hechos siguientes

Teorema 9.2.2 *Sea $f(x)$ un polinomio en $K[x]$. Entonces existen polinomios irreducibles $p_1(x), \cdots, p_s(x)$, los cuales son únicos salvo asociados, tales que*

$$f(x) = p_1(x) \cdots p_s(x).$$

Teorema 9.2.3 *Si $f(x)$ y $h(x)$ son polinomios en $K[x]$, entonces el Máximo Común Divisor entre $f(x)$ y $h(x)$, el cual denotamos por $d(x)$, siempre existe. Además se tiene*

$$d(x) = p(x)f(x) + q(x)h(x),$$

para algunos polinomios $p(x)$ y $q(x)$ en $K[x]$.

A fin de tener una mejor información sobre el anillo de polinomios $K[x]$, el paso siguiente será determinar todas las unidades en $K[x]$ y los elementos irreducibles.

Para hallar las unidades usaremos un resultado que hemos probado sobre los Dominios Euclideanos, el cual establece:

"El polinomio $u(x)$ es una unidad, si y sólo si el grado de $u(x)$ es igual al grado del polinomio 1". Luego las unidades de $K[x]$ son precisamente los polinomios constantes (distintos de cero), pues grado(1)=0.

El problema de determinar cuando un polinomio es irreducible, es uno de los más difíciles en Algebra y ha sido estudiado desde hace varios siglos. No se tiene un criterio general para decidir la condición de irreducibilidad. Sólo existen criterios que se pueden aplicar en situaciones especiales, como se verá más adelante.

Veamos mediante un ejemplo como se puede determinar si un polinomio es irreducible, usando las técnicas de la teoría de Anillos.

Ejemplo: Probar que $f(x) = x^2 + 1$ es irreducible en $\mathcal{Q}[x]$.

Solución: Sea $I = (x^2 + 1)$ el ideal principal generado por el elemento $f(x)$ en $\mathcal{Q}[x]$. Consideremos el anillo cociente $\mathcal{Q}[x]/I$.

Sea $f(x)$ un polinomio en $\mathcal{Q}[x]$, entonces por el algoritmo de división, existen polinomios $q(x)$ y $r(x)$ tales que

$$f(x) = q(x)(x^2 + 1) + r(x)$$

con $r(x) = 0$ ó $g(r(x)) < g(x^2 + 1)$.

Luego el polinomio $f(x)$ se puede reducir módulo I a un polinomio $r(x)$ de grado 1. Por lo tanto los elementos de $\mathcal{Q}[x]/I$ son polinomios lineales $ax + b$, con a y b en $\mathcal{Q}$. Además de la relación $x^2 + 1 = 0$, se sigue $x^2 = -1$.

Afirmamos que $\mathcal{Q}[x]/I$ es un cuerpo, para lo cual sea $t = ax + b \in \mathcal{Q}[x]/I$ y probaremos que si t es distinto de cero, entonces es invertible. En efecto, $t \neq 0$ implica que $a^2 + b^2 \neq 0$. Además

$$\begin{aligned}(ax+b)(-ax+b) &= -a^2x^2+b^2\\ &= a^2+b^2\end{aligned}$$

Luego hacemos $S=\lambda x+r$ con

$$\lambda=\frac{-a}{a^2+b^2} \quad \text{y} \quad r=\frac{b}{a^2+b^2}$$

Es claro que $S\in\mathcal{Q}[x]/I$, y además $ts=1$. Luego t es invertible.

Una vez demostrado que $\mathcal{Q}[x]/I$ es un cuerpo, se deduce que el ideal I es maximal y por lo tanto ideal primo. Luego el elemento x^2+1 es irreducible en $\mathcal{Q}[x]$.

Ejercicios

1) Sean $f(x)=3x^4+2x^3-5x^2+1$ y $h(x)=4x^2+10x-3$. Calcule $f(x)+g(x)$ y $f(x)h(x)$.

2) Mostrar que si $f(x), h(x)$ y $g(x)$ son polinomios en $\mathbb{Z}[x]$ entonces

i) $(f(x)+h(x))+g(x)=f(x)+(h(x)+g(x))$
ii) $[f(x)+h(x)]\,g(x)=f(x)g(x)+h(x)g(x)$

3) Si $f(x)=a_nx^n+\cdots+a_1x+a_0$, hallar los coeficientes del polinomio $f(x)(x-1)$.

4) Sea $f(x)=6x^3+3x^2-2$ y $h(x)=2x^2-6$ dos polinomios en $\mathbb{Z}_7[x]$. Hallar:

a) $f(x)+h(x)$
b) $f(x)h(x)$

5) Hallar el cociente y el resto de la división de los siguientes polinomios en $\mathcal{Q}[x]$.

a) $f(x)=10x^8-2x^2+6, \quad h(x)=x^2+2$
b) $f(x)=5x^6-3x^3+18x-1, \quad h(x)=2x^4+15x-3$
c) $f(x)=16x^7+8x^4+5x^3-6x^2, \quad h(x)=3x^4-8x^3$
d) $f(x)=x^5+x^4+x^3+x^2+x+1, \quad h(x)=x-1$

6) Hallar el Máximo Común Divisor entre $x^6 - 4x^3 + 1$ y $3x^2 + 5x - 1$ en $\mathcal{Q}[x]$.

7) Demuestre que $p(x) = x^2 - 2$ es irreducible sobre $\mathcal{Q}[x]$.

8) Sea $p(x) = 1 + x + x^2 + \cdots + x^{n-1}$ en $\mathcal{Q}[x]$. Probar que $x^n - 1 = p(x)(x - 1)$.

9) Sea $\phi : A \longrightarrow A'$ un homomorfismo de anillos. Probar que existe un homomorfismo de anillos entre $A[x]$ y $A'[x]$.

10) Demuestre que todo **polinomio lineal** $f(x) = ax + b$ en $K[x]$ es irreducible.

11) Usando las notaciones del problema 9, probar que si $f(x)$ es reducible en $A[x]$, entonces su imágen es reducible en $A'[x]$.

12) ¿Cuántos polinomios de grado 3 se pueden construir en $\mathbb{Z}_5$? Generalize este resultado para cualquier grado.

9.3 Raíces de Polinomios

A lo largo de esta sección veremos la relación existente entre un polinomio $f(x)$ y la resolución de la ecuación

$$f(x) = 0$$

Definición 9.3.1 *Sea K un cuerpo. Una* **extensión** F **de** K *es un cuerpo que contiene a K como subcuerpo. Es decir K es un cuerpo con las mismas operaciones definidas en F.*

Ejemplo: Los números complejos $\mathbb{C}$ son una extensión del cuerpo de los números reales $\mathbb{R}$.

Observación: Si F es una extensión de K y $f(x)$ es un polinomio en $K[x]$, entonces los coeficientes de $f(x)$ están todos en K y por lo tanto en F, luego $f(x)$ está en el anillo $F[x]$.

Definición 9.3.2 *Sea K un cuerpo, F una extensión de K y*

$$f(x) = a_n x^n + \cdots + a_1 x + a_0$$

un polinomio en $K[x]$. Entonces si $\lambda \in F$, **el valor del polinomio** *$f(x)$ en el elemento λ, denotado por $f(\lambda)$ es el elemento de F dado por*

$$f(b) = a_n \lambda^n + \cdots + a_1 \lambda + a_0$$

Proposición 9.3.1 *Sea K un cuerpo F una extensión de K, y $\lambda \in F$. Entonces la función*

$$\begin{array}{rcl} \phi_\lambda : K[x] & \longrightarrow & F \\ f(x) & \longrightarrow & f(\lambda) \end{array}$$

es un homomorfismo de anillos.

La imágen de $f(x)$ bajo ϕ_λ se llama **la sustitución** de x por λ, o la **evaluación de $f(x)$ en λ**.

Demostración: Sean $f(x)$ y $h(x)$ dos polinomios en $K[x]$, entonces

$$f(x) = a_n x^n + \cdots + a_1 x + a_0$$

y

$$h(x) = b_m x^m + \cdots + b_1 x + b_0$$

luego

$$f(x) + h(x) = C_s x^s + \cdots + C_1 x + C_0$$

donde $C_i = a_i + b_i$, $0 \leq i \leq s$, $s \leq \max\{n, m\}$

Por lo tanto

$$\phi_\lambda(f(x) + h(x)) = C_s \lambda^s + \cdots + C_1 \lambda + C_0$$

y por otra parte

$$\begin{aligned}\phi_\lambda(f(x)) + \phi_\lambda(h(x)) &= (a_s\lambda^s + \cdots + a_1\lambda + a_0) + (b_s\lambda^s + \cdots + b_1\lambda + b_0) \\ &= (a_s + b_s)\lambda^s + \cdots + (a_1 + b_1)\lambda + (a_0 + b_0)\end{aligned}$$

de donde concluimos que

$$\phi_\lambda(f(x) + h(x)) = \phi_\lambda(f(x)) + \phi_\lambda(h(x))$$

Con respecto al producto, hagamos

$$f(x)h(x) = d_t x^t + \cdots + d_1 x + d_0,$$

donde $t = m + n$ y

$$d_i = \sum_{k+j=i} a_k b_j \quad , \quad 0 \leq i \leq t$$

Luego

$$\phi_\lambda(f(x)h(x)) = d_t\lambda^t + \cdots + d_1\lambda + d_0 \tag{9.3}$$

y por otro lado

$$\begin{aligned}\phi_\lambda(f(x))\phi_\lambda(h(x)) &= (a_n\lambda^n + \cdots + a_1\lambda + a_0)(b_m\lambda^m + \cdots + b_1\lambda + b_0) \\ &= e_t\lambda^t + \cdots + e_1\lambda + e_0 \qquad (9.4)\end{aligned}$$

con $t = n + m$ y

$$e_i = \sum_{k+j=i} a_k b_j \quad , \quad 0 \leq i \leq t$$

Comparando las expresiones (**??**) y (**??**), vemos que ellas son iguales y por lo tanto

$$\phi_\lambda(f(x)h(x)) = \phi_\lambda(f(x))\phi_\lambda(h(x))$$

Luego ϕ_λ es un homomorfismo de anillos.

♠

Definición 9.3.3 *Una* **raíz** *o un* **cero de un polinomio** $f(x) \in K[x]$ *es un elemento* λ *en una extensión* F *de* K*, tal que* $f(\lambda) = 0$*.*

También diremos que el valor de λ **anula** al polinomio, o que λ es una **solución de la ecuación** $f(x) = 0$

Ejemplo 1: Los valores 1 y -1 anulan al polinomio $f(x) = x^4 - 1$ en $\mathcal{Q}[x]$, pues $f(1) = 1^4 - 1 = 0 \quad$ y $\quad f(-1) = (-1)^4 - 1 = 0$.

Ejemplo 2: Sea $f(x) = x^2 + 1$ en $\mathcal{Q}[x]$. Entonces $i = \sqrt{-1}$ es una raíz de $f(x)$, pues $f(i) = i^2 + 1 = 0$. Nótese que i esta en $\mathbb{C}$ pero no en $\mathcal{Q}$.

Teorema 9.3.1 *Sea* $f(x)$ *un polinomio en* $K[x]$*,* F *una extensión de* K *y* $\lambda \in F$ *una raíz de* $f(x)$*. Entonces* $f(x)$ *se factoriza en* $F[x]$

$$f(x) = (x - \lambda)q(x)$$

donde $q(x)$ *es un polinomio de grado igual al grado de* $f(x)$ *menos uno.*

Demostración: Haciendo la división de $f(x)$ entre el polinomio $x - \lambda$ se generan polinomios $q(x)$ y $r(x)$ tales que

$$f(x) = (x - \lambda)q(x) + r(x) \tag{9.5}$$

con $r(x) = 0 \quad$ ó $\quad g(r(x)) < g(x - \lambda) = 1$

Luego el grado de $r(x)$ debe ser cero y por lo tanto es un polinomio constante $r(x) = \sigma$; con $\sigma \in K$.

Haciendo la evaluación de los polinomios en (**??**) en el valor λ, tenemos

$$\begin{aligned} 0 &= f(\lambda) \\ &= (\lambda - \lambda)q(\lambda) + \sigma \\ &= \sigma \end{aligned}$$

de donde $\sigma = 0$ y por lo tanto en (**??**) se tiene

$$f(x) = (x - \lambda)q(x)$$

♠

Un polinomio del tipo $ax + b$ se llama **polinomio lineal**. Es claro que todo polinomio lineal es irreducible, pues si $ax + b = p(x)q(x)$, entonces la suma de los grados de ellos debe ser 1. Por lo tanto $p(x)$ o $q(x)$ es de grado cero y por ende constante.

Definición 9.3.4 *Sea $f(x)$ un polinomio en $K[x]$. Diremos que $f(x)$ se* **factoriza completamente** *en una extensión F de K, si existen raíces $\lambda_1, \ldots, \lambda_t$ en F tal que*

$$f(x) = a_n(x - \lambda_1)(x - \lambda_2)\cdots(x - \lambda_t)$$

donde $a_n \in K$.

Observación: Una de las metas más importantes en la teoría de los polinomios es poder factorizar cualquier polinomio como un producto de factores lineales. Lamentablemente esto no es posible en cualquier cuerpo K, pues, por ejemplo $f(x) = x^2 + 1$ no se puede factorizar en $\mathcal{Q}[x]$ como producto de factores lineales.

Sin embargo siempre se puede hallar una extensión del cuerpo K en donde este problema se resuelve.

Definición 9.3.5 *Una raíz λ de $f(x)$ se dice que tiene* **multiplicidad K**, *si $f(x) = (x - \lambda)^k q(x)$ y λ no es raíz de $q(x)$.*

Cuando contamos las raíces de un polinomio, aquellas que aparecen repetidas se cuentan tantas veces como sea su multiplicidad. Así, por ejemplo el polinomio $f(x) = x^3 - x^2$ tiene 3 raíces que son 0, con multiplicidad 2, y 1.

Teorema 9.3.2 *Sea $f(x)$ un polinomio en $K[x]$ de grado n. Entonces $f(x)$ tiene a lo sumo n raíces en cualquier extensión F de K.*

Demostración: La demostración será por inducción sobre el grado de $f(x)$.

Si el grado de $f(x)$ es 0, entonces $f(x)$ es constante y no tiene raíces. Por lo tanto no hay nada que probar en este caso.

Si el grado de $f(x)$ es 1, entonces $f(x)$ es un polinomio lineal, digamos, $f(x) = ax + b$, para algunos a y b en K.

Si λ es una raíz de $f(x)$, entonces $f(x) = a\lambda + b = 0$ y por lo tanto $\lambda = -b/a$. Luego existe una única raíz.

Supongamos el teorema cierto para todo polinomio de grado menor que n. Sea $f(x)$ de grado n. Sea F una extensión de K. Si $f(x)$ no tiene ninguna raíz en F, entonces estará listo. Si $f(x)$ tiene una raíz λ en F de multiplicidad m, entonces $f(x) = (x - \lambda)^m q(x)$, donde $q(x)$ es un polinomio de grado $n - m$ que no tiene a λ como raíz.

Podemos entonces aplicar la hipótesis de inducción a $q(x)$ para concluir que no tiene más de $n - m$ raíces en F. Como toda raíz de $q(x)$ es una raíz de $f(x)$, se deduce entonces que $f(x)$ tiene a lo sumo $m + (n - m) = n$ raíces en F. Con esto queda probada la proposición para n.

♠

A continuación daremos un resultado muy importante sobre las raíces de un polinomio con coeficientes en los complejos. La demostración de este hecho requiere algunos conocimientos de la teoría de funciones analíticas los cuales pueden ser estudiados en un curso introductorio de un semestre.

Teorema 9.3.3 *(Teorema Fundamental del Algebra) Todo polinomio $f(x) \in \mathbb{C}[x]$ de grado n, posee exactamente n raíces en $\mathbb{C}$*

Demostración: Sea $f(x) \in \mathbb{C}[x]$. Será suficiente con probar que $f(x)$ tiene una raíz en $\mathbb{C}$ (¿Por qué?)

Si suponemos $f(z) \neq 0$ para todo z en $\mathbb{C}$, entonces la función

$$g(z) = \frac{1}{f(z)}$$

es una función entera (analítica en todo el plano complejo).

Nótese que g es una función acotada en todo $\mathbb{C}$, pues g es acotada en cualquier conjunto de la forma:

$$B_r = \{z \in \mathbb{C} \mid |z| \leq r\}$$

Además si hacemos $|z| = r$, se puede probar que g es acotado en todo el plano complejo, pues se tiene

$$\lim_{r \longrightarrow \infty} g(z) = \lim_{|z| \longrightarrow \infty} \frac{1}{f(z)} = 0$$

Podemos ahora invocar el teorema de Liouville de las funciones analíticas, el cual establece:

"Toda función entera acotada en $\mathbb{C}$, es constante".

Entonces se concluye que g es una función constante, lo cual es una contradicción. Por lo tanto $f(z_0) = 0$ para algún $z_0 \in \mathbb{C}$.

♠

Corolario 9.3.1 *Sea $f(x)$ un polinomio con coeficientes complejos de grado n. Entonces $f(x)$ se factoriza completamente*

$$f(x) = a_n(x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n)$$

donde $\alpha_i \in \mathbb{C}$ son las raíces de $f(x)$.

Ejercicios

1) Probar que los siguientes polinomios son irreducibles

a) $x^2 + x + 1$ en los enteros módulo 2.

b) $x^2 + x - 3$ en los enteros módulo 4.

c) $x^2 - x - 3$ en los enteros módulo 5.

d) $x^3 - 4$ en los enteros módulo 5.

e) $x^2 - 3$ en los enteros módulo 17.

f) $x^3 - 11$ en los enteros módulo 17.

2) Determine todos los polinomios irreducibles en $\mathbb{Z}_3[x]$.

3) Fórmula de interpolación de Lagrange.

Sea K un cuerpo, $n \geq 0$ y elementos $c_0, c_1, \ldots, c_n,\ b_0, b_1, \ldots, b_n$ en K. Entonces sea

$$f(x) = \sum_{i=0}^{n} b_i \prod_{k=0, k\neq i}^{n} (c_i - c_k)^{-1}(x - c_k)$$

Probar que

i) $f(c_i) = b_i$, para todo $0 \leq i \leq n$

ii) $f(x)$ es el único polinomio de grado n en $K[x]$ que satisface i).

4) Usando la fórmula anterior, determine un polinomio de grado 4, que satisfaga:

$$f(1) = 2, \quad f(2) = 3, \quad f(3) = 2, \quad \text{y} \quad f(4) = 3.$$

5) La Derivada de un polinomio. Si $f(x) \in K[x]$, entonces la derivada de $f(x)$, denotada por $f'(x)$, es el polinomio

$$f'(x) = na_n x^{n-1} + (n-1)a_{n-1}x^{n-2} + \cdots + 2a_2 x + a_1$$

si

$$f(x) = a_n x^n + \cdots + a_1 x + a_0$$

Probar las fórmula de derivación

i) $(f(x)+g(x))' = f'(x)+g'(x)$

ii) $(f(x)\cdot g(x))' = f'(x)g(x)+f(x)g'(x)$

6) Probar que un polinomio $f(x) \in K[x]$ tiene una raíz múltiple en alguna extensión de K, si y sólo si $f(x)$ y $f'(x)$ no son primos relativos.

7) Probar que si K es un cuerpo de característica 0, entonces $f'(x) = 0$ si y sólo si $f(x)$ es constante.

8) Solución de una ecuación cúbica. Sea

$$f(x) = x^3 + Ax^2 + Bx + C$$

un polinomio en $\mathcal{Q}[x]$.

i) Probar que el cambio de variable $x = t - \dfrac{a}{3}$ en el polinomio anterior nos da un polinomio de la forma

$$h(t) = x^3 + ax - b \tag{9.6}$$

con $a, b \in \mathcal{Q}$.

ii) En (**??**) haga el cambio de variables

$$x = s + t,$$

y entonces demuestre que:

$$s^3 + t^3 + 3st^2 + 3s^2t = b - a(s+t)$$

iii) Si hacemos $s^3 + t^3 = b$, probar que s^3 satisface la ecuación cuadrática

$$x^2 - bx - \left(\frac{a}{3}\right)^3 = 0 \tag{9.7}$$

iv) Calcule s y t y demuestre que la solución de la ecuación

$$x^3 + ax - b = 0$$

viene dada por

$$x = \sqrt[3]{\frac{b}{2} + \sqrt{\left(\frac{b}{a}\right)^2 + \left(\frac{a}{3}\right)^3}} + \sqrt[3]{\frac{b}{a} - \sqrt{\left(\frac{b}{2}\right)^2 + \left(\frac{a}{3}\right)^3}}$$

9) Hallar las raíces del polinomio $f(x) = x^3 + 6x - 4$.

10) Sea D un Dominio de Integridad y $c_0, c_1, \ldots, c_n$ elementos en D. Probar que para cualquier conjunto de elementos $b_0, b_1, \ldots, b_n$ en D, existe un único polinomio $f(x)$ de grado a lo sumo $n+1$ tal que $f(c_i) = b_i$, $\leq i \leq n$.

9.4 Polinomios sobre $\mathcal{Q}$

En esta sección nos dedicaremos a estudiar la factorización de polinomios con coeficientes en el cuerpo de los números racionales $\mathcal{Q}$.

Sabemos que $\mathcal{Q}[x]$ es un Dominio de Factorización Unica y por lo tanto todo polinomio $f(x)$ en $\mathcal{Q}[x]$ se factoriza de manera única.

$$f(x) = p_1(x)p_2(x)\cdots p_s(x)$$

donde los $p_i(x)$ son irreducibles en $\mathcal{Q}[x]$.

Estudiaremos como determinar los $p_i(x)$ en la descomposición de arriba, usando el algoritmo de división. También daremos un criterio práctico para decidir si un polinomio es irreducible sobre $\mathcal{Q}[x]$.

Un hecho muy interesante, el cual será probado en el desarrollo de esta sección, es el siguiente: todo polinomio con coeficientes enteros que es irreducible en $\mathbb{Z}[x]$, también lo es en $\mathcal{Q}[x]$.

Proposición 9.4.1 *Sea $f(x)$ un polinomio de grado ≤ 3 en $\mathcal{Q}[x]$. Entonces si $f(x)$ es reducible en $\mathcal{Q}[x]$, existe $r \in Q$ tal que $f(r) = 0$.*

Demostración: Por ser $f(x)$ reducible, se tiene entonces $f(x) = h(x)g(x)$ para algunos polinomios $h(x)$ y $g(x)$ en $\mathcal{Q}[x]$ y además $h(x)$ y $g(x)$ no son constantes.

Luego se tiene

$$3 = grado(f(x)) = grado(h(x)) + grado(g(x))$$

Por lo tanto el grado de $h(x)$ o $g(x)$ debe ser igual a 1. Si suponemos que el grado de $h(x)$ es 1, entonces $h(x) = ax + b$ para $a, b \in \mathcal{Q}$, y luego

$$f(x) + (ax + b)g(x)$$

Si $b = 0$,entonces $r = 0$ es raíz de $f(x)$. Si $b \neq 0$, entonces $r = -\dfrac{a}{b}$ es raíz de $f(x)$. Con esto queda probado que $f(x)$ tiene una raíz en $\mathcal{Q}$.

♠

Definición 9.4.1 *Sea* $f(x) = a_n x^n + \cdots + a_1 x + a_0$ *un polinomio en* $\mathbb{Z}[x]$. *Se define* **el contenido** *de* $f(x)$ *como el Máximo Común Divisor de los coeficientes* $a_0, a_1, \ldots, a_n$.

Usaremos la notación $C(f)$ para el contenido de $f(x)$.

Ejemplo: Si $f(x) = 12x^3 - 6x^2 + 18x$ entonces, $C(f) = (12, 6, 18) = 6$.

Definición 9.4.2 *Sea* $f(x)$ *un polinomio con coeficientes enteros. Entonces se dice que* $f(x)$ **es primitivo**, *si* $C(f) = 1$.

Ejemplo: Sea $f(x) = 8x^5 - 13x + 4$. Luego $f(x)$ es primitivo.

Observación: Si $f(x)$ es un polinomio mónico con coeficientes en $\mathbb{Z}$, entonces $f(x)$ es primitivo.

Proposición 9.4.2 *Sean* $f(x)$ *y* $h(x)$ *polinomios primitivos en* $\mathbb{Z}[x]$, *entonces* $f(x)h(x)$ *es primitivo.*

Demostración: Supongamos que

$$f(x) = a_n x^n + \cdots + a_1 x + a_0 \quad \text{y} \quad h(x) = b_m x^m + \cdots + b_1 x + b_0$$

Entonces

$$f(x)h(x) = C_s x^s + \cdots + C_1 x + C_0$$

con $s = m + n$.

Supongamos por el absurdo que $f(x)h(x)$ no es primitivo. Entonces existe $d > 0$ tal que d divide a C_i para todo $0 \leq i \leq s$.

Como $f(x)$ es primitivo, d no puede dividir a todos los coeficientes de f. Sea a_k el primer coeficiente de f que no es divisible por d.

Similarmente, $h(x)$ es primitivo y supongamos que b_j es el primer coeficiente de $h(x)$ que no es divisible por d.

Luego $d|a_i,\ \ 0 \leq i \leq k$ y $d|b_i,\ \ 0 \leq i \leq j$ y

$$d \not| \ a_k b_j$$

Entonces el coeficiente C_{k+j} de $f(x)h(x)$ es de la forma

$$C_{k+j} = a_k b_j + (a_{k-1}b_{j+1} + \cdots + a_0 b_{j+k}) + (b_{j-1}a_{k+1} + \cdots + b_0 a_{j+k})$$

Tenemos entonces que

$$d|(a_{k-1}b_{j+1} + \cdots + a_0 b_{j+k})$$

y

$$d|(b_{j-1}a_{k+1} + \cdots + b_0 a_{j+k})$$

luego

$$d|C_{k+j} - a_k b_j$$

lo cual es una contradicción, pues $d|C_{k+j}$ y $d \not| \ a_k b_j$.

Por lo tanto $f(x)h(x)$ es primitivo.

♠

Proposición 9.4.3 *(Lema de Gauss) Sea $f(x)$ un polinomio primitivo en $\mathbb{Z}[x]$. Si $f(x) = p(x)q(x)$ con $p(x), q(x)$ en $\mathcal{Q}[x]$, entonces $f(x) = p_1(x)q_1(x)$, donde $p_1(x), q_1(x)$ son polinomios con coeficientes enteros. Además*

$$p_1(x) = \lambda p(x) \qquad \text{y} \qquad q_1(x) = \beta q(x),$$

con λ y β números racionales.

Demostración: Sea

$$\begin{aligned} p(x) &= r_s x^s + \cdots + r_1 x + r_0 \quad , \quad r_i \in \mathcal{Q} \\ q(x) &= t_l x^l + \cdots + t_1 x + t_0 \quad , \quad t_i \in \mathcal{Q} \end{aligned}$$

Sean m_1, m_2, el mínimo común multiplo de los denominadores de $p(x)$ y $q(x)$ respectivamente.

Luego $m_1 p(x)$ y $m_2 q(x)$ son polinomios con coeficientes enteros. Si hacemos

$$C_1 = C(p(x)) \quad \text{y} \quad C_2 = C(q(x))$$

Definimos entonces

$$p_1(x) = \frac{m_1}{C_1} p(x) \quad \text{y} \quad q_1(x) = \frac{m_2}{C_2} q(x)$$

luego $p_1(x)$ y $q_1(x)$ son polinomios primitivos, y además

$$\begin{aligned} f(x) &= p(x)q(x) \\ &= \frac{C_1 C_2}{m_1 m_2} p_1(x) q_1(x) \end{aligned}$$

o sea

$$m_1 m_2 f(x) = C_1 C_2 p_1(x) q_1(x)$$

Como $f(x)$ es mónico, el contenido del lado izquierdo es $m_1 m_2$ y por lo tanto $m_1 m_2 = C_1 C_2$. Luego

$$f(x) = p_1(x)q_1(x).$$

♠

Observación: Si en la proposición anterior el polinomio $f(x)$ es mónico, entonces tanto $p_1(x)$ como $q_1(x)$ resultan ser mónicos con coeficientes enteros.

El siguiente teorema da una condición necesaria para la existencia de raíces racionales en polinomios de coeficientes enteros.

Teorema 9.4.1 *Sea* $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$ *y* $r = \dfrac{s}{t}$ *un número racional. Entonces si* r *es raíz de* $f(x)$ *se debe tener*

$$s|a_0 \quad y \quad t|a_n$$

Demostración: Supongamos que $(s,t) = 1$. Luego

$$f(x) = \left(x - \frac{s}{t}\right) q(x), \quad \text{con} \quad q(x) \in \mathcal{Q}[x]$$

Usando el Lema de Gauss se obtiene

$$f(x) = (tx - s)q_1(x), \tag{9.8}$$

donde $q_1(x)$ tiene coeficientes enteros.

Comparando el coeficiente de grado n en ambos lados de (**??**) se tiene que $t|a_n$. Igualmente, comparando el término constante en ambos lados de (**??**) se sigue que $s|a_0$.

♠

Corolario 9.4.1 *Sea* $f(x) = a_n x^n + \cdots + a_1 x + a_0$ *un polinomio con coeficientes enteros. Entonces si* r *es una raíz entera de* $f(x)$*, se debe tener* $r|a_0$.

Ejemplo: Hallar las raíces racionales de

$$f(x) = 27x^3 - 8$$

Tenemos que las posibles raíces son de la forma $\frac{s}{t}$, donde $s|8$ y $t|27$. Luego los posibles valores de s son $\pm 1,\ \pm 2,\ \pm 4,\ \pm 8$; y los posibles valores de t son $\pm 1,\ \pm 3,\ \pm 9,\ \pm 27$. Después de probar todas las combinaciones posibles de s y t, el valor $s = 2$, $t = 3$ nos da una raíz. Luego dividimos el polinomio $f(x)$ entre $x - \frac{2}{3}$ para obtener

$$\begin{aligned} 27x^3 - 8 &= \left(x - \frac{2}{3}\right)(27x^2 + 18x + 12) \\ &= 3\left(x - \frac{2}{3}\right)(9x^2 + 6x + 4) \end{aligned}$$

Las raíces de $9x^2 + 6x + 4$ son complejas y por lo tanto $f(x)$ tiene una sola raíz racional.

Veamos ahora un criterio muy simple para decidir si un polinomio con coeficientes enteros es irreducible.

Teorema 9.4.2 *Sea $f(x)$ un polinomio en $\mathbb{Z}[x]$. Si para algún entero m, se tiene que $f(x)$ es irreducible en $\mathbb{Z}_m[x]$, entonces $f(x)$ es irreducible en $\mathbb{Z}[x]$.*

Demostración: Si $f(x) = a_n x^n + \cdots + a_1 x + a_0$ entonces la imágen de $f(x)$ en $\mathbb{Z}_m[x]$ es el polinomio

$$\overline{f}(x) = \overline{a_n} x^n + \cdots + \overline{a_1} x + \overline{a_0}$$

donde $\overline{a_i}$ es la imágen de a_i bajo la proyección

$$\prod_m : \mathbb{Z} \longrightarrow \mathbb{Z}_m$$

Si $f(x)$ es reducible en $\mathbb{Z}[x]$, entonces

$$f(x) = h(x)q(x)$$

y por lo tanto

$$\overline{f}(x) = \overline{h}(x)\overline{q}(x)$$

luego $\overline{f}(x)$ es reducible en $\mathbb{Z}_m[x]$.

♠

Ejemplo: Sea $f(x)$ $x^3 + x - 3$. Entonces $f(x)$ es irreducible en $\mathbb{Z}_4$ (Verificarlo!), luego $f(x)$ es irreducible en $\mathbb{Z}$.

Teorema 9.4.3 *(Criterio de Eisenstein) Sea* $f(x) = a_n x^n + \cdots + a_1 x + a_0$ *un polinomio con coeficientes enteros. Sea* p *un número primo, tal que*

i) $p | a_i \qquad 0 \leq i < n$

ii) $p \nmid a_n$

ii) $p^2 \nmid a_0$

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

Demostración: Dividimos la prueba en dos casos

Caso I: si $f(x)$ es primitivo y es reducible en $\mathcal{Q}[x]$ entonces por el lema de Gauss, se tiene

$$f(x) = h(x)q(x) \tag{9.9}$$

con $h(x), q(x)$ en $\mathbb{Z}[x]$.

Sea

$$h(x) = b_s x^s + \cdots + b_1 x + b_0,$$

y

$$q(x) = C_t x^t + \cdots + C_1 x + C_0$$

Comparando los coeficientes de grado 0, en (**??**) tenemos que

$$a_0 = b_0 C_0$$

Ahora bien, como $p|a_0$ y $p^2 \not| \, a_0$, se tiene que $p|b_0 C_0$, pero no puede dividir a ambos.

Luego, supongamos que $p|b_0$ y $p \not| \, C_0$.

Si $p|b_i$ para todos los i, entonces $p|a_i$ para todos los i, y por lo tanto $f(x)$ no es primitivo.

Supongamos que $p|b_i$ para $o \leq i < k < s$ y $p \not| \, b_k$, luego se tiene

$$a_k = b_k C_0 + b_{k-1} C_1 + \cdots + b_0 C_k$$

y por hipótesis $p|a_k$. Entonces

$$p| \, [a_k - (b_{k-1} C_1 + \cdots + b_0 C_k)]$$

lo cual es una contradicción, pues $p \not| \, b_k C_0$.

Por lo tanto $f(x)$ no es reducible en $\mathcal{Q}[x]$.

Caso II: Si $f(x)$ no es mónico, hacemos

$$f(x) = d f_1(x),$$

donde $f_1(x)$ es primitivo con coeficientes enteros. Luego los coeficientes de $f_1(x)$ satisfacen las hipótesis $i)$ $ii)$ $iii)$ del teorema, pues $p \not| \, a_n$ y por lo tanto $p \not| \, d$.

♠

Ejercicios

1) Factorizar completamente en el cuerpo de los números complejos los polinomios

a) $x^4 - 3x^3 - 4x^2 - 6x + 4$

b) $x^3 - 9x^2 + 20x - 12$

c) $x^4 - 8x^2 + 16$

d) $x^5 + 2x^4 + x^3 - 8x^2 - 16x - 8$

e) $x^5 - 3x^4 + 2x^3 - 2x^2 + 6x - 4$

f) $x^6 - 4x^5 - 12x^4 - x^2 + 4x + 12$

2) Si p es un número primo y n es un entero $n \geq 2$, probar que $f(x) = x^n - p$ es irreducible sobre los racionales.

3) Sea p un número primo. Entonces el **polinomio ciclotómico de orden** p se define por

$$f(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$$

Demuestre que $f(x)$ es irreducible sobre los racionales.

4) Sea $w = e^{2\pi i/p}$ la raíz p-ésima de la unidad en los números complejos.

Demuestre que el polinomio $f(x)$ del problema anterior se factoriza en $\mathcal{C}[x]$

$$f(x) = (x - w)(x - w^2) \cdots (x - w^{p-1})$$

5) Si a y b son dos números enteros, demostrar que

$$a^p + b^p = (a + b)(a + bw)(a + bw^2) \cdots (a + bw^{p-1})$$

donde $w = e^{2\pi i/p}$

6) Sean a y c enteros positivos, con $a > 0$ y $c > 0$. Probar que el polinomio $f(x) = x^3 + ax^2 + c$ no tiene raíces reales en el intervalo $[-a, +\infty]$.

7) Demuestre que $\mathbb{Z}_m[x]$ es un anillo finito para todo $m > 1$.

8) Factorizar en $\mathbb{Z}_5[x]$ los polinomios

a) $x^2 + 3x - 1$

b) $x^3 + 3$

c) $x^4 + x^3 + 2x$

d) $x^2 - 6x + 3$

9) Sea p un número primo. Hallar la factorización del polinomio $x^p - x$ en $\mathbb{Z}_p[x]$.

10) Usando el ejercicio 9, probar la congruencia

$$(p-1)! \equiv -1 \ mod \ p$$

11) Hallar todas las raíces de $f(x) = x^2 - x$ en $\mathbb{Z}_6$.

12) Determine los valores de s para los cuales $f(x) = x^4 + x + s$ es irreducible en $\mathbb{Z}_5$.

13) Sea $f(x) = a_n x^n + \cdots + a_1 x + a_0$ un polinomio en $\mathbb{C}[x]$. El **polinomio conjugado** de $f(x)$, se define por

$$\overline{f}(x) = \overline{a}_n x^n + \cdots + \overline{a}_1 x + \overline{a}_0,$$

donde $\overline{a}i$ es el conjugado del número complejo a_i. Probar que $r \in \mathbb{C}$ es raíz de $f(x)$ si y sólo si $\overline{r}$ es raíz de $\overline{f}(x)$.

14) Sea $f(x) = a_n x^n + \cdots + a_1 x + a_0$ un polinomio en $\mathbb{R}[x]$. Demostrar que si $f(x)$ tiene una raíz $r \in \mathbb{C}$, entonces $\overline{r}$ también es raíz de $f(x)$.

15) Halle un ejemplo de un anillo A, tal que el polinomio $f(x) = x^2 + a$ posea infinitas raíces.

9.5 Polinomios en Varias Variables

En el estudio de las curvas y superficies en el plano y el espacio, nos encontramos frecuentemente con ecuaciones con más de una variable.

Por ejemplo la circunferencia de radio 1 con centro en el origen se expresa analíticamente mediante la ecuación:

$$x^2 + y^2 - 1 = 0 \tag{9.10}$$

Es posible entonces, usar más de una variable para los polinomios y definir el polinomio en dos variables:

$$F(x, y) = x^2 + y^2 - 1$$

Entonces la ecuación (**??**) se expresa

$$F(x, y) = 0 \tag{9.11}$$

En esta sección se dara una definición formal del anillo de polinomios en varias variables, así como alguna de sus propiedades más importantes.

Si A es un anillo, entonces $A[x]$, es otro anillo y tiene significado la siguiente definición

Definición 9.5.1 *Sea A un anillo y x_1, x_2 indeterminadas. Entonces el* **anillo de polinomios en** *x_1, x_2, denotado por $A[x_1, x_2]$ es igual al anillo $(A[x_1])[x_2]$.*

Entonces un polinomio $f(x_1, x_2)$ en $A[x_1, x_2]$ es una expresión de la forma

$$f(x_1, x_2) = f_n(x_1)x_2^n + f_{n-1}(x_1)x_2^{n-1} + \cdots + f_1(x_1)x_2 + f_0(x_1)$$

donde $f_i \in A[x_1]$.

Luego $f(x_1, x_2)$ se expresa como una combinación de las incógnitas x_1 y x_2 de la forma

$$f(x_1, x_2) = \sum_{j=0}^{\infty} \sum_{i=0}^{\infty} a_{ij} x_1^i x_2^j$$

donde $a_{ij} = 0$ para casi todos los i, j.

Ejemplo: Sea $A = \mathbb{Z}$ y $f(x_1, x_2)$ el polinomio en $\mathbb{Z}[x_1, x_2]$, definido por

$$f(x_1, x_2) = x_1^2 + 3x_1x_2 + x_2^2$$

Entonces $a_{21} = 1$, $a_{12} = 1$, $a_{11} = 3$ y $a_{ij} = 0$ para los restantes subindices.

Podemos definir el anillo de polinomios de n variables $x_1, \ldots, x_n$ sobre A, en forma recursiva haciendo

$$A[x_1, \ldots, x_n] = A[x_1, \ldots, x_{n-1}][x_n]$$

Entonces $A[x_1, \ldots, x_n]$ satisface todas las propiedades de anillo.

Definición 9.5.2 *Un elemento del anillo $A[x_1, \ldots, x_n]$ de la forma*

$$u = x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n}, \quad \alpha_i \geq 0$$

se llama **un monomio**

Podemos considerar la n-upla $\alpha = (\alpha_1, \ldots, \alpha_n)$ en

$$T = S \times \cdots \times S = S^n$$

donde $S = \mathbb{N} \cup \{0\}$. Luego usamos la notación para el monomio n,

$$u = X^\alpha$$

donde $X = (x_1, \cdots, x_n)$

Consideremos aquellas funciones

$$\phi : T \longrightarrow A$$

tales que $\phi(\alpha) = 0$ para todo α, excepto para un número finito. Con estas herramientas a la mano, se tiene la siguiente

Definición 9.5.3 *Sea A un anillo, un polinomio f en $A[x_1, \cdots, x_n]$ es una combinación lineal de monomios*

$$f(X) = \sum_{\alpha \in T} \phi(\alpha) X^{\alpha} \tag{9.12}$$

Ejemplo: El polinomio en $\mathbb{Z}[x_1, x_2, x_3]$, dado por

$$f(x_1, x_2, x_3) = 2x_1^3 + x_1 x_2^2 + x_1 x_2 - 6x_1 x_2 x_3.$$

Entonces $f(x_1, x_2, x_3)$ se expresa en la forma (**??**) tomando la función $\phi : S^3 \longrightarrow \mathbb{Z}$ de la forma siguiente

$\phi(3,0,0) = 2$
$\phi(1,2,0) = 1$
$\phi(1,1,0) = 1$
$\phi(1,1,1) = -6$
$\phi(\alpha) = 0$,
para α diferente de $(3,0,0)$, $(1,2,0)$, $(1,1,0)$ y $(1,1,1)$

Teorema 9.5.1 *Si A es un Dominio de Integridad, entonces el anillo de polinomios en n variables $A[x_1, \cdots, x_n]$ es un Dominio de Integridad.*

Demostración: Hemos probado en la proposición **??** que $A[x_1]$ es un Dominio de Integridad, entonces se demuestra que $A[x_1][x_2]$ es también Dominio de Integridad y podemos entonces continuar en forma recursiva, para concluir que $A[x_1, \cdots, x_n]$ es un Dominio de Integridad.

♠

Definición 9.5.4 *Si A es un Dominio de Integridad, entonces el cuerpo de fracciones de $A[x_1, \cdots, x_n]$, se llama* **cuerpo de funciones racionales** *en $x_1, \cdots, x_n$.*

Los elementos de este cuerpo son funciones en las n variables $x_1, \cdots, x_n$, del tipo

$$f(x_1, \ldots, x_n) = \frac{p(x_1, \ldots, x_n)}{q(x_1, \ldots, x_n)}$$

donde p y q son polinomios en $A[x_1, \ldots, x_n]$.

El objetivo más importante de esta sección será probar que si A es un Dominio de Factorización Unica entonces el anillo de polinomios $A[x_1, \ldots, x_n]$ es un Dominio de Factorización Unica.

Si A es un Dominio de Factorización Unica y $f(x) = a_n x^n + \cdots + a_1 x + a_0$ es un polinomio en $A[x]$, entonces su **contenido**, denotado por $C(f)$, es el máximo común divisor de los coeficientes $a_n, a_{n-1}, \ldots, a_0$. Si $C(f) = 1$, entonces diremos que el polinomio $f(x)$ es **primitivo**.

Proposición 9.5.1 *Sea A un Dominio de Factorización Unica y $f(x) \in A[x]$ un polinomio no constante. Entonces existe un único elemento c en A, salvo unidades, tales que*

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

con $h(x)$ primitivo.

El elemento c es el contenido de $f(x)$.

Demostración: Sea $f(x) = a_n x^n + \cdots + a_1 x + a_0$. Como A es un Dominio de Factorización única, cada elemento a_i se expresa de manera única como un producto de irreducibles, salvo asociados.

Luego $C(f) = (a_n, a_{n-1}, \ldots, a_1, a_0)$ es un elemento de A. Como $C(f)$ divide a a_i, para todo i, $0 \leq i \leq n$, se tiene

$$a_i = C(f)b_i, \qquad 0 \leq i \leq n$$

para algunos elementos $b_i \in A$.

Además se tiene que $(b_n, b_{n-1}, \ldots, b_1, b_0) = u$, donde u es una unidad, pues si hay algún factor común de $b_n, \ldots, b_0$, digamos d, se tiene que $d.C(f)$ es un divisor común de los a_i, y por lo tanto $d.C(f)$ divide a $C(f)$

Luego

$$C(f) = d.C(f).t$$

para algún $t \in A$, lo cual implica que d es una unidad. Esta unidad u, se puede factorizar y entonces definimos el polinomio

$$h(x) = b'_n x^n + b'_{n-1} x^{n-1} + \cdots + b'_1 x + b'_0$$

donde $b'_i u = b_i$, para $0 \leq i \leq n$.

Entonces $h(x)$ es un polinomio primitivo y se tiene

$$f(x) = C(f).u.h(x)$$

Si c' es otro elemento de A, y $h'(x)$ es un polinomio primitivo, tal que

$$f(x) = c'.h'(x)$$

Haremos entonces

$$C(f).uh(x) = c'.h'(x) \tag{9.13}$$

Tomando el contenido en ambos lados, se concluye que

$$C(f).u = c'$$

Luego $C(f)$ es único salvo unidades. Como $A[x]$ es un Dominio de Integridad, podemos cancelar c' en ambos lados de (**??**) para obtener

$$h(x) = h'(x)$$

♠

A continuación daremos sin demostración un resultado previo al Lema de Gauss para polinomios en $A[x]$, el cual fue estudiado en la sección anterior. La demostración es exactamente igual a la demostración dada para polinomios en $\mathbb{Z}[x]$

Proposición 9.5.2 *Si A es un Dominio de Factorización Unica, entonces el producto de dos polinomios primitivos es primitivo.*

Este resultado se generaliza fácilmente a n polinomios.

Corolario 9.5.1 *Sea A un Dominio de Factorización Unica. Si los polinomios $p_1(x), p_2(x), \ldots, p_s(x)$ son primitivos en $A[x]$, entonces el producto $p_1(x)p_2(x)\ldots p_s(x)$ es también primitivo en $A[x]$.*

Corolario 9.5.2 *Sea A un Dominio de Factorización Unica y K su cuerpo de fracciones. Entonces n $f(x)$ es un polinomio irreducible y primitivo en $A[x]$, se tiene que $f(x)$ es irreducible en $K[x]$*

Demostración: Si suponemos que $f(x)$ es reducible en $K[x]$ se tendrá

$$f(x) = p_1(x)p_2(x)$$

con $p_1(x)$, $p_2(x)$ en $K[x]$. Podemos sacar factor común de los denominadores en $p_1(x)$ y $p_2(x)$, para obtener

$$f(x) = \frac{c}{d}p_1'(x)p_2'(x)$$

donde c y d están en A y $p_1'(x), p_2'(x)$ son polinomios primitivos en $A[x]$. Luego el producto $p_1'(x).p_2'(x)$ es primitivo y por la proposición (**??**), se concluye que

$$c = d.u,$$

donde u es una unidad en A. Luego tendremos

$$f(x) = up_1'(x)p_2(x)$$

lo cual es una contradicción, pues $f(x)$ es irreducible en $A[x]$

♠

Teorema 9.5.2 *Si A es un Dominio de Factorización Unica, entonces $A[x]$ es un Dominio de Factorización Unica.*

Demostración: Sea $f(x)$ un polinomio en $A[x]$ no constante, si $f(x)$ es irreducible estará listo. Si $f(x)$ es reducible, existen polinomios $f_1(x)$ y $f_2(x)$, con $g(f_1(x)) < g(f(x))$ y $g(f_2(x)) < g(f(x))$, tales que

$$f(x) = f_1(x)f_2(x)$$

Si aplicamos inducción sobre el grado de $f(x)$, se deduce entonces que los polinomios $f_1(x)$ y $f_2(x)$ se expresa como un producto de irreducibles. Luego $f(x)$ es un producto de polinomios irreducibles en $A[x]$.

Unicidad: Supongamos que $f(x)$ tenga dos descomposiciones como producto de polinomios irreducibles en $A[x]$

$$p'_1(x)\cdots p'_s(x) = q'_1(x)\cdots q'_t(x) \tag{9.14}$$

Para cada i, j hacemos $p'_i(x) = d_i p_i(x)$, $q'_j = c_j q_j(x)$ donde d_i, c_j están en A y los polinomios $p_i(x)$ y $q_j(x)$ son primitivos. Luego tendremos

$$d_1\cdots d_s p_1(x)\cdots p_s(x) = c_1\cdots c_t q_1(x)\cdots q_t(x) \tag{9.15}$$

Como cada $p_i(x)$ es primitivo, entonces el producto de todos ellos es primitivo. De igual manera se concluye que el producto de todos los $q_j(x)$ es primitivo. Luego, por la proposición (**??**), se concluye que

$$ud_1\cdots d_s = c_1\cdots c_t,$$

donde u es una unidad en A.

Luego podemos hacer cancelación en (**??**) para obtener

$$p_1(x)\cdots p_s(x) = uq_1(x)\cdots q_t(x) \tag{9.16}$$

Ahora bien, si K es el cuerpo de fracciones de A, los polinomios $p_i(x)$, $q_j(x)$ están en $K[x]$, y además son irreducibles y primitivos, luego son irreducibles en $K[x]$.

Entonces aplicando el teorema de la factorización única para polinomios en $K[x]$, concluimos $s = t$ y

$$p_i(x) = c_i q_j(x) \qquad 1 \leq i \leq n$$

para algún $l_i \in K$.

Usando el hecho de que p_i y q_j son polinomios primitivos en $A[x]$, se concluye

$$p_i(x) = u_i q_j(x), \qquad 1 \leq i \leq 1$$

donde u_i es una unidad en A.

♠

Corolario 9.5.3 *Si A es un Dominio de Factorización Unica, entonces $A[x_1, \ldots, x_n]$ es un Dominio de Factorización Unica.*

Ejemplo: Sea $\mathbb{R}$ el anillo $\mathbb{Z}[x, y]$. Como $\mathbb{Z}$ es un Dominio de Factorización Unica, se tiene que $\mathbb{R}$ lo es también. Sin embargo este anillo no es un dominio de ideales principales, pues el ideal $I = (x, y)$ no es principal.

Ejercicios

1) Probar que $A[x, y] = A[y, x]$

2) Demuestre que $f(x) = x^2 + y^2 - 1$ es irreducible sobre el cuerpo de los racionales. ¿Será reducible sobre los complejos?

3) Sean $f(x, y) = 3x^2y^5 + 6y^2x - 12xy$, y $g(x, y) = 3x^2y^2 - xy^2 + 2x^2y$, polinomios en $\mathbb{Z}[x, y]$. Expresar estos polinomios en la forma de la definición (**??**)

$$f(X) = \sum_{\alpha \in T} \phi(\alpha) X^{\alpha}$$

Usando esta forma, ejecute las operaciones

a) $f(x, y)g(x, y)$

b) $g(x, y)f(x, y)$

4) Hallar una fórmula para el producto y la suma de dos polinomios de n variables.

5) Demuestre que el producto de polinomios es conmutativo.

Capítulo

10

Cuerpos

10.1 Introducción

La estructura de cuerpo es una de las más completas dentro del álgebra. Por tener buenas propiedades de divisibilidad y factorización, los cuerpos son conjuntos adecuados para plantear y resolver ecuaciones.

En este capítulo se estudian las extensiones algebraicas de cuerpos y algunas de sus propiedades.

Existe una estrecha conexión entre la teoría de cuerpos y la teoría de los polinomios, como se verá en este capítulo. Ambas teorías tienen su origen común en uno de los problemas más antiguos de la matemática, como lo es la resolución de ecuaciones algebraicas de grado > 1 y el problema de las construcciones geométricas.

Desde la época de los babilonios, los matemáticos se plantean resolver ecuaciones cuadráticas, para lo cual comenzaron a utilizar raíces cuadradas. Los griegos resuelven algunos de estos problemas usando métodos geométricos. Uno de sus mayores logros fue demostrar que la ecuación

$$x^2 - 2 = 0$$

esa irresoluble en el cuerpo de los números racionales, pues $\sqrt{2}$ no se puede expresar como una fracción.

Además de este, los griegos plantearon otros problemas irresolubles, como la cuadratura del circulo, la trisección del ángulo y la duplicación del cubo, los cuales no se podrán resolver por fracciones, pero cuya demostración formal hubo de esperar varios siglos.

Durante la edad media y el renacimiento el álgebra se ocupa casi exclusivamente de la resolución de ecuaciones de 3^{er} grado y 4^{to} grado,

usando raíces. Vale destacar a **Escipión del Ferro** quien a comienzos del siglo XVI obtiene una solución por medio de radicales para la ecuación cúbica

$$x^3 + ax = b$$

También los matemáticos italianos del renacimiento Tartaglia, Cardano y Ludovico Ferrari, obtienen avances importantes al descubrir nuevas soluciones de estas ecuaciones mediante métodos ingeniosos de manipulación de raíces y cambios de variables.

El estudio general de las ecuaciones algebraicas de grado n, fue iniciado por Lagrange y Vandermonde en 1770. El método de Lagrange consiste en ir reduciendo de grado las ecuaciones, utilizando para ello el concepto de la resolvente de un polinomio.

Más tarde Carl F. Gauss en sus "*disquisitiones arithmethicae*" estudia el problema general de hallar las soluciones de una ecuación del tipo $x^n - 1 = 0$. Uno de los grandes logros de Gauss, es resolver el problema de la construcción geométrica con regla y compás de un poligono de n lados, lo cual se fundamenta en su estudio de esta ecuación.

El inicio de la teoría general de cuerpos se halla en la obra de los matemáticos, Ruffini, Abel y Galois, quienes demostraron que toda ecuación algebraica de grado mayor o igual que cinco no puede resolverse usando radicales.

Con Galois se inicia el estudio de las extensiones de cuerpos por adjunción de raíces. En sus trabajos se establece una conexión maravillosa entre las raíces de una ecuación polinómica, las extensiones de cuerpos que contienen estas raíces y el grupo de automorfismo de estos cuerpos. Esta teoría culmina en forma brillante uno de los capitulos más importantes de la matemática y que fue el objeto del álgebra durante varios siglos: la búsqueda de soluciones de una ecuación algebraica mediante radicales.

10.2 Cuerpos

Definición 10.2.1 *Un* **cuerpo** *es un conjunto $\mathbb{R}$, diferente del vacío, con dos operaciones llamadas suma y producto, denotadas por $+$ y $\cdot$*

tales que verifican

1) Para todo a, b en $\mathbb{R}$, se tiene:

$$a + b \in \mathbb{R} \quad y \quad a \cdot b \in \mathbb{R}$$

2) Para todos a, b, c en $\mathbb{R}$

$$\begin{aligned} a + (b + c) &= (a + b) + c \\ a \cdot (b \cdot c) &= (a \cdot b) \cdot c \end{aligned}$$

3) Para todo a, b en $\mathbb{R}$ se tiene

$$a + b = b + a \quad y \quad a \cdot b = b \cdot a$$

4) Existen elementos 0 y 1 en $\mathbb{R}$ llamados cero y uno, tales que para todo a en $\mathbb{R}$

$$\begin{aligned} a + 0 &= 0 + a = a, \\ a \cdot 1 &= 1 \cdot a = a \end{aligned}$$

5) Para todo a en $\mathbb{R}$, existe un elemento $-a$ llamado el opuesto de a tal que

$$a + (-a) = (-a) + a = 0$$

6) Si a es diferente de cero, existe un elemento a^{-1} en $\mathbb{R}$ llamado el inverso de a, tal que

$$a \cdot a^{-1} = a^{-1} \cdot a = 1$$

7) Para todos a, b, c en $\mathbb{R}$

$$\begin{aligned} a \cdot (b + c) &= a \cdot b + a \cdot c \\ (a + b) \cdot c &= a \cdot c + b \cdot c \end{aligned}$$

Observación: De acuerdo a la definición anterior, se tiene que $\mathbb{R}$ es un cuerpo si y sólo si, $\mathbb{R}$ es un anillo conmutativo con unidad, en donde todo elemento distinto de cero es una unidad.

Ejemplo 1: El conjunto de los números reales $\mathbb{R}$ bajo la suma y el producto.

Ejemplo 2: Si p es un número primo, $\mathbb{Z}_p$ el conjunto de los enteros módulo p es un cuerpo con la suma y el producto módulo p.

Ejemplo 3: Sea K un cuerpo. Entonces $K(x)$, el conjunto de funciones racionales sobre K, cuyos elementos son funciones del tipo

$$f(x) = \frac{p(x)}{q(x)}$$

donde $p(x)$ y $q(x)$ son polinomios sobre K y $q(x) \neq 0$, es un cuerpo.

Definición 10.2.2 *Un* **espacio vectorial** *sobre un cuerpo K, es un conjunto no vacío V cuyos elementos llamaremos* **vectores** *(para diferenciarlos de los elementos de K que se llaman escalares) y un par de operaciones suma de vectores y producto por un escalar, denotadas por $+$ y $\cdot$ y que satisfacen*

1) V es un grupo abeliano bajo la suma de vectores.

2) Para un vector v y $\alpha \in K$, se tiene

$$\alpha \cdot v \in V$$

3) Para v_1, v_2 en V y $\alpha, \beta \in K$ se tiene

$$\begin{aligned} (\alpha + \beta) \cdot v_1 &= \alpha \cdot v_1 + \beta \cdot v_1 \\ \alpha(v_1 + v_2) &= \alpha \cdot v_1 + \alpha \cdot v_2 \end{aligned}$$

4) Para $v \in V$ y $\alpha, \beta \in K$ se tiene

$$\alpha(\beta \cdot v) = (\alpha \cdot \beta) \cdot v$$

5) Si 1 es el uno en K, entonces

$$1 \cdot v = v$$

para todo $v \in V$

Observación: Si V es un espacio vectorial sobre K, diremos que V es un K-espacio.

Observación: El vector cero de $(V, +)$ será denotado por 0.

Ejemplo 1: Todo cuerpo K es un espacio vectorial sobre si mismo.

Ejemplo 2: Sea $V = \mathbb{R} \times \mathbb{R}$ con la suma de vectores definida por

$$(v_1, u_1) + (v_2, u_2) = (v_1 + v_2, u_1 + u_2)$$

y el producto por un escalar $\lambda \in \mathbb{R}$

$$\lambda(v, u) = (\lambda v, \lambda u)$$

Entonces es fácil verificar que V con estas operaciones es un espacio vectorial sobre $\mathbb{R}$.

Definición 10.2.3 *Sean $\{v_1, \ldots, v_n\}$ un conjunto de vectores en un espacio vectorial V sobre K. Un elemento $v \in V$, se dice que es* **combinación lineal** *de $\{v_1, \ldots, v_n\}$ si existen escalares $\lambda_1, \ldots, \lambda_n$, tales que*

$$v = \lambda_1 v_1 + \cdots + \lambda_n v_n$$

Definición 10.2.4 *Sea V un espacio vectorial y V' un subconjunto de V, de tal forma que V' es un espacio vectorial sobre K, con las mismas operaciones definidas en V. Entonces V' se dice un* **subespacio vectorial** *de V'.*

La siguiente proposición es un hecho bien conocido del álgebra lineal.

Proposición 10.2.1 *Sea $\{v_1, \ldots, v_n\}$ un conjunto de vectores de V. Entonces el conjunto de todas las combinaciones lineales de $\{v_1, \ldots, v_n\}$ genera un subespacio vectorial de V.*

Observación: El subespacio generado por $\{v_1, \ldots, v_n\}$ se denota por $\langle v_1, \ldots, v_n \rangle = W$. Los elementos $v_1, \ldots, v_n$ se llaman los **generadores de W**.

Observación: Si $V = \langle v_1, \ldots, v_n \rangle$, para algún conjunto de vectores $\{v_1, \ldots, v_n\}$ en V, entonces se dice que V es **finitamente generado**.

Definición 10.2.5 *Sea V un espacio vectorial. Un conjunto de vectores $\{v_1, \ldots, v_n\}$ se dicen* **linealmente dependientes**, *si existen escalares $\lambda_1, \ldots, \lambda_n$ no todos nulos, tales que*

$$\lambda_1 v_1 + \cdots + \lambda_n v_n = 0$$

Caso contrario, diremos que el conjunto $\{v_1, \ldots, v_n\}$ es **linealmente independientes**.

Definición 10.2.6 *Sea V un espacio vectorial. Un conjunto de vectores $\{v_1, \ldots, v_n\}$ se llama* **base** *del espacio V, si satisface*

i) $V = \langle v_1, \ldots, v_n \rangle$

ii) Los vectores $v_1, \ldots, v_n$ son linealmente independientes.

La siguiente proposición del álgebra lineal es bien conocida.

Proposición 10.2.2 *Sea V un espacio vectorial y*

$$B = \{v_1, \ldots, v_n\} \qquad C = \{u_1, \ldots, u_m\}$$

dos bases de V. Entonces $m = n$.

Observación: De acuerdo a la proposición anterior podemos asignar a cada espacio vectorial un entero no negativo n, el cual llamamos **la dimensión del espacio** y que es igual al número de vectores de una base cualquiera de V. Por supuesto, nuestra definición de dimensión, no dependerá de la base elegida.

Usaremos la notación $dim(V)$ para indicar la dimensión de V.

Definición 10.2.7 *Sean V y V' dos espacios vectoriales sobre K. Una aplicación $\phi : V \longrightarrow V'$ se llama* **homomorfismo** *entre espacios vectoriales, si satisface*

i) Para v_1, v_2 en V

$$\phi(v_1 + v_2) = \phi(v_1) + \phi(v_2)$$

ii) Para $v \in V$ y $\lambda \in K$

$$\phi(\lambda v) = \lambda \phi(v)$$

Un homomorfismo entre espacios vectoriales, también se llama homomorfismo lineal o aplicación lineal.

Definición 10.2.8 *Dos espacios vectoriales V y V' se dicen* **isomorfos** *y lo denotamos por $V \approx V'$, si existen un homomorfismo $\phi : V \longrightarrow V'$, el cual es biyectivo.*

Definición 10.2.9 *Sean V y V' espacios vectoriales y $\phi : V \longrightarrow V'$ un homomorfismo. El conjunto de los elementos v de V tales que $\phi(v) = 0$, se denomina el* **Kernel o núcleo de** *ϕ y lo denotamos por* $\ker \phi$.

Observación: Es fácil verificar que $\ker \phi$ es un subespacio vectorial de V. Además ϕ es $1:1$ si y sólo si $\ker \phi = \{0\}$. Para hallar la dimensión del Kernel, usamos el siguiente teorema del álgebra lineal el cual es bien conocido.

Teorema 10.2.1 *Sea $\phi : V \longrightarrow V'$ un homomorfismo de espacios vectoriales. Entonces*

$$dim(\ker \phi) = \quad dimV - \quad dimV'$$

Ejercicios

1) Probar que el anillo $\mathbb{C}$ de los números complejos es un cuerpo.

2) Probar que todo cuerpo K es un espacio vectorial sobre K. ¿Cuál es la dimensión de este espacio?

3) Sea $V = \mathbb{R}^n = \mathbb{R} \times \cdots \times \mathbb{R}$ el conjunto de las n-uplas $(x_1, \ldots, x_n)$, con $x_i \in \mathbb{R}$. Definimos una suma en V, mediante

$$(x_1, \ldots, x_n) + (y_1, \ldots, y_n) = (x_1 + y_1, \ldots, x_n + y_n)$$

y el producto por un escalar $\lambda \in \mathbb{R}$:

$$\lambda(x_1, \ldots, x_n) = (\lambda x_1, \ldots, \lambda x_n)$$

Probar que V con estas dos operaciones es un espacio vectorial sobre $\mathbb{R}$. Halle una base para este espacio y determine su dimensión. El espacio V se denomina **espacio n-dimensional sobre $\mathbb{R}$.**

4) Sea $n = 3$ como en el ejercicio anterior. Determine cuáles de los siguientes conjuntos de vectores son linealmente independientes.

a) $(1,1,1),\ (1,1,0),\ (0,1,0)$
b) $(1,2,3),\ (1,0,1),\ (0,0,2)$
c) $(1,1,1),\ (1,1,2),\ (1,0,1)$
d) $(1,2,1),\ (0,\frac{1}{2},1),\ (1,0,0)$

5) Determine el Kernel del homomorfismo

$$\begin{array}{rcl} \phi:\ \mathbb{R}^3 & \longrightarrow & \mathbb{R} \\ (x,y,z) & \longrightarrow & x+y+z \end{array}$$

6) Sea K un cuerpo. Probar que $K[x]$ es un K-espacio vectorial de dimensión infinita.

7) Si V_1 y V_2 son dos subespacios de V, entonces la suma de V y V' se define por

$$V_1 + V_1' = \{v_1 + v_2 \mid v_1 \in V,\ v_2 \in V'\}$$

Probar que $V_1 + V_2$ es un subespacio de V.

8) Demostrar que

$$dim(V_1 + V_2) = dimV_1 + dimV_2 - dim(V_1 \cap V_2)$$

9) Sea W el subconjunto de $\mathbb{R}^3$, formado por los vectores (x,y,z), tales que

$$3x - 2y - z = 0$$

Probar que W es un subespacio de $\mathbb{R}^3$ de dimensión 2.

10) Demuestre que a cada aplicación lineal $\phi:\ \mathbb{R}^2 \longrightarrow \mathbb{R}^2$ se le puede asociar una matriz A_ϕ de orden 2×2 sobre $\mathbb{R}$.

11) Demuestre que la aplicación ϕ del ejercicio de arriba es inyectiva, si y sólo si la matriz A_ϕ es invertible.

12) Demuestre que el conjunto de aplicaciones lineales inyectivas de $\mathbb{R}^2$ en $\mathbb{R}^2$ es un grupo, el cual es isomorfo al grupo lineal $L_2(\mathbb{R})$ estudiado en el capítulo 1.

10.3 Extensiones de Cuerpos

Cuando estudiabamos las raíces de un polinomio $f(x)$ sobre un cuerpo $K[x]$, vimos que algunas de ellas estaban sobre otro cuerpo F, el cual contiene a K como subcuerpo. Esto sugiere entonces la necesidad de construir extensiones de cuerpos, como una técnica para poder resolver ciertas ecuaciones polinómicas.

El caso típico de una extensión del cuerpo $\mathcal{Q}$, consiste en un cuerpo de la forma $\mathcal{Q}(\alpha)$, donde α es raíz de un polinomio $p(x)$ irreducible en $\mathcal{Q}[x]$. Dichas extensiones son cuerpos que están dentro del cuerpo de los números complejos, y contienen a $\mathcal{Q}$ como subcuerpos. La forma de construirlos, depende del polinomio $p(x)$ y de la raíz α, y la extensión $\mathcal{Q}(\alpha)$ será un espacio vectorial sobre $\mathcal{Q}$.

Definición 10.3.1 *Un cuerpo F se dice una* **extensión** *de un cuerpo K, si $K \subseteq F$ y además K es un subcuerpo de F.*

Si F es una **extensión finita de** K, entonces se puede probar fácilmente que F es un espacio vectorial sobre K. Esto da origen a la siguiente

Definición 10.3.2 *Sea F una extensión de K. La dimensión de F como espacio vectorial sobre K, se denomina* **grado de la extensión** *de F sobre K, y se denota por $[F : K]$.*

Si el grado de la extensión F sobre K es finito, diremos que F es una **extensión** finita de K. Caso contrario diremos que F es una **extensión trascendente** de K.

Ejemplo 1: El cuerpo $\mathbb{C}$ de los números complejos es una extensión finita del cuerpo $\mathbb{R}$ de los números reales.

Ejemplo 2: El cuerpo $\mathbb{R}$ de los números reales es una extensión trascendente de $\mathcal{Q}$.

Definición 10.3.3 *Sea K un cuerpo y α un elemento en una extensión de K. Entonces el* **cuerpo engendrado por α sobre K,** *denotado por $K(\alpha)$, es igual a la intersección de todas las extensiones de K que contienen a α.*

Observación: Es claro que la definición de arriba tiene sentido, pues si α está en una extensión F, se tiene que $K(\alpha) \subseteq F$.

Por otro lado, es fácil probar que la intersección de cualquier número de cuerpos es un cuerpo.

Si K es un cuerpo, F una extensión de K y $\alpha \in F$, sea $K[\alpha]$ el subanillo de F formado por todas las expresiones polinomiales en K.

$$f(\alpha) = a_n\alpha^n + \cdots + a_1\alpha + a_0 \tag{10.1}$$

donde $a_i \in K$.

Entonces $K[\alpha]$ es un Dominio de Integridad que contiene a K y al elemento α.

El cuerpo de cociente de este Dominio de Integridad, formado por los cocientes de las expresiones del tipo (**??**), lo denotamos por U_α.

Es claro entonces que U_α es una extensión de K que contiene a α, y por lo tanto está contenido en $K(\alpha)$. Por otro lado, si L es una extensión de K que contiene a α, entonces debe contener todas las expresiones del tipo $a_n\alpha^n + \cdots + a_1\alpha + a_0$. Como L es un cuerpo, se tiene que L contiene todos los cocientes de dichas expresiones y por lo tanto L contiene a U_α. Luego U_α y $K(\alpha)$ son la misma cosa. Hemos demostrado entonces

Proposición 10.3.1 *Sea K un cuerpo y α un elemento en una extensión de K. Entonces $K(\alpha)$ consiste en todas las formas racionales*

$$\frac{f(\alpha)}{g(\alpha)}$$

donde $f(\alpha), g(\alpha)$ están en $K[\alpha]$ y $g(\alpha) \neq 0$

Definición 10.3.4 *Sea F una extensión de K. Un elemento $\alpha \in F$ se dice* **algebraico sobre** *K si α satisface una ecuación polinomial*

$$f(\alpha) = a_n\alpha^n + \cdots + a_1\alpha + a_0 = 0$$

con $a_i \in K$.

Observación: Si α es algebraico sobre K, entonces α puede ser raíz de muchos polinomios con coeficientes en K, y entonces el polinomio f en la definición anterior no es único.

Sin embargo hay un polinomio especial, entre los polinomios que anulan a α, que merece particular antención.

Definición 10.3.5 *Sea α algebraico sobre K. Entonces el* **polinomo minimal de** *α, es el polinomio mónico, de grado mínimo que anula a α.*

Observación: Si $f(x)$ es el polinomio minimal de α, entonces $f(x)$ es irreducible sobre $\mathcal{Q}$. Si $f(x)$ es reducible entonces $f(x) = p(x)q(x)$, y entonces ambos polinomios $p(x)$ y $q(x)$ son mónicos. Además alguno de ellos anula a α y esto contradice la minimalidad de $f(x)$.

Ejemplo: Sea $\alpha = 1 + \sqrt{2}$, el cual es algebraico sobre $\mathcal{Q}$. El polinomio minimal de α viene dado por:

$$f(x) = x^2 - 2x - 1$$

Definición 10.3.6 *Sea α algebraico sobre K. Entonces diremos que α es* **algebraico de grado** *n, si el grado del polinomio minimal de α es n.*

Teorema 10.3.1 *Sea α algebraico sobre K de grado n. Entonces el grado de $K(\alpha)$ sobre K es n.*

Demostración: Sea $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$ el polinomio minimal de α, el cual es irreducible, y consideremos el Dominio de Integridad $K[\alpha]$, formado por todas las expresiones del tipo:

$$b_m\alpha^m + \cdots + b_1\alpha + b_0$$

donde $b_i \in K$.

Notemos que α satisface el polinomio $f(x)$ y por lo tanto

$$\alpha^n = -(a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0$$

Esta última expresión, nos permite reducir toda potencia de α de grado n o superior, a una combinación lineal de los elementos $\alpha^{n-1}, \ldots, \alpha, 1$. Luego

$$K[\alpha] = \{b_{n-1}\alpha^{n-1} + \cdots + b_1\alpha + b_0 \cdot 1 \mid b_i \in K\}$$

Afirmamos además que $K[\alpha]$ es un cuerpo, para lo cual probaremos que todos los inversos de los elementos de $K[\alpha]$ están en $K[\alpha]$.

En efecto, sea $t = b_{n-1}\alpha^{n-1} + \cdots + b_1\alpha + b_0$ un elemento en $K[\alpha]$ distinto de cero. Entonces el polinomio $g(x) = b_{n-1}x^{n-1} + \cdots + b_1x + b_0$ es primo relativo con $f(x)$, pues $f(x)$ es irreducible y $f(x)$ no divide a $g(x)$. Luego existen polinomios $q(x)$ y $s(x)$ en $\mathcal{Q}[x]$, tales que

$$f(x)q(x) + g(x)s(x) = 1$$

Sustituyendo esta expresión en el valor de $x = \alpha$, tenemos

$$f(\alpha)q(\alpha) + g(\alpha)s(\alpha) = 1$$

Teniendo en cuenta que $f(\alpha) = 0$, se deduce

$$g(\alpha)s(\alpha) = 1$$

o sea

$$t \cdot s(\alpha) = 1$$

lo cual implica que $t^{-1} = s(\alpha) \in K[\alpha]$.

Por lo tanto, hemos probado que $k[\alpha]$ es un cuerpo y su cuerpo de cocientes es igual a si mismo. Por lo tanto $K(\alpha) = K[\alpha]$.

Para finalizar mostraremos que los elementos $1, \alpha, \ldots, \alpha^{n-1}$ es una base de $K(\alpha)$ sobre K. Para probar esto, sólo nos falta verificar que estos elementos son linealmente independientes.

Supongamos que

$$C_{n-1}\alpha^{n-1} + \cdots + C_1\alpha + C_0 \cdot 1 = 0$$

para algunos elementos $C_i \in K$.

Luego el polinomio $f'(x) = C_{n-1}x^{n-1} + \cdots + C_1x + C_0$ es de grado menor que el grado de $f(x)$ y además anula a α. Esto contradice la minimalidad de $f(x)$ y por lo tanto $C_{n-1} = C_{n-2} = \cdots = C_1 = C_0 = 0$.

Los elementos $\{1, \alpha, \ldots, \alpha^{n-1}\}$ forman una base de $K(\alpha)$ sobre K y por lo tanto

$$[K(\alpha) : K] = n$$

Con esto se da fin a la prueba.

♠

Teorema 10.3.2 *Sea K un cuerpo y $K(\alpha)$ una extensión finita de grado n. Entonces α es algebraico de grado n sobre K.*

Demostración: Consideremos los elementos $1, \alpha, \alpha^2, \ldots, \alpha^n$ en $F(\alpha)$. Puesto que la dimensión del espacio $K(\alpha)$ sobre K es n, estos $(n+1)$ elementos son linealmente independientes. Luego existen elementos $a_0, a_1, \ldots, a_n$ en K, no todos nulos, tales que

$$a_n\alpha^n + \cdots + a_1\alpha + a_0 \cdot 1 = 0$$

Luego α es algebraico sobre K. El grado del polinomio minimal de α es menor o igual a n. Si suponemos que el grado de este polinomio es

$m < n$, entonces por el teorema anterior se deduce $[K(\alpha) : K] = m < n$, lo cual es una contradicción. Luego α es algebraico de grado n.

♠

Nuestro próximo paso será probar que el conjunto de los elementos algebraicos sobre un cuerpo K, es un cuerpo. Antes necesitamos el siguiente resultado.

Proposición 10.3.2 *Sea K un cuerpo y F una extensión finita de K. Sea L una extensión finita de F. Entonces L es una extensión finita de K y además: $[L : K] = [L : F][F : K]$.*

Demostración: Sea $[F : K] = n$ y $[L : F] = m$. Sean $\{x_1, \ldots, x_n\}$ una base de F sobre K, y $\{y_1, \ldots, y_m\}$ una base de L sobre F.

Probaremos que $\{x_i y_j\}$ $1 \leq i \leq n$, $1 \leq j \leq m$, es una base de L sobre K.

Sea $l \in L$. Entonces existen elementos $l_1, \ldots, l_m$ en F, tal que

$$l = l_1 y_1 + \cdots + l_m y_m \tag{10.2}$$

Como los l_i están en F, para cada l_i existen elementos $k_{ij} \in K$, tales que

$$l_i = k_{i1} x_1 + \cdots + k_{in} x_n, \quad \text{para todo} \quad 1 \leq i \leq m \tag{10.3}$$

Sustituyendo estos valores de l_i en la expresión (**??**) obtenemos

$$l = k_{11} x_1 y_1 + \cdots + k_{m1} x_1 y_m + \cdots + k_{1n} x_n y_1 + \cdots + k_{mn} x_m y_n$$

Luego los elementos $\{x_i y_j\}$ son un conjunto de generadores de L sobre K.

Supongamos que para algunos elementos a_{ij} en K, $1 \leq i \leq n$, $1 \leq j \leq m$, no todos nulos, se tiene

$$(a_{11} x_1 y_1 + \cdots + a_{1m} x_1 y_m) + \cdots + (a_{n1} x_n y_1 + \cdots + a_{nm} x_n y_m) = 0$$

Luego reagrupamos estos elementos para obtener

$$(a_{11}x_1 + a_{21}x_2 + \cdots + a_{n1}x_n)y_1 + \cdots + (a_{1m}x_1 + \cdots + a_{nm}x_n)y_m = 0$$

Como $x_i \in F$ para todo $1 \leq i \leq n$ y $a_{ij} \in K \subseteq F$, se tiene que los elementos

$$C_j = a_{1j}x_1 + \cdots + a_{nj}x_n, \qquad 1 \leq j \leq m$$

están todos en F, pues F es un cuerpo.

Luego se tendrá la combinación lineal

$$C_1y_1 + \cdots + C_my_m = 0$$

Como los $y_1, \ldots, y_m$ son linealmente independientes sobre F, se deben anular todos los C_i. Por lo tanto

$$C_k = 0, \quad \text{para todo} \quad 1 \leq k \leq m$$

o sea

$$a_{1j}x_1 + \cdots + a_{nj}x_n = 0, \qquad 1 \leq j \leq m$$

Nótese que los a_{ij} están en K y los elementos $x_1, \ldots, x_n$ son linealmente independientes sobre K. Luego se deduce de esto que $a_{ij} = 0$ para todo $1 \leq i \leq n$, $1 \leq j \leq m$.

En conclusión hemos probado que el conjunto $\{x_iy_j\}$ constituye una base de L sobre K, la cual tiene $m.n$ elementos. Luego $[L : K] = m.n$. Con esto queda probado la proposición.

♠

Teorema 10.3.3 *Sea K un cuerpo, y F una extensión de K. Entonces el conjunto de elementos de F que son algebraicos sobre K es un subcuerpo de F.*

Demostración: Sea $\mathcal{A}$ el conjunto de los elementos de F que son algebraicos sobre K. Para probar que $\mathcal{A}$ es un cuerpo basta tomar un par de elementos cualquiera a y b en $\mathcal{A}$, y demostrar

i) $a \pm b$ está en $\mathcal{A}$
ii) ab está en $\mathcal{A}$
ii) a/b está en $\mathcal{A}$, si $b \neq 0$

Sea $T = K(a)$ y $L = T(b)$. Entonces $a \in L$ y $b \in L$. Por ser L un cuerpo se tiene que $a \pm b \in L$, $ab \in L$ y $a/b \in L$, si $b \neq 0$.

Luego $[K(a+b) : K] \leq [L : K] = [L : T][T : K]$

Ahora bien, como b es algebraico sobre K, de grado n, digamos, entonces b es algebraico sobre $K(a)$, de grado $\leq n$. Luego

$$[L : T] = [T(b) : K(a)] \leq n$$

Sabemos también que a es algebraico sobre K, de grado m digamos. Luego

$$[T : K] = [K(a) : K] = m$$

Por lo tanto

$$[K(a+b) : K] \leq m.n$$

Luego $K(a+b)$ es una extensión finita de K, y por el teorema **??**, se tiene que $a+b$ es algebraico sobre K. De igual forma se prueba que los elementos $a-b$, ab y a/b son algebraicos sobre K.

♠

Definición 10.3.7 *Una extensión F de K se dice* **extensión algebraica**, *si todos los elementos de F son algebraicos sobre K.*

Definición 10.3.8 *Un número complejo c se dice* **número algebraico**, *si c es algebraico sobre $\mathcal{Q}$. Caso contrario diremos que c es un* **número trascendente**.

El teorema **??** establece entonces, en el caso $k = \mathcal{Q}$, que el conjunto de los números algebraicos es un cuerpo. Este cuerpo está contenido en $\mathcal{C}$, pero es diferente de $\mathcal{C}$, pues existen números reales que no son algebraicos como por ejemplo π y e.

Si α es un elemento algebraico sobre $\mathcal{C}$, entonces α es raíz de algún polinomio con coeficientes complejos, y por el Teorema Fundamental del Algebra, se tiene que $\alpha \in \mathcal{C}$. Luego el cuerpo de los elementos algebraicos sobre $\mathcal{C}$ es precisamente $\mathcal{C}$.

Definición 10.3.9 *Un cuerpo F se dice* **algebraicamente cerrado** *si todo elemento algebraico sobre F, está en F.*

Podemos establecer entonces el siguiente resultado.

Teorema 10.3.4 *El cuerpo de los números complejos es algebraicamente cerrado.*

Ejercicios

1) Sea r un número racional, y supongamos que $\sqrt{r} \notin \mathcal{Q}$. Probar que

$$\mathcal{Q}(\sqrt{r}) = \{a + b\sqrt{r} \mid a, b \in \mathcal{Q}\}$$

es una extensión algebraica de $\mathcal{Q}$, de grado 2.

$\mathcal{Q}(\sqrt{r})$ se llama **cuerpo cuadrático** generado por $\sqrt{r}$.

2) Probar que todo cuerpo cuadrático es de la forma $\mathcal{Q}(\sqrt{d})$, donde d es un entero libre de cuadrados.

3) Si $s = a+b\sqrt{d} \in \mathcal{Q}(\sqrt{d})$, entonces **la traza y la norma** del elemento x, se definen por

$$\begin{aligned} Tr(s) &= s + \overline{s} = 2a \\ N(s) &= s.\overline{s} = a^2 - db^2 \end{aligned}$$

Probar que para cualquier par de elementos s y t en $\mathcal{Q}(\sqrt{d})$ se tiene

i) $Tr(s+t) = Tr(s) + Tr(t)$
ii) $N(s.t) = N(s)N(t)$

4) Un elemento s en $\mathcal{Q}(\sqrt{d})$ se denomina **entero algebraico**, si satisface un polinomio mónico con coeficientes en $\mathcal{Q}$.

Demuestre que s es un entero algebraico, si y sólo si $Tr(s)$ y $N(s)$ son enteros.

5) Demuestre que el conjunto de los enteros algebraicos de $\mathcal{Q}(\sqrt{d})$ es un anillo.

Bibliografía

[1] Redheffer R. M. *What! Another note just on the Fundamental Theorem of Algebra*. Math. Monthly vol. 71, p. 180-185, Feb. 1964.

[2] Zassenhauss, Hans. *On the Fundamental Thgeorem of Algebra*. Math. Monthly vol. 74, p. 485-497, Mayo 1967.

[3] Fefferman, Charles. *An easy proof of the Fundamental Theorem of Algebra*. The Am. Math. Monthly vol. 74, p. 854-855, 1967.

[4] Chrystal, G. (1898-1900). *Algebra, an elementary textbook*. 7 $\underline{\text{th}}$ ed. A. and C. Black, London. Repr. (1964) Chelsea, New York.

[5] Kuhn, H. W. (1974). *A new proof of the Fundamental Theorem of Algebra*. Mathematical Programming Studies 1, 148-158.

[6] Perron Oscar. *Algebra*. 3rd. edition, Berlin 1951.

[7] Rosenbloom P. C. *An elementary constructive proof of Fundamental Theorem of Algebra*. The American Math. Monthly vol. 53, (1946), 562-570.

[8] Courant R. & Robbins H. *¿Qué es la matemática?*. (1971) Aguilar-Madrid.

[9] O'connor J. J. & Robertson E. F. *"The Fundamental Theorem of Algebra"*, en el sitio web www.history.mcs.st-andrews.ac.uk.

[10] Stillwell John.*Mathematics and its history*. (1989)Springer-Verlag. New York.

[11] Rodríguez José. "Teoría Combinatoria" Primera Escuela Venezolana para la enseñanza de la Matemática. Kariña. Mérida Venezuela 1997.