ALGEBRA

Versión Preliminar

Renato A. Lewin

Indice

CAPITULO 1

Introducción a la Teoría de Números

La Teoría de Números, al menos originalmente, es la rama de la matemática que estudia las propiedades de los números naturales $1, 2, 3, \ldots$. A poco andar uno descubre que este estudio no se confina a dicho conjunto de números, ni siquiera al conjunto de los números enteros $\ldots, -3, -2, -1, 0, 1, 2, \ldots$, sino que muchas veces se debe recurrir a otros conjuntos de números, algebraicos, reales, complejos, etc. para resolver asuntos relacionados con los numeros naturales (y viceversa).

Algunos problemas clásicos de la Teoría de Números como el llamado último teorema de Fermat o el de la distribución de los números primos, (ver más adelante) han dado origen a grandes desarrollos de la matemática. Por ejemplo, al primero de estos se debe gran parte del desarrollo de los cuerpos ciclotómicos, al segundo todo el desarrollo de la función zeta de Riemann. Es así que en la Teoría de Números moderna se emplean sofisticadas teécnicas de análisis matemático y de teoría de probabilidades. Estudiaremos aquí tan sólo los rudimentos de esta disciplina y haremos algunos alcances acerca de su relación con la llamada álgebra abstracta.

1. Los Números Naturales y los Números Enteros

Comenzaremos nuestro estudio suponiendo que el lector está familiarizado con los conjuntos

$$\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, \ldots\} \text{ y}$$

$$\mathbb{N} = \{1, 2, 3, \ldots\},$$

de los números enteros y de los números naturales (o enteros positivos), respectivamente. En particular supondremos conocimiento de las operaciones de suma y multiplicación así como de la estructura de orden sobre estos conjuntos, por lo tanto, no daremos una definición axiomática de ellas.

La propiedad más importante de los números naturales es el siguiente principio:

PRINCIPIO DE BUEN ORDEN

Todo conjunto no vacío de números naturales tiene un menor elemento.

Decimos que $\mathbb{N}$ es un conjunto *Bien Ordenado*. Intuitivamente, este sencillo principio nos dice que siempre puedo encontrar el más pequeño número natural tal que ....., donde la línea de puntos puede ser llenada por cualquier propiedad (siempre que exista al menos un número natural que verifique dicha propiedad). Como consecuencia de esto, por ejemplo, podemos probar que todo número natural n tiene un (único) *sucesor*, o sea, el número que le sigue en el orden natural. (Esto ya lo sabemos: el sucesor de n es $n + 1$). Para demostrarlo, basta considerar el conjunto no vacío de los números naturales estrictamente mayores que n y aplicar el Principio de Buen Orden. El menor elemento de ese conjunto es el sucesor de n.

Cabe hacer notar que este menor elemento de un conjunto no vacío A cuya existencia garantiza el Principio es único ya que si hubiera dos, digamos a y b, entonces $a \leq b$, ya que a es el menor elemento de A y $b \in A$. Similarmente, $b \leq a$, por lo tanto $a = b$. Tampoco est de más recalcar que, a diferencia del infimo de un conjunto, que puede no pertenecer a él, el menor elemento de A pertenece a A.

Obsérvese que $\mathbb{Z}$ no verifica el Principio de Buen Orden: $\mathbb{Z}$ mismo (o los enteros menores que 8, o los enteros negativos, etc.) es un subconjunto no vacío de $\mathbb{Z}$ que no tiene un menor elemento. La propiedad de ser un conjunto bien ordenado no es exclusiva de los conjuntos de números enteros. Dado cualquier conjunto linealmente ordenado uno puede preguntarse si es bien ordenado o no. Ver ejercicios.

La segunda propiedad importante de los números naturales es:

PRINCIPIO DE INDUCCION

Sea P un conjunto de números naturales tal que:

i. $1 \in P$,

ii. si $k \in P$ entonces $k + 1 \in P$.

Entonces $P = \mathbb{N}$.

Intuitivamente, el Principio de Inducción corresponde al "Principio de Dominó": si cae el primero, cae el que le sigue y el que le sigue y el que le sigue..., por lo tanto caen todos.

Supondremos que el lector está familiarizado con este principio y sus aplicaciones. Aunque no lo usaremos mayormente en estas notas, es conveniente saber que ambos principios, el de Inducción y el de buen orden, son equivalentes.

Un resultado interesante es que los dos principios anteriores son equivalentes.

TEOREMA 1.1. *El Principio de Buen Orden implica el Principio de Inducción.*

DEMOSTRACIÓN. Sea P un conjunto de números naturales que verifica las hipótesis del Principio de Inducción. Sea A el conjunto de los números que no pertenecen a P. (Nos basta pues demostrar que A es vacío). Supongamos que A es no vacío. En virtud del Principio de Buen Orden, A tiene un menor elemento "a". a no puede ser 1 ya que por hipótesis, $1 \in P$. Luego $a-1$, el predecesor a, es un entero positivo que pertenece a P porque a es el más pequeño que *no* pertenece a P. Pero entonces, por la segunda parte de la hipótesis de inducción, $a = (a-1)+1 \in P$, lo que es una contradicción. Esta contradicción proviene de suponer que A es no vacío. Luego todos los enteros positivos pertenecen a P. □

Analogamente tenemos:

TEOREMA 1.2. *El Principio de Inducción implica el Principio de Buen Orden.*

DEMOSTRACIÓN. Ejercicio. □

EJERCICIOS 1.1.
(1) Sea $\mathbb{R}^+$ el conjunto de los números reales positivos ordenados en la forma habitual. ¿Es este un buen orden?
(2) Sea $A = \{n^2 : n \in \mathbb{Z}\}$, con el orden natural. ¿Es este un buen orden?
(3) Demuestre que no puede existir una cadena descendente infinita de enteros positivos.
(4) Demuestre el teorema 1.2.

2. Divisibilidad

DEFINICIÓN 1.1. Sean a y b dos enteros con $a \neq b$. Decimos que a *divide* a b si existe un entero n tal que $na = b$. También decimos que b es un *múltiplo* de a. Denotamos este hecho por $a \mid b$. Si a no divide a b escribiremos $a \nmid b$.

TEOREMA 1.3. *Si a, b y c son enteros, entonces:*
(1) *Si $a \mid b$ y $b \mid c$, entonces $a \mid c$.*
(2) *Si $a \mid b$ y $a \mid c$, entonces $a \mid mb + nc$, para cualquier par de enteros m, n.*
(3) *Si $a \mid b$ y $b \neq 0$, entonces $0 < |a| \leq |b|$.*
(4) *Si $a \mid b$ y $b \mid a$, entonces $a = \pm b$.*

DEMOSTRACIÓN.
(3) $b = ma \neq 0$, luego $a \neq 0$ y $m \neq 0$. Por lo tanto, $|a| \geq 1, |m| \geq 1$ y $|b| = |ma| = |m||a| \geq 1\,|a| \geq 1 > 0$.

(4) Si $b = 0$, entonces $a = nb = n0 = 0$, luego $a = \pm b$. Si $b \neq 0$, como $a \mid b$, por (3), $0 < |a| \leq |b|$. Analogamente, $0 < |b| \leq |a|$. Luego $|a| = |b|$ y $a = \pm b$. □

El teorema más importante sobre divisibilidad es:

TEOREMA 1.4. **El Algoritmo de la División.**
Sean a y b dos enteros, $b > 0$. Entonces existen dos enteros q y r tales que $a = bq + r$ y $0 \leq r < |b|$. Los enteros q y r son únicos.

DEMOSTRACIÓN. Si a es un múltiplo de b, $a = bq + 0$ y el teorema se cumple, luego podemos suponer que a no es un múltiplo de b. Consideremos el conjunto

$$A = \{a - bn : n \in \mathbb{Z} \text{ y } a - bn \geq 0\}.$$

Como $a \geq -|a| \geq -|a|b$, tenemos $a + |a|b \geq 0$, luego

$$a - (-|a|)b \geq 0,$$

o sea, A es un conjunto no vacío de enteros positivos. Obsérvese que $0 \notin A$ ya que a no es un múltiplo de b.

Por el principio de Buen Orden, A debe tener un menor elemento. Llamémoslo r. Quiere decir que existe un entero q tal que $r = a - bq$, i.e., $a = bq + r$.

Supongamos que $r \geq b$. Entonces $r - b = a - bq - b = a - b(q + 1) \geq 0$, luego $r - b \in A$ y $0 \leq r - b < r$, contradiciendo la minimalidad de r. Por lo tanto $0 \leq r < b$. ($r = 0$ si y sólo si a es un múltiplo de b).

Finalmente, para probar la unicidad de q y r, supongamos que existen q' y r' tales que $a = bq' + r'$ y $0 \leq r' < b$. Entonces $bq - bq' + r - r' = 0$, luego $b(q - q') = r' - r$, o sea, $b \mid (r' - r)$. Por Teorema 1.3(3), si $r \neq r'$, $|r' - r| \geq |b| = b > 0$. Pero esto es imposible ya que $-b < r' - r < b$. Luego $r = r'$. Pero entonces $b(q - q') = 0$ y $b \neq 0$, luego $q = q'$.

□

DEFINICIÓN 1.2.

(1) Un entero positivo $p \neq 1$ se dice *primo* si sus únicos divisores son ± 1 y $\pm p$.
(2) Sean a, b dos enteros no ambos nulos. El mayor entero que divide tanto a a como a b se llama el *máximo común divisor* de a y b. El máximo común divisor de a y b se denota (a, b) (o bien M.C.D.(a, b)).
    Similarmente definimos $(a_1, a_2, \ldots, a_n)$ el máximo común divisor de $a_1, a_2, \ldots, a_n$, como el mayor entero que divide a todos esos números.
(3) Dos enteros se dicen *primos relativos* si su máximo común divisor es 1.

A priori no es obvio que el máximo común divisor de dos números deba existir, sin embargo esto es consecuencia inmediata del próximo teorema.

TEOREMA 1.5. *Dados dos enteros a y b, su máximo común divisor (a, b) es el menor entero positivo que se puede escribir como suma de multiplos de a y de b.*

DEMOSTRACIÓN. Consideremos el conjunto $A = \{ma + nb : m, n \in \mathbb{Z} \text{ y } ma + nb > 0\}$. A no es vacío ya que $0 < |a| = \pm 1a + 0b \in A$. Por el Principio de Buen Orden, A tiene un menor elemento, al que llamaremos d. Obsérvese que $d > 0$. Como $d \in A$, existen m, n enteros tales que $d = ma + nb$. Debemos verificar que éste es el máximo común divisor de a y b.

Por el algoritmo de la división, $a = qd + r$, con $0 \leq r < d$. Entonces,

$$r = a - qd = a - q(ma + nb) = (1 - mq)a - nqb.$$

Si $r > 0$, entonces $r \in A$, pero $r < d$, lo que contradice la minimalidad de d. Por lo tanto $r = 0$ y $d \mid a$.

Análogamente podemos demostrar que $d \mid b$, por lo tanto d es un divisor común de a y de b.

Para verificar que d es el mayor divisor común, sea $s \geq 1$ otro divisor común. Por el Teorema 1.3(2), $s \mid ma + nb$, para cualquier $m, n \in \mathbb{Z}$, en particular, $s \mid d$, luego $0 < s \leq d$. □

COROLARIO 1.6. *El máximo común divisor de $a_1, a_2, \ldots, a_n$ es el menor entero positivo que puede escribirse como suma de múltiplos de los números $a_1, a_2, \ldots, a_n$.*

OBSERVACIÓN 1.1.

(1) a y b son relativamente primos si y sólo si existen $m, n \in \mathbb{Z}$ tales que $1 = ma + nb$.
(2) El máximo común divisor de $a_1, a_2, \ldots, a_n$ divide a $a_1, a_2, \ldots, a_n$. Si $s \mid a_1$, $s \mid a_2, \ldots, s \mid a_n$, entonces $s \mid (a_1, a_2, \ldots, a_n)$.

COROLARIO 1.7. *Si $a_1, a_2, \ldots, a_n$ son enteros, entonces*

$$(a_1, a_2, \ldots, a_n) = ((a_1, a_2, \ldots, a_{n-1}), a_n).$$

DEMOSTRACIÓN. Sea $d = (a_1, a_2, \ldots, a_n)$. Por la observación anterior, $d \mid a_1$, $d \mid a_2, \ldots, d \mid a_n$, luego $d \mid (a_1, a_2, \ldots, a_{n-1})$ y también $d \mid a_n$, por lo tanto $d \mid ((a_1, a_2, \ldots, a_{n-1}), a_n)$.

A la inversa, $((a_1, a_2, \ldots, a_{n-1}), a_n)$ es divisor común de $(a_1, a_2, \ldots, a_{n-1})$ y de a_n, luego $((a_1, a_2, \ldots, a_{n-1}), a_n) \mid d$. Como ambos son positivos, por 1.3(4), son iguales. □

COROLARIO 1.8. *Si $d = (a, b)$, entonces $(\frac{a}{d}, \frac{b}{d}) = 1$. (I.e. $\frac{a}{d}$ y $\frac{b}{d}$ son relativamente primos. ¡ Obsérvese que ($\frac{a}{d}$ y $\frac{b}{d}$) son enteros!).*

COROLARIO 1.9. *Si $(a, b) = 1$ y $a \mid bc$, entonces $a \mid c$.*

DEMOSTRACIÓN. Si $a \mid bc$, entonces $bc = ak$ para algún k, y como $1 = ma + nb$, multiplicando ambos miembros por c,

$$c = mac + nbc = mac + nak = a(mc + nk).$$

□

COROLARIO 1.10. *Si p es un número primo, $p \mid bc$ y $p \nmid b$, entonces $p \mid c$.*

COROLARIO 1.11. *Si $a = bq + r$ y $b \neq 0$, entonces $(a, b) = (b, r)$.*

DEMOSTRACIÓN. $(a, b) = ma + nb = m(bq + r) + nb = (mq + n)b + mr$, es decir, (a, b) es una suma de múltiplos de b y de r, luego por el teorema 1.5, $(a, b) \mid (b, r)$.
De una manera similar demostramos que $(b, r) \mid (a, b)$. □

2.1. El Algoritmo de Euclides.

Existe un método para calcular el máximo común divisor de dos números, tal método se denomina el *Algoritmo de Euclides*.

Sean a y b dos números no ambos nulos, digamos, $b \neq 0$. Entonces, por el algoritmo de la división, existen q y r tales que $a = bq + r$, con $0 \leq r < |b|$.

Si $r = 0$, entonces $b \mid a$, $(a, b) = |b|$ y hemos terminado.

Si $r > 0$, entonces existen q_1 y r_1 tales que $b = rq_1 + r_1$, con $0 \leq r_1 < r$.

Si $r_1 = 0$, entonces $(b, r) = r$ y por el Corolario 1.11, $(a, b) = r$ y nuevamente hemos terminado.

Si $r_1 > 0$, entonces existen q_2 y r_2 tales que $r = r_1 q_2 + r_2$ y $0 \leq r_2 < r_1$.

Este proceso se puede continuar indefinidamente de tal manera que en cada paso, si obtenemos un resto cero, nos detenemos y si no, aplicamos el algoritmo de la división una vez más. Es importante notar que en cada aplicación del algoritmo de la división, el resto obtenido es estrictamente menor que el de la aplicación precedente. Vale decir, tenemos $r > r_1 > r_2 > \cdots > r_n > \cdots \geq 0$.

Por el Principio de Buen Orden (ver Ejercicios), tiene que existir un n tal que $r_n = 0$, ya que si no, habría una cadena descendente infinita. Pero entonces, $r_{n-1} \mid r_{n-2}$ en cuyo caso $(r_{n-2}, r_{n-1}) = r_{n-1}$ y aplicando el Corolario 1.11 varias veces,

$$(a, b) = (r, r_1) = (r_1, r_2) = \cdots = (r_{n-2}, r_{n-1}) = r_{n-1}.$$

Vale decir, el máximo común divisor de a y de b es el resto inmediatamente anterior al resto que se anula.

Ejemplo: Calculemos el máximo común divisor de 454 y 136.

$$\begin{aligned} 454 &= 136 \cdot 3 + 46 \\ 136 &= 46 \cdot 2 + 44 \\ 46 &= 44 \cdot 1 + 2 \\ 44 &= 2 \cdot 22 + 0 \end{aligned}$$

Es decir, el máximo común divisor de 454 y 136 es 2.

Para calcular el máximo común divisor de tres o más números, aplicamos el Teorema 1.7 y el algoritmo de Euclides.

DEFINICIÓN 1.3. El *mínimo común múltiplo* de dos enteros no nulos a y b es el menor entero positivo que es múltiplo de a y de b. Se le denotará por $[a, b]$ (o bien por m.c.m.(a, b)

Como en el caso del máximo común divisor, el mínimo común múltiplo de dos números siempre existe. En este caso, en virtud del Principio de Buen Orden.

TEOREMA 1.12. *Si m es un múltiplo común de a y de b, entonces $[a, b] \mid m$.*

DEMOSTRACIÓN. Por el algoritmo de la división, $m = [a, b]q + r$, con $0 \leq r < [a, b]$. Pero $a \mid m$ y $a \mid [a, b]$, luego $a \mid r = m - [a, b]q$.

Similarmente, $b \mid r$, o sea, r es un múltiplo común de a y de b y $0 \leq r < [a, b]$. Si $r > 0$, r sería el mínimo común múltiplo de a y de b y no lo es. Por lo tanto $r = 0$ y $[a, b] \mid m$. □

TEOREMA 1.13. *Si a y b son enteros no nulos,*

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

DEMOSTRACIÓN. Sean $d = (a, b)$ y $m = [a, b]$. Entonces

$$\frac{|ab|}{d} = \frac{|a|}{d}|b| = |a|\frac{|b|}{d},$$

o sea $\frac{|ab|}{d}$ es un múltiplo de a y de b, luego $m \mid \frac{|ab|}{(a,b)}$.

Por otra parte, $|ab|$ es un múltiplo común de a y b, luego $m \mid |ab|$ y, en particular, $\frac{|ab|}{m}$ es un entero.

Ahora bien, $m = ka$, luego

$$k\frac{|ab|}{m} = \frac{k|a|}{m}|b| = \pm b,$$

o sea,

$$\frac{|ab|}{m} \mid b.$$

Analogamente, $\frac{|ab|}{m} \mid a$. Es decir, $\frac{|ab|}{m}$ es divisor comun de a y de b, luego $\frac{|ab|}{m} \mid d$ y $\frac{|ab|}{m} \leq d$. Por lo tanto $\frac{|ab|}{d} = m$. □

El siguiente teorema conocido también como teorema de factorización única, es la piedra angular de toda la teoría de números.

TEOREMA 1.14. **El Teorema Fundamental de la Aritmética.**
Todo número entero mayor que 1 *o bien es un número primo o bien se puede factorizar como producto de números primos. Más aún, tal factorización es única salvo por el orden de los factores.*

DEMOSTRACIÓN. Supongamos que el teorema no es cierto, es decir, existe un entero positivo mayor que 1 que no es primo y que no se descompone como producto de primos. Sea n el más pequeño tal número. Este debe existir por el Principio de Buen Orden.

Como n no es primo, debe tener divisores no triviales. Sea $n = ab$, donde a y b son distintos de ± 1 y de $\pm n$. Sin pérdida de generalidad podemos suponer que a y b son positivos. Ademas sabemos que $a < n$ y $b < n$. Pero entonces, como n es minimal para la propiedad indicada, tanto a como b son o bien primos, o bien producto de primos y por lo tanto n es producto de números primos, contradiciendo la suposición original. Luego ésta es falsa.

Para demostrar la unicidad de la descomposición, sea n ahora el menor entero positivo tal que la factorización no es única. Es decir,

$$n = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s,$$

donde $p_1, p_2, \ldots, p_r, q_1, q_2, \ldots, q_s$ son números primos. Entonces $p_1 | q_1 q_2 \cdots q_s$ y por el Corolario 1.10, para algún j, $1 \leq j \leq s$, $p_1 | q_j$. Pero como ambos son primos, $p_1 = q_j$. Podemos suponer (reordenando) que $j = 1$, luego

$$n' = p_2 p_3 \cdots p_r = q_2 q_3 \cdots q_s,$$

pero $n' < n$, luego n' verifica la condición de unicidad de la factorización, por lo tanto $r = s$ y, reordenando, $p_i = q_i$, para $1 \leq i \leq r$, por lo tanto la descomposición de n es única. □

OBSERVACIÓN 1.2. Obviamente no todos los primos que aparecen en la descomposición de un número tienen que ser distintos. En general todo entero positivo n se puede escribir como

$$n = p_1^{k_1} p_2^{k_2} \cdots p_m^{k_m},$$

donde los p_k son primos, los k_i son enteros positivos. k_i suele llamarse la *multiplicidad* de p_i en la descomposición de n.

El siguiente corolario es uno de los más famosos y hermosos resultados de Euclides.

COROLARIO 1.15. *Existen infinitos números primos.*

DEMOSTRACIÓN. Supongamos que existe solamente una cantidad finita de primos p_1, p_2, ... , p_n. Consideremos ahora el número

$$m = p_1 p_2 \cdots p_n + 1.$$

Obviamente m es mayor que todos los primos, luego no es primo. Por otra parte, m no es divisible por p_1, ni por p_2, ..., ni por p_n, o sea, m no es divisible por ningún primo. Pero por el teorema 1.14, m debe ser divisible por algún primo, lo cual es una contradicción. □

Este teorema tiene muchas aplicaciones, la más elemental es probablemente el algoritmo para calcular máximo común divisor y mínimo común múltiplo de dos o más números:

El máximo común divisor de dos números es el producto de todos los primos (considerando su multiplicidad) que se repiten en la factorización de ambos números.

El mínimo común múltiplo de dos números es el producto de las máximas potencias de cada primo que aparece en la descomposición de alguno de los números.

Ejemplo

Calcular el máximo común divisor y el mínimo común múltiplo de 48 y 180.

Como $48 = 2^4 \cdot 3$ y $180 = 2^2 \cdot 3^2 \cdot 5$,

$$(48, 180) = 2^2 \cdot 3 = 12 \text{ y } [48, 180] = 2^4 \cdot 3^2 \cdot 5 = 720.$$

Como sabemos, este algoritmo puede generalizarse a cualquier cantidad de números.

Podemos dar una fórmula general para calcular el máximo común divisor y el mínimo común múltiplo de dos números basada en la descomposición en números primos. Sean

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k},$$
$$m = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k},$$

donde $0 \leq \alpha_i$ y $0 \leq \beta_i$, para $1 \leq i \leq k$. Obsérvese que si $\alpha_i = 0$, entonces el primo p_i no aparece en la descomposición de n, y algo análogo ocurre con m. Entonces

$$(n, m) = p_1^{min\{\alpha_1,\beta_1\}} p_2^{min\{\alpha_2,\beta_2\}} \cdots p_k^{min\{\alpha_k,\beta_k\}},$$
$$[n, m] = p_1^{max\{\alpha_1,\beta_1\}} p_2^{max\{\alpha_2,\beta_2\}} \cdots p_k^{max\{\alpha_k,\beta_k\}}.$$

Ejercicios 1.2.

(1) Demuestre que el mínimo común múltiplo de dos números siempre existe.

(2) Demuestre que si $(a, m) = 1$ y $(b, m) = 1$, entonces $(ab, m) = 1$.

(3) Demuestre o de un contraejemplo
   (a) Si $a \mid a + b$, entonces $a \mid b$.
   (b) Si $a \mid bc$, entonces $a \mid b$ o bien $a \mid c$.
   (c) Si $a^2 \mid b^2$, entonces $a \mid b$.
   (d) Si $a \mid b^2$, entonces $a^2 \mid b^2$.
   (e) Si $d = (a, b)$, $a \mid c$ y $b \mid c$, entonces $ab \mid dc$.

(4) Demuestre los criterios de divisibilidad que aprendió en el colegio. Recordemos que si un entero se escribe en notación decimal como

$$a_n a_{n-1} \cdots a_2 a_1 a_0,$$

a_0 es su *dígito de las unidades*, a_1 es su *dígito de las decenas*, etc.
   (a) Un número es divisible por 2 si $2 \mid a_0$.

(b) Un número es divisible por 3 si la suma de sus dígitos es divisible por 3.
(c) Un número es divisible por 4 si $4 \mid a_1a_0$. También es divisible por 4 si $4 \mid 2a_1 + a_0$.
(d) Un número es divisible por 5 si su dígito de las unidades es 5 o 0.
(e) Un número es divisible por 6 si es divisible por 2 y por 3.
(f) Un número es divisible por 7 si

$$a_2a_1a_0 - a_5a_4a_3 + a_8a_7a_6 - \cdots$$

es divisible por 7.
(g) Un número es divisible por 8 si $8 \mid a_2a_1a_0$. También es divisible por 8 si $8 \mid 4a_2 + 2a_1 + a_0$.
(h) Un número es divisible por 9 si la suma de sus dígitos es divisible por 9.
(i) Un número es divisible por 11 si

$$a_2a_1a_0 - a_5a_4a_3 + a_8a_7a_6 - \cdots$$

es divisible por 11.

(5) Invente criterios de divisibilidad para otros números mas grandes.
(6) Demuestre que el cuadrado de cualquier número entero puede tener la forma $3k$ o bien $3k + 1$, pero no puede tener la forma $3k + 2$.
(7) Demuestre que no existen enteros a y b tales que $(a, b) = 7$ y $2a + b = 50$.
(8) Probar que si a y b son impares, entonces $a^2 + b^2$ no puede ser un cuadrado perfecto.
(9) Demuestre que hay infinitos enteros de la forma $5^n - 1$ que son divisibles por 7.
(10) Demuestre que si $(a, b) = 1$, entonces $(a + b, ab) = 1$.
(11) Demuestre el teorema **??**.

3. Congruencias

En esta sección estudiaremos una importante relacion definida sobre el conjunto de los números enteros. Esta relación tiene numerosas aplicaciones y sirve para introducir varios conceptos algebraicos.

Definición 1.4. Sea m un entero positivo. Decimos que *a es congruente con b módulo m* si y sólo si $m \mid a - b$.

Denotaremos este hecho por $a \equiv b \pmod{m}$.

Teorema 1.16. *La relación de congruencia módulo m es una relación de equivalencia.*

Demostración. Ejercicio. □

TEOREMA 1.17. *Si* $a \equiv b \pmod{m}$ *y* $c \equiv d \pmod{m}$, *entonces*

$$\begin{aligned} a+c &\equiv b+d \pmod{m}, \\ ac &\equiv bd \pmod{m} \text{ and} \\ -a &\equiv -b \pmod{m}. \end{aligned}$$

DEMOSTRACIÓN. Ejercicio. □

OBSERVACIÓN 1.3.

(1) Si $m = 1$, entonces $a \equiv b \pmod{1}$ para todo a y todo b.
(2) La ley de cancelación para la suma es válida para congruencias, es decir, si $a + c \equiv b + c \pmod{m}$, entonces $a \equiv b \pmod{m}$.
(3) La ley de cancelación para el producto no es válida para congruencias como lo demuestra el ejemplo siguiente:
$5 \cdot 6 \equiv 3 \cdot 6 \pmod{12}$, pero $5 \not\equiv 3 \pmod{12}$.

TEOREMA 1.18. *Si* $ab \equiv ac \pmod{m}$ *y* $d = (a, m)$, *entonces* $b \equiv c \pmod{\frac{m}{d}}$.

DEMOSTRACIÓN. Como $(a, m) = d$, existen r y s tales que $a = rd$ y $m = sd$, donde $(r, s) = 1$.

Por otra parte, como $ab \equiv ac \pmod{m}$, $a(b - c) = ab - ac = km$, para algún $k \in \mathbb{Z}$. Luego $rd(b - c) = ksd$ y cancelando d, $s \mid r(b - c)$, y por el Corolario 1.9, $s \mid b - c$, o sea, $b - c = ts = t\frac{m}{d}$, vale decir, $b \equiv c \pmod{\frac{m}{d}}$. □

Si bien la ley de cancelación no es siempre válida para congruencias, el siguiente corolario inmediato del teorema anterior nos indica cuándo se puede cancelar.

COROLARIO 1.19. *Supongamos* $(a, m) = 1$. *Si* $ab \equiv ac \pmod{m}$, *entonces* $b \equiv c \pmod{m}$.

3.1. Ecuaciones.

TEOREMA 1.20. *La ecuación* $ax \equiv b \pmod{m}$ *tiene solución si y solamente si* $(a, m) \mid b$.

DEMOSTRACIÓN. Si $ax \equiv b \pmod{m}$ tiene solución, existen enteros x e y tales que $ax - b = my$, luego $b = ax - my$, es decir, b es suma de múltiplos de a y de m, por lo tanto, $(a, m) \mid b$.

Por otra parte, si $(a, m) \mid b$, para algún k, $b = k(a, m)$. Ahora bien, como $(a, m) = ra + sm$, para ciertos enteros r y s, $b = k(a, m) = (kr)a + (ks)m$. Luego kr es solución de la ecuación $ax \equiv b \pmod{m}$. □

Obsérvese que la solución a la ecuación $ax \equiv b \pmod{m}$ nunca es única ya que si x_0 es una solución, entonces para cualquier k, $x_0 + km$ también lo es.

Ejemplo

Consideremos la ecuación $42x \equiv 50 \pmod{76}$.

$$\begin{aligned} 42x &\equiv 50 \pmod{76} \\ 2 \cdot 21x &\equiv 2 \cdot 25 \pmod{76} \\ 21x &\equiv 25 \pmod{38} \\ 21x &\equiv 25 + 38 \pmod{38} \\ 21x &\equiv 63 \pmod{38} \\ 21x &\equiv 21 \cdot 3 \pmod{38} \\ x &\equiv 3 \pmod{38}. \end{aligned}$$

Es decir, las soluciones de la ecuación $42x \equiv 50 \pmod{76}$ son todos los enteros $\{\cdots, -73, -35, 3, 41, 79, \cdots\}$. Estas se pueden expresar en términos de el módulo original 76. En efecto, como las soluciones obedecen la fórmula $x = 3 + 38k$, separando en dos casos si k es par o si k es impar, tenemos $x = 3+38 \cdot 2n = 3+76n$ y $x = 3 + 38(2n + 1) = 41 + 76n$. Obsérvese que $41 \not\equiv 3 \pmod{76}$.

Recordando que una ecuación de primer grado en los enteros (o los racionales o los reales) tiene, a lo más una solución, la pregunta obvia es ¿Cuántas soluciones no congruentes entre si puede tener una ecuación en congruencias?

Consideremos la ecuación $ax \equiv b \pmod{m}$ y sea x_0 una solución. Si x es otra solución, entonces $ax \equiv ax_0 \equiv b \pmod{m}$, luego por el Teorema 1.18

$$x \equiv x_0 \pmod{\frac{m}{d}},$$

donde $d = (a, m)$. Es decir, $x = x_0 + t\frac{m}{d}$, o sea, x pertenece al conjunto

$$\{\cdots, x_0 - 2\frac{m}{d}, x_0 - \frac{m}{d}, x_0, x_0 + \frac{m}{d}, x_0 + 2\frac{m}{d}, \cdots, x_0 + (d-1)\frac{m}{d}, x_0 + m, \cdots\}.$$

¿Cuántas de estas soluciones son "distintas", en el sentido de no ser congruentes mdulo m entre sí?

Observemos que $x_0 + m \equiv x_0 \pmod{m}$. De la misma manera, $x_0 - \frac{m}{d} \equiv x_0 + (d-1)\frac{m}{d} \pmod{m}$, etc.

Es claro que cualquier solución de la ecuación será congruente $\pmod{m}$ con uno de los enteros

$$x_0, x_0 + \frac{m}{d}, x_0 + 2\frac{m}{d}, \cdots x_0 + (d-1)\frac{m}{d}.$$

No resulta difícil ver que ninguno de estos números es congruente $\pmod{m}$ con otro porque las diferencias entre ellos son todas menores que m. Decimos que el conjunto anterior es un *conjunto completo de representantes* de las soluciones de $ax \equiv b \pmod{m}$.

En los párrafos anteriores hemos demostrado el siguiente teorema:

TEOREMA 1.21. *Si $(a, m) \mid b$, la ecuación $ax \equiv b \pmod{m}$ tiene (a, m) soluciones no congruentes entre si.*

Ejemplo

Consideremos la ecuación $68x \equiv 100 \pmod{120}$. Entonces

$$\begin{aligned} 68x &\equiv 100 + 2 \cdot 120 \pmod{120} \\ 68x &\equiv 340 \pmod{120} \text{ y como } (68, 120) = 4, \\ x &\equiv 5 \pmod{30}. \end{aligned}$$

Por lo tanto $\{5, 35, 65, 95\}$ es un conjunto completo de representantes de las soluciones de $68x \equiv 100 \pmod{120}$.

Dijimos antes que la relación de congruencia módulo m es una relación de equivalencia. Las clases de equivalencia de esta relación juegan un papel muy importante, sobre todo en las conecciones con el álgebra. Es fácil ver que existirá exactamente m clases de equivalencia módulo m, ya que para cualquier entero n, por el algoritmo de la división, $n = qm + r$, luego $n \equiv r \pmod{m}$, para algún $r = 0, 1, \cdots, m-1$. Por lo tanto existen m clases distintas.

3.2. Sistemas de Congruencias.

Consideremos el siguiente problema.

En algún lugar del sur de Chile vive un pastor, que cuida de su piño de ovejas con singular dedicación. Cierto día, acertó a pasar por este lugar un funcionario municipal, quien tenía por misión averiguar la cantidad exacta de ovejas de este pastor. Este es (resumidamente) el diálogo que tuvo lugar:

—Y, ¿Cuántas ovejas tiene Ud.?

—Bueno, mire, en realidad no sé. Fíjese que yo aprendí a contar hasta cinco no más. Lo que sí le puedo decir es que si cuento las ovejas de tres en tres, me sobran dos; si las cuento de cuatro en cuatro, me sobra una, y si las cuento de cinco en cinco, me sobran tres.

El funcionario miró someramente el piño de ovejas y decidió que en ningún caso éste tenía más de cien ovejas. Hecho esto, se dió por satisfecho. ¿Cómo pudo el funcionario averiguar cuántas ovejas formaban el piño?

Supongamos que el número de ovejas es x.

"si cuento las ovejas de tres en tres, me sobran dos". O sea, $x \equiv 2 \pmod{3}$.

"si cuento las ovejas de cuatro en cuatro, me sobra una". O sea,
$x \equiv 1 \pmod{4}$.

"si cuento las ovejas de cinco en cinco, me sobran tres". O sea, $x \equiv 3 \pmod{5}$.

Se trata entonces de encontrar un número x que verifique las tres congruencias:

$$\begin{aligned} x &\equiv 2 \pmod{3} \\ x &\equiv 1 \pmod{4} \\ x &\equiv 3 \pmod{5}, \end{aligned}$$

además x debe ser menor que 100.

Este tipo de problema recibe el nombre de *sistema de congruencias* y en esta sección veremos métodos para resolverlos.

Veamos primero dos ejemplos algo más sencillos que el de nuestro funcionario. Queremos solucionar el siguiente problema, encontrar un número x que satisfaga las dos ecuaciones:

$$\begin{aligned} x &\equiv 3 \pmod 7 \\ 5x &\equiv 7 \pmod{12}. \end{aligned}$$

Sea x_0 una solución. Entonces $x_0 = 3+7s$, para algún s, por ser x_0 solución de la primera ecuación. Entonces, reemplazando en la segunda ecuación,

$$\begin{aligned} 5(3+7s) &\equiv 7 \pmod{12} \\ 35s &\equiv -8 \pmod{12} \\ 35s &\equiv -8+288 \pmod{12} \\ 35s &\equiv 280 \pmod{12} \\ s &\equiv 8 \pmod{12}. \end{aligned}$$

Esto es, $s = 8+12t$, para algún t, luego $x_0 = 3+7(8+12t)$, o bien, $x_0 = 59+84t$, es decir, toda solución del sistema anterior es congruente con 59 $\pmod{84}$.

Veamos ahora un segundo ejemplo. Consideremos el sistema:

$$\begin{aligned} x &\equiv 2 \pmod 4 \\ x &\equiv 5 \pmod 6). \end{aligned}$$

y procedamos como en el ejemplo anterior. Sea x_0 una solución del sistema.

$$\begin{aligned} x_0 = 2+4s &\equiv 5 \pmod 6 \\ 4s &\equiv 3 \pmod 6), \end{aligned}$$

por lo tanto $4s = 3+6t$, para algún t, lo que es claramente imposible. Luego este sistema no tiene solución. Obsérvese que el punto importante aquí es que no podemos cancelar el 4, ya que $(4,6) \not| 3$.

¿Cuáles sistemas tienen solución y cuáles no la tienen?

Teorema 1.22. *El sistema*

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \end{aligned}$$

tiene solución si y solamente si $(m_1, m_2) \mid a_1 - a_2$.

Si x_0 *es una solución, entonces toda solución es congruente con* x_0 *módulo* $[m_1, m_2]$.

DEMOSTRACIÓN. x_0 es solución del sistema si y sólo si existe un entero s tal que $x_0 = a_1 + sm_1 \equiv a_2 \pmod{m_2}$ si y sólo si existe un entero s tal que $sm_1 \equiv a_2 - a_1 \pmod{m_2}$.

Tal s existe si y sólo si $(m_1, m_2) \mid a_2 - a_1$.

Supongamos ahora que $(m_1, m_2) \mid a_2 - a_1$ y que x_0 es una solución del sistema. Entonces si x es una solución,

$$x \equiv a_1 \equiv x_0 \pmod{m_1}$$

$$x \equiv a_2 \equiv x_0 \pmod{m_2},$$

luego $m_1 \mid x - x_0$ y $m_2 \mid x - x_0$, o sea, $x - x_0$ es un múltiplo común de m_1 y de m_2, luego $[m_1, m_2] \mid x - x_0$, por lo tanto $x \equiv x_0 \pmod{[m_1, m_2]}$. □

Uno de los más famosos teoremas de la Teoría de Números es el siguiente:

TEOREMA 1.23. **Teorema Chino del Resto**
Si $(m_i, m_j) = 1$, para $i \neq j$, $i, j \leq k$, entonces el sistema de congruencias

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_2 \pmod{m_k} \end{aligned}$$

tiene solución. Dos soluciones son congruentes $\pmod{m_1 \cdot m_2 \cdots m_k}$.

DEMOSTRACIÓN. La demostración del teorema nos proporciona un método que nos permite calcular las soluciones del sistema.

Observemos que si $M = m_1 \cdot m_2 \cdots m_k$, entonces para todo $j \leq k$, $(\frac{M}{m_j}, m_j) = 1$. Por lo tanto, existen enteros α_j y β_j tales que $1 = \alpha_j \frac{M}{m_j} + \beta_j m_j$, es decir, $\alpha_j \frac{M}{m_j} \equiv 1 \pmod{m_j}$.

Consideremos ahora

$$x_0 = a_1\alpha_1\frac{M}{m_1} + a_2\alpha_2\frac{M}{m_2} + \cdots + a_k\alpha_k\frac{M}{m_k}.$$

La segunda observación es que $\frac{M}{m_j}$ es múltiplo de m_i, para $i \neq j$, así, por ejemplo,

$$x_0 \equiv a_1\alpha_1\frac{M}{m_1} \pmod{m_1},$$

pero como $\alpha_1 \frac{M}{m_1} \equiv 1 \pmod{m_1}$,

$$a_1\alpha_1\frac{M}{m_1} \equiv a_1 \pmod{m_1},$$

luego $x_0 \equiv a_1 \pmod{m_1}$.

En forma análoga se obtiene que $x_0 \equiv a_i \ (\mod m_i)$, para todo $i \leq k$, o sea, x_0 es una solución del sistema.

La demostración de que dos soluciones son congruentes $(\mod m_1 \cdot m_2 \cdots m_k)$ es análoga a la de la última parte del teorema 1.22 y se deja como ejercicio. □

Ejemplo.

Encontremos la solución al problema de las ovejas y el funcionario.

$$\begin{aligned} x &\equiv 2 \ (\mod 3) \\ x &\equiv 1 \ (\mod 4) \\ x &\equiv 3 \ (\mod 5). \end{aligned}$$

En este caso, $M = 3 \cdot 4 \cdot 5 = 60$. $\frac{M}{m_1} = 20$, $\frac{M}{m_2} = 15$ y $\frac{M}{m_3} = 12$. Como

$$\begin{aligned} 2 \cdot 20 &\equiv 1 \ (\mod 3) \\ 3 \cdot 15 &\equiv 1 \ (\mod 4) \\ 3 \cdot 12 &\equiv 1 \ (\mod 5). \end{aligned}$$

$\alpha_1 = 2$, $\alpha_2 = 3$ y $\alpha_3 = 3$, luego

$$x_0 = 2 \cdot 2 \cdot 20 + 3 \cdot 15 + 3 \cdot 3 \cdot 12 \ (\mod 60)$$

o sea,

$$x_0 \equiv 233 \equiv 53 \ (\mod 60),$$

por lo tanto el piño tenía 53 ovejas.

EJERCICIOS 1.3.

(1) Demuestre el Teorema[1.16].
(2) Demuestre el Teorema[1.17].
(3) Encuentre todas las soluciones de las ecuaciones

$$3x \equiv 1 \ (\mod 4) \tag{1}$$
$$4x \equiv 2 \ (\mod 6) \tag{2}$$
$$3(x-8) \equiv 18 - x \ (\mod 10) \tag{3}$$

(4) Demuestre que si $13 \nmid a$ y $13 \nmid b$, entonces $a^{12} \equiv b^{12} \ (\mod 13)$.
(5) Demuestre que si a y b son primos relativos con 91, entonces $a^{12} - b^{12}$ es divisible por 91.
(6) Si de un canasto se saca huevos de a dos, de a tres y de a cinco, sobran uno, dos y tres, respectivamente. ¿Cuántos huevos había en el canasto?
(7) Para una fiesta se compraron paquetes de papas fritas a 39 pesos y paquetes de galletas a 47 pesos, gastándose un total de 4151 pesos. ¿Cuántos paquetes de cada producto se compraron?
(8) Demuestre el teorema **??**.

4. Clases Residuales

Estudiaremos ahora las clases de equivalencia definidas en $\mathbb{Z}$ por la relacion de congruencia módulo m. A estas clases a menudo se les denomina *clases residuales*. ¿Cuántas clases de equivalencia hay? ¿Qué aspecto tienen?

Comencemos con un ejemplo, el caso $m = 4$? ¿Cuál es la clase de equivalencia del entero n? Es fácil, son todos aquellos números enteros x tales que $n - x$ es divisible por 4. Si designamos por $\underline{n}$ la clase residual de n entonces

$$\begin{aligned}
\underline{0} &= \{\ldots, -8, -4, 0, 4, 8, \ldots\} \\
\underline{1} &= \{\ldots, -7, -3, 1, 5, 9, \ldots\} \\
\underline{2} &= \{\ldots, -6, -2, 2, 6, 10, \ldots\} \\
\underline{3} &= \{\ldots, -5, -1, 3, 7, 11, \ldots\}
\end{aligned}$$

Sabemos que las clases de equivalencia forman una partición del conjunto, por lo tanto no hay más clases residuales que las anteriores, ya que $\{\underline{0}, \underline{1}, \underline{2}, \underline{3}\}$ es una partición. Así por ejemplo, $\underline{47} = \underline{-1} = \underline{3}$.

En general, hay m clases residuales módulo m. En efecto, por el algoritmo de la división, dado cualquier entero n, $n = qm + r$, o sea, $n \equiv r \pmod{m}$, o lo que es lo mismo, $\underline{n} = \underline{r}$. Pero como sabemos que el resto o residuo (de ahí el nombre de clase residual) $0 \leq r < m$, tenemos sólo m clases residuales distintas, a saber,

$$\{\underline{0}, \underline{1}, \underline{2}, \ldots, \underline{m-1}\}.$$

Al conjunto $\{0, 1, 2, \ldots, m-1\}$ se le llama *conjunto completo de representantes* ya que contiene un elemento de cada clase residual. En general cualquier conjunto de m números tal que ningún par de ellos es congruente modulo m, es un conjunto completo de representantes.

Volvamos a nuestro ejemplo. Observemos que si tomamos por ejemplo cualquier elemento de $\underline{1}$ y lo sumamos a cualquier elemento de, digamos, $\underline{2}$ obtenemos un elemento de $\underline{3}$. Algo parecido ocurre con todas las combinaciones de clases: el resultado no depende del representante que usemos. Lo mismo ocurre si multiplicamos representantes. Este hecho no es fortuito ni una característica de las clases residuales módulo cuatro como lo establecimos en el teorema 1.17. Este resultado nos permite definir operaciones de suma multiplicación sobre el conjunto de todas las clases residuales módulo m, para cualquier m, como sigue:

Definición 1.5. Si $\underline{a}$ y $\underline{b}$ son dos clases residuales módulo m, definimos:

$$\begin{aligned}
\underline{a} \oplus \underline{b} &= \underline{a+b} \\
\underline{a} \otimes \underline{b} &= \underline{ab} \\
\ominus \underline{a} &= \underline{-a}
\end{aligned}$$

Hemos usado un símbolo nuevo para las operaciones de suma, multiplicación y diferencia de clases residuales para enfatizar el hecho de que estas son operaciones distintas de las correspondientes en los números enteros. Más adelante eliminaremos el círculo y usaremos el mismo símbolo para la suma de clases residuales y la suma de enteros. De la misma manera, cuando no haya riesgo de confusión, escribiremos n por la clase residual $\underline{n}$.

EJEMPLOS 1.1. (1) Consideremos las clases residuales módulo 2. Hay dos clases $\underline{0}$ y $\underline{1}$, (constituidas por los números pares y por los números impares, respectivamente). Podemos hacer tablas de las operaciones entre estas clases.

$\oplus$	$\underline{0}$	$\underline{1}$
$\underline{0}$	$\underline{0}$	$\underline{1}$
$\underline{1}$	$\underline{1}$	$\underline{0}$

$\otimes$	$\underline{0}$	$\underline{1}$
$\underline{0}$	$\underline{0}$	$\underline{0}$
$\underline{1}$	$\underline{0}$	$\underline{1}$

x	$\ominus x$
$\underline{0}$	$\underline{0}$
$\underline{1}$	$\underline{1}$

(2) Las operaciones para las clases módulo 3 son:

$\oplus$	$\underline{0}$	$\underline{1}$	$\underline{2}$
$\underline{0}$	$\underline{0}$	$\underline{1}$	$\underline{2}$
$\underline{1}$	$\underline{1}$	$\underline{2}$	$\underline{0}$
$\underline{2}$	$\underline{2}$	$\underline{0}$	$\underline{1}$

$\otimes$	$\underline{0}$	$\underline{1}$	$\underline{2}$
$\underline{0}$	$\underline{0}$	$\underline{0}$	$\underline{0}$
$\underline{1}$	$\underline{0}$	$\underline{1}$	$\underline{2}$
$\underline{2}$	$\underline{0}$	$\underline{2}$	$\underline{1}$

x	$\ominus x$
$\underline{0}$	$\underline{0}$
$\underline{1}$	$\underline{2}$
$\underline{2}$	$\underline{1}$

(3) Las operaciones para las clases módulo 4 son:

$\oplus$	$\underline{0}$	$\underline{1}$	$\underline{2}$	$\underline{3}$
$\underline{0}$	$\underline{0}$	$\underline{1}$	$\underline{2}$	$\underline{3}$
$\underline{1}$	$\underline{1}$	$\underline{2}$	$\underline{3}$	$\underline{0}$
$\underline{2}$	$\underline{2}$	$\underline{3}$	$\underline{0}$	$\underline{1}$
$\underline{3}$	$\underline{3}$	$\underline{0}$	$\underline{1}$	$\underline{2}$

$\otimes$	$\underline{0}$	$\underline{1}$	$\underline{2}$	$\underline{3}$
$\underline{0}$	$\underline{0}$	$\underline{0}$	$\underline{0}$	$\underline{0}$
$\underline{1}$	$\underline{0}$	$\underline{1}$	$\underline{2}$	$\underline{3}$
$\underline{2}$	$\underline{0}$	$\underline{2}$	$\underline{0}$	$\underline{2}$
$\underline{3}$	$\underline{0}$	$\underline{3}$	$\underline{2}$	$\underline{1}$

x	$\ominus x$
$\underline{0}$	$\underline{0}$
$\underline{1}$	$\underline{3}$
$\underline{2}$	$\underline{2}$
$\underline{3}$	$\underline{1}$

DEFINICIÓN 1.6. Elconjunto de todas las clases residuales módulo m, dotado de la s operaciones $\oplus$ y $\otimes$ lo denotaremos por $\mathbb{Z}_m$.

Es inmediato que las operaciones sobre $\mathbb{Z}_m$ heredan de $\mathbb{Z}$ algunas propiedades. Por ejemplo, al igual que la suma y la multiplicación entre números enteros, estas operaciones son asociativas y conmutativas, es decir, para cualquier clases $\underline{a}, \underline{b}, \underline{c}$.

$$\begin{aligned}
(\underline{a} \oplus \underline{b}) \oplus \underline{c} &= \underline{a} \oplus (\underline{b} \oplus \underline{c}) \\
(\underline{a} \otimes \underline{b}) \otimes \underline{c} &= \underline{a} \otimes (\underline{b} \otimes \underline{c}) \\
\underline{a} \oplus \underline{b} &= \underline{b} \oplus \underline{a} \\
\underline{a} \otimes \underline{b} &= \underline{b} \otimes \underline{a}
\end{aligned}$$

y también

$$(\underline{a} \oplus \underline{b}) \otimes \underline{c} = (\underline{a} \otimes \underline{c}) \oplus (\underline{b} \otimes \underline{c})$$

¿Será válida la ley de cancelación para clases residuales? O sea, si $\underline{a} \neq \underline{0}$ y $\underline{a} \otimes \underline{b} = \underline{a} \otimes \underline{c}$, ¿es cierto que $\underline{b} = \underline{c}$?

Veámoslo en $\mathbb{Z}_3$. Si $\underline{a} = \underline{1}$, entonces

$$\underline{b} \ = \underline{a} \otimes \underline{b} = \underline{a} \otimes \underline{c} = \underline{c}.$$

Si $\underline{a} = \underline{2}$, entonces como $\underline{a} \otimes \underline{b} = \underline{2b}$, basta comprobar que $\underline{2b} = \underline{1}$ ssi $\underline{b} = \underline{2}$ y $\underline{2b} = \underline{2}$ ssi $\underline{b} = \underline{1}$, para verificar que también puedo cancelar.

Esto puede fácilmente verificarse con la tabla de multiplicación anterior ya que no hay ninguna línea (o columna) en la que una misma clase se repite.

Si verificamos la tabla de multiplicación de $\mathbb{Z}_4$ en cambio, vemos que en la tercera fila se repite la clase residual $\underline{2}$ y tenemos que

$$\underline{2} \otimes \underline{1} = \underline{2} = \underline{2} \otimes \underline{3},$$

luego en $\mathbb{Z}_4$ no podemos cancelar.

La pregunta natural entonces es ¿Cuándo podemos cancelar y cuándo no podemos? Notemos que $x \otimes y = x \otimes z$ si y sólo si $x \otimes (y \ominus z) = \underline{0}$, luego $\otimes$ verifica la ley de cancelación si sólo si no existen clases residuales a y b tales que $a \otimes b = \underline{0}$. Esto motiva una definición importante.

Definición 1.7. Dos clases residuales x e y no nulas (o sea distintas de $\underline{0}$,) son divisores del cero si y sólo si $x \otimes y = \underline{0}$.

Observación 1.4. Podemos hacernos la misma pregunta respecto de los enteros, ¿existirán divisores del cero en $\mathbb{Z}$? Bien sabemos que no.

Entonces, dado m, existirán divisores del cero si y sólo si existen enteros a y b tales que $\underline{a} \otimes \underline{b} = \underline{ab} = \underline{0}$, es decir, $ab \equiv 0 \pmod{m}$, o sea, $m \mid ab$.

Teorema 1.24. *En $\mathbb{Z}_n$ hay divisores del cero si y sólo si n no es primo.*

Demostración. Si n es primo y $\underline{a}$, $\underline{b}$ son clases no nulas tales que $\underline{a} \otimes \underline{b} = \underline{0}$, como vimos antes, $n \mid ab$, pero n es primo, luego $n \mid a$ o bien $n \mid b$, pero entonces $\underline{a} = \underline{0}$ o bien $\underline{b} = \underline{0}$, en cualquier caso, una contradicción. Luego si n es primo, no hay divisores del cero.

Si n no es primo, entonces existen enteros a y b tales que $n = ab$. Pero entonces $\underline{a} \otimes \underline{b} = \underline{ab} = \underline{n} = \underline{0}$, es decir, hay divisores del cero. □

Corolario 1.25. *La multiplicacion en $\mathbb{Z}_n$ verifica la ley de cancelación si y sólo si n es primo.*

El teorema anterior nos indica para qué clases residuales puedo cancelar *cualquier* factor no nulo, sin embargo es fácil ver de la tabla de $\mathbb{Z}_4$ que aunque no podemos cancelar un factor $\underline{2}$, si podemos cancelar un factor $\underline{3}$. Dado n, ¿qué factores podemos cancelar?

Teorema 1.26. *Si $(a, n) = 1$, entonces $\underline{a} \otimes \underline{b} = \underline{a} \otimes \underline{c} \ \Rightarrow \ \underline{b} = \underline{c}$*

Demostración. Es consecuencia inmediata del corolario 1.19. □

Observemos ahora que si $(a, n) = 1$, existen enteros b y c tales que $ba + cn = 1$, o lo que es lo mismo, $ba \equiv 1 \pmod{n}$, o bien $\underline{b} \otimes \underline{a} = \underline{ba} = \underline{1}$, es decir, la clase $\underline{a}$ tiene un *inverso multiplicativo*.

DEFINICIÓN 1.8. Una clase $\underline{a}$ de $\mathbb{Z}_n$ es una *unidad* si y sólo si existe una clase $\underline{b}$ de $\mathbb{Z}_n$ tal que $\underline{a} \otimes \underline{b} = \underline{1}$.

OBSERVACIÓN 1.5. De manera análoga, podemos preguntarnos cuáles son las unidades de $\mathbb{Z}$. Es claro que solamente 1 y -1 son unidades de $\mathbb{Z}$.

Para cada n entonces, las unidades de $\mathbb{Z}_n$ son precisamente aquellas clases que son "primas relativas con" n, vale decir, todos sus elementos son primos relativos con n. Como sabemos, los enteros menores que n constituyen un conjunto completo de representantes de las clases residuales. Un conjunto de representantes de las unidades de $\mathbb{Z}_n$ se llama un *conjunto reducido de representantes*. En otras palabras, un conjunto reducido contiene un representante de cada clase que es una unidad de $\mathbb{Z}_n$. De lo anterior se deduce entonces que

$$\{k : 0 < k < n \text{ y } (k, n) = 1\}$$

es un sistema reducido de representantes para $\mathbb{Z}_n$.

Resulta interesante entonces saber el número de elementos de un conjunto reducido de representantes, o lo que es lo mismo, el número de enteros menores que n que son primos relativos con n. Este número tiene muchas aplicaciones interesantes.

DEFINICIÓN 1.9. Para todo entero positivo n, definimos

$$\varphi(n) = \sharp\{m : 0 < m < n \text{ y } (m, n) = 1\}.$$

φ se llama la *función de Euler*.

Ejemplos

$$\begin{array}{rcll} \varphi(12) & = & \sharp\{1,5,7,11\} & = 4 \\ \varphi(6) & = & \sharp\{1,5\} & = 2 \\ \varphi(7) & = & \sharp\{1,2,3,4,5,6\} & = 6 \\ \varphi(p) & = & \sharp\{1,2,\ldots,p-1\} & = p-1, \end{array}$$

para p primo.

TEOREMA 1.27.

(1) *Si p es primo, entonces $\varphi(p^n) = p^n - p^{n-1}$.*
(2) *Si $(m, n) = 1$, entonces $\varphi(mn) = \varphi(m)\varphi(n)$.*

DEMOSTRACIÓN. 1) Observemos que los números que no son primos relativos con p^n son los múltiplos de p. Como sólo nos interesan aquellos menores o iguales que p^n, hay p^{n-1} de ellos. Por lo tanto hay $p^n - p^{n-1}$ números menores que p^n que son primos relativos con éste.

2) Sean

$$r_1, r_2, \ldots, r_{\varphi(m)} \text{ y } s_1, s_2, \ldots, s_{\varphi(n)}$$

los residuos reducidos módulo m y módulo n, respectivamente.

Sea x un residuo módulo mn, primo relativo con mn, es decir, $(x, mn) = 1$. Luego $(x, m) = 1$ y $(x, n) = 1$, o sea,

$$x \equiv r_i \pmod{m},$$

$$x \equiv s_j \pmod{n},$$

para algún $i \leq \varphi(m)$ y $j \leq \varphi(n)$. Entonces, por el Teorema Chino del Resto, existe una solución t_{ij} para este sistema, la que es única módulo mn. Es claro también que para cada i y j hay una solución distinta y que $(t_{ij}, mn) = 1$, por lo tanto hay exactamente $\varphi(m)\varphi(n)$ de estos t_{ij}, lo que termina la demostración. □

COROLARIO 1.28. *Si $n = p_1^{k_1} p_2^{k_2} \cdots p_m^{k_m}$, donde $p_1, \ldots, p_m$ son primos, entonces* $\varphi(n) = n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \cdots (1 - \frac{1}{p_m})$.

TEOREMA 1.29. **Euler–Fermat**
Si m es un entero positivo y $(a, m) = 1$, entonces

$$a^{\varphi(m)} \equiv 1 \pmod{m}.$$

DEMOSTRACIÓN. Sean $r_1, r_2, \ldots, r_{\varphi(m)}$ todos los residuos módulo m, que son primos relativos con m, o sea, que son un conjunto reducido de representantes. Entonces $ar_1, ar_2, \ldots, ar_{\varphi(m)}$ también son primos relativos con m, (ver ejercicio 3e).

Si $ar_i \equiv ar_j \pmod{m}$, para $i \neq j$, como $(a, m) = 1$, puedo cancelar a, obteniendo $r_i \equiv r_j \pmod{m}$, lo que es una contradicción. Luego los ar_1, ar_2, ..., $ar_{\varphi(m)}$ son todos distintos, por lo tanto también son un conjunto reducido de representantes. Pero entonces, para cada i, existe un único j tal que $ar_i \equiv r_j \pmod{m}$ y por lo tanto

$$ar_1 ar_2 \cdots ar_{\varphi(m)} \equiv r_1 r_2 \cdots r_{\varphi(m)} \pmod{m},$$

luego

$$a^{\varphi(m)} r_1 r_2 \cdots r_{\varphi(m)} \equiv r_1 r_2 \cdots r_{\varphi(m)} \pmod{m}.$$

Cancelando los r_i, obtenemos el resultado requerido. □

Un caso particular de este teorema es el llamado Pequeño Teorema de Fermat.

COROLARIO 1.30. **Teorema de Fermat**
Sea p un número primo y a un entero tal que $p \nmid a$. Entonces

$$a^{p-1} \equiv 1 \pmod{p}.$$

EJEMPLOS 1.2. Aplicaciones del Teorema de Fermat.

(1) Calcule $3^{1000} \pmod{7}$.

Por el teorema de Fermat, $3^6 \equiv 1 \pmod{7}$, luego $3^{6k} \equiv 1 \pmod{7}$, para cualquer k, por lo tanto,

$$\begin{aligned} 3^{1000} = 3^{6\cdot 166+4} &\equiv 3^4 \ (\mod 7) \\ 3^{1000} &\equiv 81 \ (\mod 7) \\ 3^{1000} &\equiv 4 \ (\mod 7) \end{aligned}$$

(2) Calcule $5^{100}(\mod 8)$.

Como $\varphi(8) = 4$, por el teorema de Euler–Fermat,

$$5^{100} = 5^{4\cdot 25} \equiv 1 \ (\mod 8).$$

(3) Si p es primo, $(a \pm b)^p \equiv a^p \pm b^p \ (\mod p)$.

Por el teorema del binomio, sabemos que

$$(a+b)^p = \sum_{k=0}^{p} \left(\begin{array}{c} p \\ k \end{array} \right) a^{p-k} b^k,$$

donde

$$\left(\begin{array}{c} p \\ k \end{array} \right) = \frac{p(p-1)\cdots(p-k+1)}{k!(p-k)!}.$$

Observemos que p aparece en la descomposición en primos del numerador pero no en la del denominador, luego p no puede cancelarse, es decir, aparece en la descomposición de $\left(\begin{array}{c} p \\ k \end{array} \right)$, o sea, $p \mid \left(\begin{array}{c} p \\ k \end{array} \right)$, para cada $k \neq 0, p$. Pero entonces

$$\left(\begin{array}{c} p \\ k \end{array} \right) \equiv 0 \ (\mod p),$$

para $1 \leq k < p$, de donde se obtiene el resultado pedido.

Ejercicios 1.4.

(1) Encuentre la intersección de la clase del 7 módulo 4 y la clase del 5 módulo 15.

(2) Demuestre que si n es impar, $\underline{0} + \underline{1} + \cdots + \underline{n-1} = \underline{0}$.

¿Que sucede si n es par?

(3)

Teorema 1.31. **Teorema de Wilson** *Sea p un número primo. Entonces*

$$(p-1)! \equiv -1 \ (\mod p).$$

CAPITULO 2

Polinomios

En este capítulo estudiaremos las propiedades algebraicas de los polinomios en una variable. No desarrollaremos aquí una teoría formal de polinomios sino que, como en el caso de los números enteros, recurriremos a los conocimientos más o menos intuitivos que tenemos sobre estos desde la escuela secundaria o de cursos de álgebra elemental. Para un tratamiento más formal y riguroso, el lector puede consultar por ejemplo [**2**]. Supondremos entonces que estamos familiarizados con los conceptos de polinomio y las operaciones habituales entre ellos, suma, resta, producto etc.

El propósito de este capítulo es hacer un paralelo entre las propiedades de las operaciones con polinomios y las operaciones entre números enteros. Nos concentraremos en polinomios con coeficientes racionales, aunque también veremos algunos teoremas importantes sobre polinomios con coeficientes enteros. Sólo ocasionalmente mencionaremos polinomios con coeficientes reales, complejos o, incluso, clases residuales en $\mathbb{Z}_n$.

1. Polinomios sobre los Racionales y los Enteros

Definición 2.1.

(1) El conjunto de los *polinomios sobre* $\mathbb{Q}$ (o de los polinomios con coeficientes en $\mathbb{Q}$), denotado $\mathbb{Q}[x]$, es el conjunto de todas las expresiones

$$a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0,$$

donde n es un entero positivo o cero y $a_0, a_1, \ldots, a_n \in \mathbb{Q}$.

Los racionales a_i se llaman los *coeficientes* del polinomio. El polinomio 0, es decir, aquel cuyos coeficientes son todos cero, se llama el *polinomio nulo*. Los polinomios tales que todos sus coeficientes salvo a_0 son cero se llaman *polinomios constantes*.

(2) El *grado* de un polinomio $p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$, es el mayor k tal que $a_k \neq 0$. Al polinomio nulo no se le asigna un grado. El grado de $p(x)$ se denota por $\partial p(x)$.

De manera análoga a la anterior, podemos definir polinomios sobre $\mathbb{Z}$, $\mathbb{R}$, $\mathbb{Z}_n$, etc., los que denotaremos respectivamente $\mathbb{Z}[x]$, $\mathbb{R}[x]$, $\mathbb{Z}_n[x]$.

Recordemos que dos polinomios $p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$ y $q(x) = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_0$ son iguales siempre y cuando $n = m$ y todos los coeficientes respectivos sean iguales. Así mismo, las operaciones se definen como sigue:

$$p(x) + q(x) = (a_n + b_n)x^n + (a_{n-1} + b_{n-1})x^{n-1} + \cdots + (a_0 + b_0),$$

aquí si $n > m$ hacemos $b_k = 0$ para $m \leq k \leq n$, y similarmente si $m > n$.

$$p(x) \cdot q(x) = c_l x^l + c_{l-1}x^{l-1} + \cdots + c_0,$$

donde

$$c_k = \sum_{i+j=k} a_i b_j = a_k b_0 + a_{k-1}b_1 + \cdots + a_0 b_k,$$

para $k \leq l = n + m$.

Lema 2.1.

(1) *Si* $p(x) + q(x) \neq 0$, *entonces* $\partial(p(x) + q(x)) \leq max\{\partial p(x), \partial q(x)\}$.
(2) *Si* $p(x)\ q(x) \neq 0$, *entonces* $\partial(p(x)\ q(x)) = \partial p(x) + \partial q(x)$.

De la definición de las operaciones, se desprende que el polinomio nulo 0 actua sobre los polinomios igual que el número 0 sobre los enteros, vale decir, si lo sumamos a cualquier polinomio $p(x)$, la suma es igual a este último. Por otra parte, si lo multiplicamos por un polinomio, obtenemos 0. Es decir, el polinomio nulo actua como un elemento neutro con respecto a la suma.

Algo similar se puede decir del polinomio 1, es decir aquel cuyos coeficientes son todos 0, salvo a_0 que es 1. Si lo multiplicamos por cualquier polinomio $p(x)$, el resultado será este último. Es decir tiene el mismo comportamiento que el entero 1.

Si consideramos ahora el polinomio

$$-p(x) = -a_n x^n - a_{n-1}x^{n-1} - \cdots - a_0,$$

notaremos que $p(x) + -p(x) = -p(x) + p(x) = 0$, o sea, $-p(x)$ es el equivalente del inverso aditivo de los números enteros.

Por último, podemos observar que las operaciones entre polinomios tienen otras de las propiedades de las operaciones entre enteros: tanto suma como multiplicación son asociativas y conmutativas, además, la segunda es distributiva respecto de la primera.

2. Divisibilidad

Ya que contamos con una multiplicación tan parecida a la de los números enteros, es natural preguntarse hasta donde podemos repetir las ideas sobre divisibilidad que desarrollamos en el capítulo anterior. Como bien sabemos, podemos usar

la misma definición para divisibilidad entre polinomios que la usada para números enteros.

DEFINICIÓN 2.2. Sean $p(x)$ y $q(x)$ dos polinomios. Decimos que $p(x)$ *divide* a $q(x)$ si existe un polinomio $r(x)$ tal que $p(x)\ r(x) = q(x)$. También decimos que $q(x)$ es un *múltiplo* de $p(x)$. Denotamos este hecho por $p(x) \mid q(x)$.

Ejemplo:
$x + 1 \mid x^2 - 1$, ya que $(x + 1)(x - 1) = x^2 - 1$.

Otras propiedades de $\mathbb{Q}[x]$ y sus operaciones que son similares a las de los enteros y de las clases residuales son:

TEOREMA 2.2.

(1) *En $\mathbb{Q}[x]$ no hay divisores del cero.*
(2) *La multiplicación en $\mathbb{Q}[x]$ verifica la ley de cancelación.*
(3) *Las unidades de $\mathbb{Q}[x]$ son los polinomios constantes no nulos.*

DEMOSTRACIÓN.

(1) Si $p(x) \neq 0$ y $q(x) \neq 0$, entonces $\partial(p(x)\ q(x)) = \partial p(x) + \partial q(x) \geq 0$.
(2) Esto es consecuencia inmediata de 1).
(3) Si $p(x)q(x) = 1$, entonces, en particular, $0 = \partial(p(x)\ q(x)) = \partial p(x) + \partial q(x)$.
Luego $\partial p(x) = \partial q(x) = 0$, o sea, las unidades de $\mathbb{Q}[x]$ son polinomios constantes no nulos.
Por otra parte, si $\partial p(x) = 0$, $p(x) = a_0 \neq 0$. Si tomamos $q(x) = \frac{1}{a_0}$, tendremos $p(x)q(x) = 1$, o sea, todo polinomio constante no nulo es una unidad de $\mathbb{Q}[x]$.

□

Obsérvese que el teorema también es cierto para $\mathbb{R}[x]$, sin embargo, sólo las dos primeras son ciertas para $\mathbb{Z}[x]$. Aquí las unidades son sólo los polinomios constantes 1 y -1.

¿Cuáles de estas propiedades serán ciertas en $\mathbb{Z}_5[x]$? ¿En $\mathbb{Z}_6[x]$?

TEOREMA 2.3. **Algoritmo de la División**
Sean $f(x)$ y $g(x)$ polinomios en $\mathbb{Q}[x]$ y $\partial g(x) \geq 1$. Entonces existen dos únicos polinomios $q(x)$ y $r(x)$ tales que

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

y

$$r(x) = 0 \quad ó \quad \partial r(x) < \partial g(x).$$

DEMOSTRACIÓN. Consideremos el conjunto

$$S = \{f(x) - p(x)g(x) : p(x) \in \mathbb{Q}[x]\}.$$

Si $0 \in S$, entonces $g(x) \mid f(x)$ y el teorema se cumple con $r(x) = 0$. En caso contrario, los grados de los polinomios de S son un conjunto no vacío de enteros positivos o 0. Este conjunto debe tener un menor elemento, luego existe un polinomio $r(x) \in S$ que tiene grado minimal y tal que

$$r(x) = f(x) - q(x)g(x),$$

para algún polinomio $q(x)$, o lo que es lo mismo,

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

Supongamos que $r(x) \neq 0$. Debemos demostrar ahora que $\partial r(x) < \partial g(x)$.

Para una demostración por contradicción, sean

$$r(x) = c_m x^m + c_{m-1}x^{m-1} + \cdots + c_0,$$

$$g(x) = b^n x^n + b_{n-1}x^{n-1} + \cdots + b_0,$$

con $c_m \neq 0$ y $b_n \neq 0$ y supongamos que $m \geq n$.

En este caso consideramos el polinomio

$$\begin{aligned} s(x) &= r(x) - c_m b_n^{-1} x^{m-n} g(x) \\ &= c_m x^m + c_{m-1}x^{m-1} + \cdots + c_0 - c_m x^m - c_m \frac{b_{n-1}}{b_n} x^{m-1} - \cdots - \frac{b_0}{b_n}, \end{aligned}$$

cuyo grado es menor que el de $r(x)$. Pero

$$\begin{aligned} r(x) - c_m b_n^{-1} x^{m-n} g(x) &= f(x) - q(x)g(x) - c_m b_n^{-1} x^{m-n} g(x) \\ &= f(x) - (q(x) + c_m b_n^{-1} x^{m-n}) g(x) \in S. \end{aligned}$$

Lo que contradice la minimalidad del grado de $r(x)$, luego la suposición es incorrecta y $m < n$.

Para terminar la demostración, debemos verificar que $q(x)$ y $r(x)$ son únicos. Supongamos entonces que

$$f(x) = q_1(x)g(x) + r_1(x) = q_2(x)g(x) + r_2(x).$$

o sea,

$$g(x)(q_1(x) - q_2(x)) = r_2(x) - r_1(x).$$

Si estos polinomios no son nulos, entonces por el lema 2.1, el grado del de la derecha es menor que n, en cambio el de la izquierda es mayor o igual que n, lo que es una contradicción, luego estos polinomios son nulos, es decir, $r_1(x) = r_2(x)$ y como no hay divisores del cero y $g(x) \neq 0$, $q_1(x) = q_2(x)$. □

El algoritmo de la división no es cierto para $\mathbb{Z}[x]$, el lector podrá fácilmente verificar que para $f(x) = x^2 + 1$ y $g(x) = 3x + 2$, no se puede encontrar polinomios $q(x)$ y $r(x)$ en $\mathbb{Z}[x]$ que verifiquen el teorema 2.3.

Como es habitual, denotaremos por $p(a)$ al número que resulta de reemplazar la variable x en $p(x)$ por el número a. $p(a)$ se llama la *evaluacion* de $p(x)$ en a.

DEFINICIÓN 2.3. Un racional a es una *raíz* (o un *cero*) del polinomio $p(x)$ si y sólo si $p(a) = 0$.

TEOREMA 2.4. *a es un cero de $p(x)$ si y sólo si $x - a$ es un factor de $p(x)$.*

DEMOSTRACIÓN. Aplicamos el teorema 2.3 a $p(x)$ y $x - a$ obteniendo

$$p(x) = q(x)(x - a) + r(x),$$

con $\partial r(x) < 1$, o sea,

$$p(x) = q(x)(x - a) + b,$$

para algún $b \in \mathbb{Q}$. Evaluando en a,

$$0 = p(a) = q(a)(a - a) + b = b,$$

por lo tanto $p(x)$ es un múltiplo de $x - a$.

Reciprocamente, si $x - a \mid p(x)$, entonces $p(a) = q(a)(a - a) = 0$. □

COROLARIO 2.5. *Un polinomio de grado $n \geq 0$ tiene a lo más n ceros.*

DEMOSTRACIÓN. La demostración la haremos por inducción sobre el grado del polinomio $p(x)$.

Si $\partial p(x) = 1$, $p(x) = ax + b = a(x + \frac{b}{a})$ y el único cero es $-\frac{b}{a}$.

Supongamos que todo polinomio de grado n tiene a lo más n ceros y supongamos que $\partial p(x) = n + 1$. Si $p(x)$ no tiene ceros, el teorema se cumple. Si a es un cero de $p(x)$, entonces $p(x) = q(x)(x - a)$, donde $\partial q(x) = n$. Luego los ceros de $p(x)$ son a y los ceros de $q(x)$, por lo tanto hay a lo más $n + 1$ ceros de $p(x)$. □

TEOREMA 2.6. *Sea $p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$. Si $a = \frac{b}{c} \in \mathbb{Q}$, donde $(b, c) = 1$, es una raíz de $p(x)$, entonces*

$$b|a_0 \quad y \quad c|a_n.$$

DEMOSTRACIÓN. Como a es raiz de $p(x)$,

$$p(a) = a_n(\frac{b}{c})^n + a_{n-1}(\frac{b}{c})^{n-1} + \cdots a_1\frac{b}{c} + a_0 = 0$$

y multiplicando por c^n, tenemos

$$a_n b^n + a_{n-1}b^{n-1}c + \cdots + a_1 bc^{n-1} + a_0 c^n = 0.$$

O sea,

$$b(a_n b^{n-1} + a_{n-1}b^{n-2}c + \cdots + a_1 c^{n-1}) = -a_0 c^n,$$

es decir, $b|a_0 c^n$ y como $(b, c) = 1$,

$$b|a_0.$$

Analogamente,

$$c(a_{n-1}b^{n-1} + \cdots + a_1bc^{n-2} + a_0c^{n-1}) = -a_nb^n,$$

es decir, $c|a_nc^n$ y como $(b, c) = 1$,

$$c|a_n.$$

□

COROLARIO 2.7. *Sea* $p(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x]$, *donde* $a_0 \neq 0$. *Si* $p(x)$ *tiene una raíz en* $\mathbb{Q}$, *entonces esa raíz es entera y divide a* a_0.

DEMOSTRACIÓN. Inmediato. □

EJERCICIOS 2.1. (1) Determine todos los racionales para los cuales el polinomio $p(x) = 7x^2 - 5x$ toma un valor entero.

3. Irreducibilidad sobre los Racionales. El Criterio de Eisenstein

DEFINICIÓN 2.4. Un polinomio $p(x)$ no constante se dice *irreducible sobre* $\mathbb{Q}[x]$ si toda vez que $p(x) = q(x)\, r(x)$, entonces o bien $q(x)$ es una unidad de $\mathbb{Q}[x]$ o bien $r(x)$ es una unidad $\mathbb{Q}[x]$.

De manera análoga podemos definir polinomio irreducible sobre $\mathbb{Z}[x]$ o $\mathbb{R}[x]$, etc.

TEOREMA 2.8. *En* $\mathbb{Q}[x]$ *un polinomio es irreducible si y sólo si no es el producto de dos polinomios de grado menor.*

OBSERVACIÓN 2.1.

(1) Debe tenerse en cuenta que el concepto de irreducibilidad es relativo al conjunto de polinomios del que estamos hablando, así el polinomio $x^2 - 2$ es irreducible sobre $\mathbb{Q}[x]$, pero no lo es sobre $\mathbb{R}[x]$ ya que aquí

$$x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2}),$$

y los dos últimos no son unidades de $\mathbb{R}[x]$.

(2) Consideremos $p(x) = 2x^2 - 4$. Si bien $p(x)$ se puede factorizar como $p(x) = 2(x^2 - 2)$, estos factores no tienen grado menor que el de $p(x)$.

En general, si $p(x)$ es irreducible sobre $\mathbb{Q}[x]$ y $0 \neq a \in \mathbb{Q}$, entonces $a \cdot p(x)$ es irreducible sobre $\mathbb{Q}[x]$.

(3) Todo polinomio de primer grado es irreducible sobre $\mathbb{Q}[x]$.

El concepto de polinomio irreducible es central en la teoría de polinomios ya que ocupa dentro de ésta el lugar que tiene el de número primo en la teoría de números, resulta por lo tanto importante contar con métodos para determinar si un polinomio es o no irreducible. Eso es lo que estudiaremos a continuación.

TEOREMA 2.9. *Sea* $p(x) \in \mathbb{Q}[x]$ *de grado* 2 *o* 3. *Entonces* $p(x)$ *es irreducible si y sólo si* $p(x)$ *no tiene un cero en* $\mathbb{Q}$.

DEMOSTRACIÓN. Si a es un cero de $p(x)$, $p(x) = q(x)(x-a)$ y $\partial(x-a) = 1 < \partial p(x)$ y $\partial q(x) = \partial p(x) - 1 < \partial p(x)$. Luego por 2.8, $p(x)$ no es irreducible.

Reciprocamente, si $p(x)$ no es irreducible, existen factores $q(x)$ y $r(x)$ de menor grado que $p(x)$, o sea, de grado menor que 3. Pero $\partial q(x) + \partial r(x) = 3$, luego uno de los dos factores es de grado 1, digamos, $r(x) = ax + b$, o sea, $-\frac{b}{a}$ es un cero de $r(x)$ y por lo tanto también de $p(x)$. □

DEFINICIÓN 2.5. Sea $p(x) = a_n x^n + \cdots + a_0 \in \mathbb{Z}[x]$, $p(x)$ es *primitivo* si y sólo si $(a_0, \ldots, a_n) = 1$.

LEMA 2.10. *Dado un polinomio $p(x) \in \mathbb{Z}[x]$, existe un único polinomio primitivo $q(x)$ y un único entero positivo c tales que $p(x) = cq(x)$.*

DEMOSTRACIÓN. Es obvio que basta tomar $c = (a_0, \ldots, a_n)$ y factorizar c. El polinomio resultante será primitivo. □

Obsérvese que en el teorema anterior, $p(x)$ y $q(x)$ tienen el mismo grado.

LEMA 2.11. *El producto de dos polinomios primitivos es primitivo.*

DEMOSTRACIÓN. Sean

$$\begin{aligned} p(x) &= a_n x^n + \cdots + a_0 \\ q(x) &= b_m x^m + \cdots + b_0 \\ p(x)q(x) &= c_{m+n} x^{m+n} + \cdots + c_0, \end{aligned}$$

donde c_j se define como arriba.

Supongamos que $p(x)q(x)$ no es primitivo. Entonces existe un número primo p tal que $p \mid c_j$, para $0 \leq i \leq m+n$.

Pero como $(a_0, \ldots, a_n) = 1$ y $(b_0, \ldots, b_n) = 1$, existe el menor j y el menor k tales que $p \nmid a_j$ y $p \nmid b_k$, y como p es primo, $p \nmid a_j b_k$.

Ahora bien,

$$c_{j+k} = a_0 b_{j+k} + a_1 b_{j+k-1} + \cdots + a_{j-1} b_{k+1} + a_j b_k + a_{j+1} b_{k-1} + \cdots + a_{j+k} b_0,$$

luego

$$a_j b_k = c_{j+k} - a_0 b_{j+k} - a_1 b_{j+k-1} - \cdots - a_{j-1} b_{k+1} - a_{j+1} b_{k-1} + \cdots - a_{j+k} b_0.$$

Como $p \mid a_i$ para $i < j$,$p \mid b_i$ para $i < k$ y por hipótesis $p \mid c_{j+k}$, todos los términos del lado derecho son divisibles por p, luego $a_j b_k$ también lo es y esto es una contradicción. □

TEOREMA 2.12. **Lema de Gauss**
Sea $p(x) \in \mathbb{Z}[x]$, $\partial p(x) > 0$. Si $p(x)$ es irreducible en $\mathbb{Q}[x]$, entonces $p(x)$ también es irreducible en $\mathbb{Z}[x]$.

DEMOSTRACIÓN. Supongamos que $p(x) = q(x)r(x)$, para ciertos polinomios $q(x), r(x) \in \mathbb{Q}[x]$ tales que $\partial q(x), \partial r(x) < \partial p(x)$. O sea,

$$p(x) = (\frac{a_k}{b_k}x^k + \cdots + \frac{a_1}{b_1}x + \frac{a_0}{b_0})(\frac{c_m}{d_m}x^m + \cdots + \frac{c_1}{d_1}x + \frac{c_0}{d_0}).$$

Multiplicando por $a = [b_0, \ldots, b_k][d_0, \ldots, d_m]$, obtenemos

$$a \cdot p(x) = (a'_k x^k + \cdots + a'_0)(c'_m x^m + \cdots + c'_0),$$

donde los dos polinomios de la derecha, llamemoslos $q'(x)$ y $r'(x)$, están en $\mathbb{Z}[x]$.

Por el lema 2.10 existen enteros positivos b, c y d y polinomios primitivos $\hat{p}(x)$, $\hat{q}(x)$ y $\hat{r}(x)$, tales que $p(x) = b \cdot \hat{p}(x)$, $q'(x) = c \cdot \hat{q}(x)$ y $r'(x) = d \cdot \hat{r}(x)$. Luego

$$a \cdot p(x) = ab \cdot \hat{p}(x) = cd \cdot \hat{q}(x)\hat{r}(x),$$

pero por el lema 2.11 $\hat{q}(x)\hat{r}(x)$ es primitivo y $\hat{p}(x)$ también lo es, luego

$$ab = cd,$$

por la unicidad de las constantes del lema 2.10, es decir,

$$\hat{p}(x) = \hat{q}(x)\hat{r}(x),$$

pero entonces, multiplicando por b,

$$p(x) = b \cdot \hat{p}(x) = b\hat{q}(x)\hat{r}(x),$$

y $b \cdot \hat{q}(x)$, $\hat{r}(x) \in \mathbb{Z}[x]$, o sea, $p(x)$ se descompone como producto de polinomios de menor grado en $\mathbb{Z}[x]$. □

Ejemplo

Demostrar que $p(x) = x^4 - 2x^2 + 8x + 1$ es irreducible sobre $\mathbb{Q}[x]$.

Supongamos que $p(x) = q(x)\ r(x)$. Si $\partial r(x) = 1$, $p(x)$ tiene un cero en $\mathbb{Z}$ que divide a 1. Luego ese cero debe ser ± 1. Pero observamos que $p(1) = 8 \neq 0$ y $p(-1) = -8 \neq 0$, luego ni 1 ni -1 son ceros de $p(x)$, es decir, el grado de $r(x)$ no puede ser 1. En ese caso, la única posibilidad es que $p(x)$ se factorize como

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

es decir,

$$\begin{aligned} a + c &= 0 \\ b + d + ac &= -2 \\ bc + ad &= 8 \\ bd &= 1. \end{aligned}$$

La última ecuación implica que o bien $b = d = 1$, o bien $b = d = -1$ y reemplazando en la ecuación anterior, obtenemos $a + c = \pm 8 \neq 0$, lo que es una contradicción. Por lo tanto $p(x)$ no se puede descomponer como producto de polinomios de menor grado luego es irreducible.

El siguiente es uno de los teoremas más poderosos para determinar la irreducibilidad de un polinomio.

TEOREMA 2.13. **Criterio de Eisenstein**

Sean $p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x]$ *y* p *un número primo. Si* $p \nmid a_n$, $p \mid a_i$, *para* $0 \leq i < n$ *y* $p^2 \nmid a_0$, *entonces* $p(x)$ *es irreducible en* $\mathbb{Q}[x]$.

DEMOSTRACIÓN. Por el teorema 2.12, basta ver que $p(x)$ es irreducible en $\mathbb{Z}[x]$.

Supongamos entonces que $p(x)$ no es irreducible. Entonces

$$p(x) = (b_m x^m + b_{m-1}x^{m-1} + \cdots + b_0)(c_k x^k + c_{k-1}x^{k-1} + \cdots + c_0),$$

en donde $m < n$ y $k < n$. Entonces

$$a_0 = b_0 c_0,$$

y como $p \mid a_0$, $p \mid b_0$ o bien $p \mid c_0$ pero no a ambos ya que $p^2 \nmid a_0$. Digamos que $p \mid c_0$ y $p \nmid b_0$.

Por otra parte, como $p \nmid a_n = b_m c_k$, $p \nmid b_m$ y $p \nmid c_k$.

Sea r el menor índice i tal que $p \nmid c_i$. Por la discusión anterior, tal índice existe y $0 < r \leq k$. Obsérvese que ésto significa que $p \mid c_0, \ldots, p \mid c_{r-1}$.

Por lo tanto si consideramos

$$a_r = b_0 c_r + b_1 c_{r-1} + \cdots + b_r c_0,$$

como $p \nmid b_0 c_r$, $p \nmid a_r$, pero por hipótesis, esto sólo puede ocurrir si $r = n$, lo que es una contradicción. □

Ejemplos

(1) Considere el polinomio $p(x) = 3x^3 + 6x^2 + 4x + 2$. Entonces $p(x)$ es irreducible al aplicar el criterio de Eisenstein con $p = 2$.

(2) Así mismo, $x^n - p$ es irreducible para todo entero positivo n y primo p.

(3) Si p es primo, el polinomio $\varphi(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$, es irreducible.

El criterio de Eisenstein no puede ser aplicado directamente en este caso. Sin embargo si notamos que

$$\varphi(x) = \frac{x^p - 1}{x - 1},$$

y consideramos

$$q(x) = \varphi(x+1) = \frac{(x+1)^p - 1}{x + 1 - 1} = \frac{x^p + \binom{p}{1} x^{p-1} + \cdots + \binom{p}{1} x + 1 - 1}{x}$$

$$= x^{p-1} + \binom{p}{1} x^{p-2} + \cdots + \binom{p}{p-2} x + p.$$

Es claro que $q(x)$ es irreducible por el criterio de Eisenstein. Si $\varphi(x)$ fuese reducible, $q(x)$ también lo sería.

EJERCICIOS 2.2. (1) Diga si los siguientes polinomios son irreducibles sobre $\mathbb{Q}$.
(a) $x^3 + 3x^2 - x - 3$,
(b) $x^3 + 3x^2 - x + 3$,
(c) $2x^5 + 6x^4 - 12x + 15$,
(d) $x^4 + 4$.

Unica

4. Teorema de Factorización Unica

Si bien en el caso de dos polinomios $p(x)$ y $q(x)$ en $\mathbb{Q}[x]$ existen divisores comunes, no podemos hablar de un "máximo común divisor" por la sencilla razón de que los polinomios no están bien ordenados, al menos no de una manera obvia. Podemos entonces pensar en el polinomio de mayor grado que es divisor común de los dos polinomios $p(x)$ y $q(x)$. Resulta obvio que el concepto anterior no está bien definido, consideremos el ejemplo siguiente:

$$p(x) = 2x^3 + x^2 + 2x + 1 \quad \text{y} \quad q(x) = 2x^2 + x\,.$$

Un simple cálculo nos permitirá determinar que $2x + 1$ divide a ambos polinomios y que ningún polinomio de grado mayor los dividirá a ambos (por ejemplo, $p(x)$ no tiene más ceros que $-\frac{1}{2}$ y $q(x)$ sí los tiene). Sin embargo este polinomio no es único ya que, por ejemplo, $x + \frac{1}{2}$ tiene el mismo grado y también es un divisor común de $p(x)$ y $q(x)$. De hecho, dado $a \in \mathbb{Q}$, $a \neq 0$, el polinomio $2ax + a$ es un divisor común de $p(x)$ y $q(x)$ del mismo grado. De entre todos estos (infinitos) polinomios, podemos individualizar uno, aquel cuyo primer coeficiente es 1.

DEFINICIÓN 2.6. El polinomio $p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Q}[x]$ se dice *mónico* si y sólo si $a_n = 1$.

LEMA 2.14. *El producto de polinomios mónicos es mónico.*

DEFINICIÓN 2.7. Definimos el *máximo común divisor* de los polinomios $p(x)$ y $q(x)$ en $\mathbb{Q}[x]$, $\text{MCD}(p(x), q(x))$, como el polinomio mónico de mayor grado que divide a ambos polinomios.

Veremos a continuación que esta definición tiene sentido, es decir, dados dos polinomios no nulos, su máximo común divisor siempre existe. Más aún, veremos que éste tiene muchas de las propiedades del máximo común divisor para números enteros.

TEOREMA 2.15.

(1) *Si $p(x)$ y $q(x)$ pertenecen a $\mathbb{Q}[x]$, entonces MCD$(p(x), q(x))$ es el polinomio mónico de grado más pequeño que puede escribirse como $\alpha(x)p(x)+\beta(x)q(x)$, donde $\alpha(x), \beta(x) \in \mathbb{Q}[x]$.*
(2) *Cualquier divisor común de $p(x)$ y $q(x)$ divide a MCM$(p(x), q(x))$.*
(3) *Si $r(x)$ es un divisor común de $p(x)$ y $q(x)$ del mismo grado que MCM$(p(x), q(x))$, entonces existe $a \in \mathbb{Q}$ tal que $r(x) = a\text{MCD}(p(x), q(x))$.*

Demostración. Sólo demostraremos 1) ya que 2) y 3) son inmediatas. Para este efecto consideremos

$$S = \{r(x) \in \mathbb{Q}[x] : r(x) = \alpha(x)p(x) + \beta(x)q(x),\ \alpha(x), \beta(x) \in \mathbb{Q}[x] \ \text{ y } \ \partial r(x) \geq 0\}.$$

Consideremos un polinomio de grado minimal que pertenezca a este conjunto. Si dividimos por el coeficiente de mayor índice, obtendremos un polinomio mónico de grado minimal que pertenece a S. Este debe ser único ya que si $d_1(x)$ y $d_2(x)$ son dos tales polinomios, $d_1(x) - d_2(x) \in S$ es un polinomio de menor grado.

Denotémos $d(x)$ al único polinomio mónico de grado minimal en S. Demostraremos a continuación que $d(x) = \text{MCD}(p(x), q(x))$. La demostración sigue fielmente las ideas usadas en el teorema análogo para $\mathbb{Z}$ (ver teorema 1.5).

Por el algoritmo de la división, si $d(x)$ no divide a $p(x)$, existen polinomios $r(x), s(x) \in \mathbb{Q}[x]$ tales que $\partial r(x) < \partial d(x)$ y

$$p(x) = s(x)d(x) + r(x).$$

pero entonces

$$\begin{aligned} r(x) &= p(x) - s(x)d(x) \\ &= p(x) - s(x)[\alpha(x)p(x) + \beta(x)q(x)] \\ &= [1 - s(x)\alpha(x)]p(x) - s(x)\beta(x)q(x) \in S, \end{aligned}$$

como $r(x) \neq 0$, ésto contradice la minimalidad del grado de $d(x)$, por lo tanto $r(x) = 0$ y $d(x) \mid p(x)$.

Analogamente, demostramos que $d(x) \mid q(x)$.

Para verificar que $d(x)$ es el polinomio de mayor grado que divide a $p(x)$ y $q(x)$, basta notar que si $r(x)$ es otro divisor común, entonces divide a todos los elementos de S, en particular divide a $d(x)$, y por lo tanto $\partial r(x) \leq \partial d(x)$. □

Teorema 2.16. *Si $p(x)$ es irreducible sobre $\mathbb{Q}[x]$ y $p(x) \mid r(x)s(x)$, entonces $p(x) \mid r(x)$ o bien $p(x) \mid s(x)$.*

Demostración. Supongamos que $p(x) \nmid r(x)$. Entonces, como $p(x)$ es irreducible, $\text{MCD}(p(x), r(x)) = 1$. Luego existen $\alpha(x)$, $\beta(x) \in \mathbb{Q}[x]$ tales que

$$\begin{aligned} 1 &= \alpha(x)p(x) + \beta(x)r(x) \\ s(x) &= \alpha(x)p(x)s(x) + \beta(x)r(x)s(x) \\ s(x) &= [\alpha(x)s(x) + \beta(x)q(x)]p(x), \end{aligned}$$

donde $q(x)p(x) = r(x)s(x)$. Por lo tanto $p(x) \mid s(x)$. □

Observación 2.2. **Algoritmo de Euclides**
El lector puede comprobar que el máximo común divisor entre dos polinomios puede encontrarse usando *exactamente* el mismo algoritmo de Euclides que se usó en el capítulo 1.

El siguiente teorema, el más importante de esta sección, nos indica el rol de los polinomios irreducibles dentro de la teoría de polinomios.

Teorema 2.17. **Teorema de Factorización Unica**
Todo polinomio no nulo en $\mathbb{Q}[x]$ se puede factorizar como una constante por un producto de polinomios mónicos irreducibles. Tal factorización es única salvo por el orden de los factores.

Demostración. Haremos la demostración por inducción sobre el grado del polinomio $p(x)$.

Si $\partial p(x) = 1$, $p(x) = ax + b$, donde $a \neq 0$, entonces

$$p(x) = a(x + \frac{b}{a}),$$

y como sabemos, los polinomios de primer grado son irreducibles.

Supongamos entonces que el teorema es válido para polinomios de grado menor que $\partial p(x) = n$.

Si $p(x)$ es irreducible, factorizamos por el coeficiente del término de mayor grado, como en el caso de primer grado.

Si no, existen polinomios $p_1(x)$ y $p_2(x)$, de grado menor que n, tales que $p(x) = p_1(x)p_2(x)$.

Por hipótesis de inducción, existen constantes a y b y polinomios $q_1(x), \ldots, q_k(x)$ y $r_1(x), \ldots, r_m(x)$ tales que

$$p_1(x) = aq_1(x) \cdots q_k(x),$$
$$p_2(x) = br_1(x) \cdots r_m(x),$$

y por lo tanto

$$p(x) = abq_1(x) \cdots q_k(x)r_1(x) \cdots r_m(x),$$

que es lo que queriamos demostrar.

Para demostrar unicidad, supongamos que

$$aq_1(x) \cdots q_k(x) = br_1(x) \cdots r_m(x).$$

son dos descomposiciones de $p(x)$.

En primer lugar, como todos los polinomios son mónicos, $a = b$ y lo podemos cancelar. Ademas $q_1(x) \mid r_1(x) \cdots r_m(x)$, y por el teorema 2.16, existe algun i tal que

$$q_1(x) \mid r_i(x).$$

Como el orden de los factores no interesa, podemos suponer que $i = 1$. Ahora bien, $r_1(x)$ es irreducible y mónico, por lo tanto

$$q_1(x) = r_1(x).$$

Cancelando,

$$q_2(x) \cdots q_k(x) = r_2(x) \cdots r_m(x).$$

Vemos que si aplicamos el procedimiento anterior un número finito de veces, se cancelan todos los polinomios, luego $k = m$ y para $i \leq m$, $q_i(x) = r_i(x)$, lo que completa la demostración de unicidad de la descomposición. □

EJERCICIOS 2.3. (1) Encuentre el máximo común divisor de los siguientes pares de polinomios y expreselo como combinación de ellos.
   (a) $p(x) = 2x^3 - 4x^2 + x + 2$ y $q(x) = x^3 - x^2 - x - 2$,
   (b) $p(x) = x^4 + x^3 + x^2 + x + 1$ y $q(x) = x^3 - 1$,
   (c) $p(x) = x^2 - x + 4$ y $q(x) = x^4 + x + 1$,
   (d) $p(x) = x^3 - 1$ y $q(x) = x^5 - x^4 + x^3 - x^2 + x - 1$.

(2) Demuestre el Teorema 2.17 usando el principio de Buen Orden sobre el grado de $p(x)$.

5. Irreducibilidad sobre los reales y los complejos

Como vimos en la sección **2**, la irreducibilidad de un polinomio depende del conjunto de referencia, es decir, del conjunto del cual estamos tomando los coeficientes. Así $x^2 - 2$ es irreducible si lo consideramos como un polinomio en $\mathbb{Z}[x]$ o $\mathbb{Q}[x]$, pero no lo es si lo consideramos como polinomio en $\mathbb{R}[x]$ o $\mathbb{C}[x]$.

En secciones anteriores hemos visto lo que sucede a polinomios sobre $\mathbb{Q}$, veremos ahora que podemos describir explícitamente todos lo polinomios sobre $\mathbb{R}$ y sobre $\mathbb{C}$ que son irreducibles. Esto se logra usando un teorema muy importante cuya demostración requiere de herramientas matemáticas más avanzadas que las que disponemos. La primera demostración la dió Gauss en 1799.

Supondremos en esta sección que el lector está familiarizado con los conceptos elementales acerca de los números complejos, así como su aritmética. Usaremos también en forma algo arbitraria algunos teoremas que hemos demostrado en el contexto de los polinomios sobre $\mathbb{Q}$, pero que también son válidos aquí. Invitamos al lector a revisar las demostraciones y verificar esta afirmación.

TEOREMA 2.18. **Teorema Fundamental del Algebra**
Todo polinomio no constante de $\mathbb{C}[x]$ tiene una raíz en $\mathbb{C}$.

COROLARIO 2.19. *Un polinomio es irreducible sobre $\mathbb{C}[x]$ si y sólo si es de primer grado.*

DEMOSTRACIÓN. Si $p(x) \in \mathbb{C}[x]$ es de grado mayor que 1, como tiene una raíz, por el teorema 2.4, que también es válido para polinomios sobre $\mathbb{C}$, $p(x)$ no es irreducible. Es claro que los polinomios de primer grado son irreducibles. □

COROLARIO 2.20. *Todo polinomio $p(x) \in \mathbb{C}[x]$ de grado n se puede escribir en la forma*

$$p(x) = c(x - a_1)(x - a_2) \cdots (x - a_n),$$

donde $c, a1, a_2 \ldots, a_n \in \mathbb{C}$. Esta descomposición es única salvo por el orden de los factores.

DEMOSTRACIÓN. Por el teorema 2.17, que también es válido para polinomios sobre $\mathbb{C}$ y por el corolario anterior, $p(x)$ se descompone como producto de factores lineales

$$p(x) = (b_1x + c_1) \cdots (b_n + c_n),$$

donde por consideraciones sobre el grado del producto, debe haber n factores. Por último, factorizando los coeficientes b_i y haciendo $a_i = -\frac{c_i}{b_i}$, llegamos a la forma indicada. □

Debe observarse que los números complejos a_i del corolario anterior no son necesariamente distintos. También es obvio que cada uno de ellos es una raíz del polinomio. Resumimos esto en el siguiente corolario.

COROLARIO 2.21. *Un polinomio $p(x) \in \mathbb{C}[x]$ de grado n tiene exactamente n raíces complejas considerando las repeticiones.*

Estudiaremos ahora los polinomios irreducibles sobre $\mathbb{R}[x]$.

LEMA 2.22. *Si $p(x) \in \mathbb{R}[x]$ y $a + bi$ es una raíz compleja de $p(x)$, entonces su conjugado $a - bi$ también es una raíz de $p(x)$.*

DEMOSTRACIÓN. Recordemos que si z_1 y z_2 son complejos entonces sus conjugados verifican

$$\overline{z_1 + z_2} = \overline{z_1} + \overline{z_2} \quad \text{y} \quad \overline{z_1 \cdot z_2} = \overline{z_1} \cdot \overline{z_2},$$

por lo tanto, si

$$p(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$$

y $z = a + bi$ es una raíz de $p(x)$,

$$0 = \overline{0} = \overline{p(z)} = \overline{a_n}\overline{z^n} + \overline{a_{n-1}}\overline{z^{n-1}} + \cdots + \overline{a_1z} + \overline{a_0},$$

pero como los a_i son reales, $\overline{a_i} = a_i$, luego

$$0 = \overline{p(z)} = a_n\overline{z}^n + a_{n-1}\overline{z}^{n-1} + \cdots + a_1\overline{z} + a_0 = p(\overline{z}),$$

por lo tanto $\overline{z} = a - bi$ también es raíz de $p(x)$. □

TEOREMA 2.23. *Un polinomio $p(x) \in \mathbb{R}[x]$ es irreducible sobre $\mathbb{R}[x]$ si y sólo si se verifica una de las siguientes condiciones:*

(1) $p(x)$ *es de primer grado o*
(2) $p(x) = ax^2 + bx + c$, *donde* $b^2 - 4ac < 0$.

DEMOSTRACIÓN. Es obvio que los polinomios de primer grado son irreducibles. Si $p(x)$ es del tipo indicado en (2), sabemos que tiene dos raíces complejas conjugadas α y $\overline{\alpha}$ luego

$$p(x) = a(x - \alpha)(x - \overline{\alpha}),$$

y como esta descomposición es única en $\mathbb{C}[x]$, $p(x)$ no puede descomponerse como producto de otros factores en $\mathbb{R}[x]$. Luego ambos tipos de polinomios son irreducibles sobre $\mathbb{R}[x]$.

Veamos ahora que si $p(x)$ no es de esa forma, entonces es reducible.

Si $p(x) = ax^2 + bx + c$ y $b^2 - 4ac \geq 0$, entonces $p(x)$ tiene dos raíces reales a_1 y a_2 luego $p(x) = a(x - a_1)(x - a_2)$, luego $p(x)$ no es irreducible sobre $\mathbb{R}[x]$. Podemos entonces concentrarnos en polinomios de grado mayor que 2.

Supongamos que $\partial(p(x) \geq 3$. Por el teorema 2.18, $p(x)$ tiene una raíz compleja $\alpha = a + bi$ y por el lema anterior, $\overline{\alpha} = a - bi$ es también una raíz de $p(x)$, por lo tanto

$$p(x) = (x - (a + bi))(x - (a - bi))h(x),$$

donde $h(x) \in \mathbb{C}[x]$ y $\partial(h(x)) > 0$.

Observamos ahora que

$$g(x) = (x - (a + bi))(x - (a - bi)) = x^2 - 2ax + (a^2 + b^2),$$

o sea, $g(x) \in \mathbb{R}[x]$ y

$$p(x) = g(x)h(x). \qquad (*)$$

Hacemos notar ahora que el algoritmo de la división también es válido para polinomios en $\mathbb{R}[x]$ y en $\mathbb{C}[x]$.

Entonces, lo aplicamos primero en $\mathbb{R}[x]$. Dados $p(x)$ y $g(x)$ existen polinomios únicos $q(x)$ y $r(x)$ en $\mathbb{R}[x]$ tales que

$$p(x) = g(x)q(x) + r(x), \qquad (**)$$

con $r(x) = 0$ o $\partial(r(x)) < \partial(g(x))$.

Observemos que $p(x)$, $g(x)$, $q(x)$ y $r(x)$ pueden considerarse polinomios en $\mathbb{C}[x]$, luego comparando $(*)$ y $(**)$, si aplicamos la unicidad del cuociente y el resto en algoritmo de la división en $\mathbb{C}[x]$, tenemos

$$h(x) = q(x) \in \mathbb{R}[x].$$

Por lo tanto $p(x)$ no es irreducible. □

COROLARIO 2.24. *Todo polinomio* $p(x)$ *en* $\mathbb{R}[x]$ *de grado impar tiene una raiz real.*

Demostración. Por el teorema 2.17, que también es válido para polinomios en $\mathbb{R}[x]$,

$$p(x) = p_1(x)p_2(x)\cdots p_k(x),$$

donde los polinomios $p_i(x)$ son polinomios irreducibles en $\mathbb{R}[x]$, luego de grado 1 o 2.

Como

$$\partial(p(x)) = \partial(p_1(x)) + \partial(p_2(x)) + \cdots + \partial(p_k(x))$$

es impar, uno de los factores p_i tiene que ser de primer grado, luego $p(x)$ tiene una raíz en $\mathbb{R}$. □

Ejercicios 2.4.

(1) Verifique que todos los teoremas sobre polinomios en $\mathbb{Q}[x]$ usados en esta sección para polinomios sobre $\mathbb{R}[x]$ y $\mathbb{C}[x]$, son también válidos en estos contextos.

CAPITULO 3

Anillos

En este capítulo desarrollaremos algunos aspectos de una teoría general que englobe a todos los ejemplos que hemos visto en los capítulos anteriores, a otros que el lector ha estudiado en distinto contexto y nuevos ejemplos de conjuntos dotados de operaciones con las que se puede desarrollar una aritmética similar a la de los números enteros.

1. Definiciones y Ejemplos

DEFINICIÓN 3.1. Un *anillo* es un conjunto no vacío A dotado de dos operaciones que denotamos $+$ y $\cdot$ que satisfacen las siguientes condiciones:

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

b) Existe un elemento $\mathbf{0} \in A$, al que llamaremos *neutro aditivo de* A, tal que para todo $a \in A$,
$$a+\mathbf{0} = \mathbf{0}+a = a$$

c) Para cada $a \in A$ existe $b \in A$ tal que
$$a+b = b+a = \mathbf{0}$$
Demostraremos después de los ejemplos que tal elemento es único. Lo llamaremos *inverso aditivo de* a y lo denotaremos $-a$, asimismo, abreviaremos la expresión $a+(-b)$ por $a-b$.

d)
$$a+b = b+a$$

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

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

Si además
$$a\cdot b = b\cdot a,$$
el anillo se dice *conmutativo.* **1** Si existe un elemento $\mathbf{1} \in A$ tal que
$$a\cdot\mathbf{1} = \mathbf{1}\cdot a,$$

el anillo se dice *unitario*. Al elemento $\mathbf{1}$ lo llamaremos *neutro multiplicativo de* A.

Como veremos en los ejemplos, sobre un mismo conjunto A puede definirse distintas operaciones y, por lo tanto, obtener distintos anillos. Debemos entonces explicitar las operaciones sobre A de las que estamos hablando, así en estricto rigor, un anillo es un triple $\langle A, +, \cdot \rangle$. Sin embargo, es habitual hablar del anillo A cuando no hay posibilidad de confusión respecto de las operaciones de las que estamos hablando.

Seguiremos la convención de escribir ab en lugar de $a \cdot b$.

EJEMPLOS 3.1. (1) En los dos capítulos anteriores hemos estudiado los ejemplos clásicos de anillos. Todos ellos son conmutativos y unitarios.

Los enteros $\langle \mathbb{Z}, +, \cdot \rangle$.

Las clases residuales $\langle \mathbb{Z}_n, \oplus, \otimes, \rangle$.

Los polinomios $\langle \mathbb{Q}[x], +, \cdot \rangle$. También $\mathbb{Z}[x]$, $\mathbb{R}[x]$, etc.

(2) Los anillos de números $\mathbb{Q}$,$\mathbb{R}$ y $\mathbb{C}$ dotados de las operaciones habituales.

(3) Definimos $2\mathbb{Z} = \{2n : n \in \mathbb{Z}\}$ y lo dotamos de la suma y producto de $\mathbb{Z}$. Este es un anillo conmutativo y *no* unitario.

Analogamente, para cualquier entero positivo n podemos definir el anillo $n\mathbb{Z}$.

(4) Dado un anillo cualquiera A, podemos generalizar el trabajo del Capítulo 2 y definir el conjunto $A[x]$ de los polinomios sobre A.

$$A[x] = \{a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 \ : \ n \in \mathbb{N},\, a_0, a_1, \ldots, a_n \in A\},$$

y las operaciones se definen como para polinomios sobre $\mathbb{Q}$. $A[x]$ es el *anillo de los polinomios sobre* A.

(5) El conjunto $M_2(\mathbb{R})$, de las matrices cuadradas de orden 2, con las operaciones de suma y producto matricial habituales, es un anillo no conmutativo y unitario, donde

$$\mathbf{0} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}. \qquad \mathbf{1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

(6) El siguiente ejemplo requiere de ciertas nociones elementales de cálculo. Consideramos el conjunto $C[0,1]$ de todas las funciones continuas

$$f : [0,1] \longrightarrow \mathbb{R},$$

donde las operaciones $f + g$ y $f \cdot g$ están definidas punto a punto:

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

Este es un anillo no conmutativo y unitario. ¿Cuáles son sus neutros aditivo y multiplicativo?

(7) Los llamados *enteros de Gauss*, $\mathbb{Z}[i] = \{m + ni : m, n \in \mathbb{Z}\}$, con las operaciones habituales de los números complejos es también un anillo.
(8) Consideremos ahora el conjunto $\mathbb{Z}$ de los números enteros pero con nuevas operaciones definidas como sigue:

$$\begin{aligned} a \oplus b &= a + b \\ a \otimes b &= 0 \end{aligned}$$

(9) Definimos $\mathbb{Z} \times \mathbb{Z} = \{(a, b) : a, b \in \mathbb{Z}\}$ con operaciones por coordenadas, es decir,

$$\begin{aligned} (a, b) + (c, d) &= (a + c, b + d) \\ (a, b) \cdot (c, d)) &= (ac, bd). \end{aligned}$$

$\mathbb{Z} \times \mathbb{Z}$ así definido es un anillo.

Resulta obvio que este ejemplo es un caso particular de una construcción mucho más general. Dados dos anillos cualquiera A y B, podemos definir el anillo $A \times B$, llamado el *producto directo de A y B*, con las operaciones definidas de manera análoga a la anterior.

TEOREMA 3.1. *En todo anillo A se verifica:*

(1) $\mathbf{0}$ *es el único elemento de A con la propiedad que lo define, es decir, si para todo $a \in A$, $a + c = c + a = a$, entonces $c = \mathbf{0}$.*
(2) *El inverso aditivo de a es único.*
(3) $a\mathbf{0} = \mathbf{0}a = \mathbf{0}$
(4) $a(-b) = (-a)b = -(ab)$
(5) $(-a)(-b) = ab$
(6) $-(-a) = a$
(7) *Si A es unitario,* $\mathbf{1}$ *es el único elemento de A con la propiedad que lo define, es decir, si para todo $a \in A$, $ac = ca = a$, entonces $c = \mathbf{1}$.*
(8) *Si A es unitario, $(-\mathbf{1})a = -a$.*
(9) $(a + b)^2 = a^2 + ab + ba + b^2$

DEMOSTRACIÓN.

(1) Si para todo $a \in A$, $a + c = c + a = a$, entonces, en particular para $a = \mathbf{0}$,

$$\mathbf{0} = \mathbf{0} + c = c.$$

La primera igualdad se verifica por hipótesis y la segunda es por la definición de $\mathbf{0}$.

(2) Supongamos que a tiene dos inversos aditivos b y c. Entonces

$$\begin{aligned} b &= b + \mathbf{0} \\ &= b + (a + c) \\ &= (b + a) + c \\ &= \mathbf{0} + c \\ &= c. \end{aligned}$$

Luego el inverso es único. Obsérvese que es esta unicidad la que nos da derecho a hablar de *el* inverso aditivo de a. El lector debe revisar cuáles reglas de la definición de anillo se ha usado en cada línea de la demostración.

(3)

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

sumando $-(a\mathbf{0})$ a cada miembro de la ecuación anterior, tenemos

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

lo que termina la demostración. De manera analoga se demuestra que $\mathbf{0} = \mathbf{0}a$.

(4) Observemos que

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

Analogamente, $a(-b) + ab = \mathbf{0}$, es decir, $a(-b)$ es un inverso aditivo de ab, pero éste es único, luego $a(-b) = -(ab)$.

De la misma manera, $(-a)b = -(ab)$, luego son todos iguales entre sí.

(5) La demostración es análoga a la anterior.

(6) Idem.

(7) Idem.

(8) Idem.

(9)

$$\begin{aligned}(a+b)^2 &= (a+b)(a+b)\\ &= a(a+b)+b(a+b)\\ &= aa+ab+ba+bb,\end{aligned}$$

que es lo que queriamos demostrar.

□

Recordaremos aquí un concepto que introdujimos en capítulos anteriores pero ahora dentro de este contexto más general.

Definición 3.2.

(1) Decimos que $a \in A$ es *divisor del cero* si $a \neq \mathbf{0}$ y existe $b \neq \mathbf{0}$ tal que $ab = \mathbf{0}$.
(2) Un anillo conmutativo que no tiene divisores del cero es un *dominio de integridad* o simplemente un *dominio*.
(3) En un anillo unitario A con neutro multiplicativo $\mathbf{1}$, decimos que un elemento u es una *unidad* si existe un elemento v talque

$$uv = vu = \mathbf{1}.$$

Tal elemento se llama *inverso* de u. El conjunto de todas las unidades de A se denota A^*.

Ya hemos visto ejemplos de anillos que son dominios, $\mathbb{Z}$, $\mathbb{Z}_5$ y $\mathbb{Q}[x]$, y otros de anillos conmutativos que no son dominios, por ejemplo, $\mathbb{Z}_4$.

Los anillos no conmutativos también pueden tener divisores del cero. Consideremos por ejemplo el anillo $M_2(\mathbb{R})$. Aquí

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

luego estas matrices son divisores del cero.

En $\mathbb{Z}$, las unicas unidades son 1 y -1. En general, en cualquier anillo unitario, el neutro multiplicativo $\mathbf{1}$ es una unidad.

Ejercicios 3.1. (1) Diga cuáles de los siguientes conjuntos son un anillo con respecto a las operaciones habituales.
(a) $\{m + n\sqrt{2} : m, n \in \mathbb{Z}\}$,
(b) $\{m + n\sqrt[3]{2} : m, n \in \mathbb{Z}\}$,
(c) $\{m + n\sqrt[3]{2} + \sqrt[3]{9} : m, n \in \mathbb{Z}\}$,
(d) $\{\frac{m}{n} : m, n \in \mathbb{Z},\ (m, n) = 1$ y n es impar$\}$,
(e) $\{\frac{m}{p^r} : m \in \mathbb{Z},\ r \geq 1,\ p$ un primo fijo$\}$,

(2) En $\mathbb{Z} \times \mathbb{Z}$ definimos las siguientes operaciones.

$$\begin{aligned}(a,b)+(c,d) &= (a+c, b+d)\\ (a,b)\cdot(c,d)) &= (ac+bd, ad+bc+bd).\end{aligned}$$

Verifique que este es un anillo conmutativo. ¿Es este un dominio de integridad?

(3) En $\mathbb{Z}$ definimos las nuevas operaciones:

$$\begin{aligned}a \oplus b &= a+b-1\\ a \otimes b &= a+b-ab\end{aligned}$$

Verifique que este es un anillo conmutativo y unitario. Encuentre sus neutros aditivo y multiplicativo. ¿Es este un dominio de integridad?

(4) Verifique que los siguientes conjuntos de números enteros, con las operaciones habituales, satisfacen todos los axiomas de anillos excepto uno.
   (a) El conjunto de todos los números impares más 0.
   (b) El conjunto de todos los enteros no negativos.

(5) Dé dos ejemplos de anillos unitarios en los que $\mathbf{1} = -\mathbf{1}$.

(6) Encuentre todas las unidades de los anillos
   (a) $\mathbb{Z}[x]$ y $\mathbb{Q}[x]$,
   (b) $\mathbb{Z}_3$, $\mathbb{Z}_6$, $\mathbb{Z}_{11}$, $\mathbb{Z}_{12}$ y en general, $\mathbb{Z}_n$,
   (c) $M_2(\mathbb{R})$.

(7) Haga los detalles de la demostración de las partes (6) y (7) del teorema 3.1.

(8) Demuestre que el inverso de una unidad es único y que también es una unidad.

(9) Demuestre que las unidades se pueden cancelar, es decir, si u es una unidad y

$$ua = ub \text{ o bien } au = bu,$$

entonces $a = b$.

2. Subanillos e Ideales

En la sección anterior vimos ejemplos de anillos que están contenidos en otros anillos más grandes, por ejemplo, $\mathbb{Z}$ está contenido en $\mathbb{Q}$. Formalizaremos aquí estas ideas.

2.1. Definiciones y Ejemplos.

Definición 3.3. Si A es un anillo, un subconjunto no vacío B de A es un *subanillo* de A si y sólo si B dotado de las mismas operaciones de A restringidas a B es un anillo. Escribimos en este caso $B \leq A$.

TEOREMA 3.2. *B es un subanillo de A si sólo si $B \subset A$, $B \neq \emptyset$ y B es cerrado bajo la diferencia y el producto, i.e., para todo $x, y \in B$,*

$$x - y \in B \ \text{ y } \ xy \in B.$$

DEMOSTRACIÓN. Que la primera afirmación implica la segunda es obvio.

Supongamos entonces que para todo $x, y \in B$, $x - y \in B$ y $xy \in B$.

Como B no es vacío, tomemos $a \in B$. Por la primera propiedad,

$$\mathbf{0} = a - a \in B,$$

es decir, B tiene elemento neutro. Además, usando nuevamente la primera propiedad,

$$-a = \mathbf{0} - a \in B,$$

o sea, B contiene los inversos aditivos de todos sus elementos. Por último, para todo $a, b \in B$

$$a + b = a - (-b) \in B,$$

o sea, B es cerrado bajo la suma. Como por hipótesis B también es cerrado bajo el producto, las operaciones están bien definidas.

Observemos ahora que las propiedades de asociatividad de la suma y del producto, la conmutatividad de la suma y la distributividad del producto sobre la suma se verifican en todo el anillo A, luego con mayor razón se verifican sobre B. Por último, como vimos antes, el neutro $\mathbf{0} \in B$ y B es cerrado bajo inversos aditivos. Por lo tanto, B es un anillo. □

EJEMPLOS 3.2.
(1) $\mathbb{Z} \leq \mathbb{Q} \leq \mathbb{R} \leq \mathbb{C}$.
(2) Para cualquier entero positivo k, $k\mathbb{Z} \leq \mathbb{Z}$.
(3) $\mathbb{Z}[i] \leq \mathbb{C}$.
(4) $\{0, 2\} \leq \mathbb{Z}_4$.
(5) Todo anillo A tiene por lo menos dos subanillos, $\{0\}$ y A.
(6) Definimos

$$\mathbb{Q}[\sqrt{3}] = \{a + b\sqrt{3} : a, b \in \mathbb{Q}\}.$$

Entonces $\mathbb{Q}[\sqrt{3}] \leq \mathbb{R}$.

DEFINICIÓN 3.4. Si A es un anillo, un subconjunto no vacío $\mathcal{I}$ de A es un *ideal* de A si y sólo si

(1) Para todo a,$b \in \mathcal{I}$, $a - b \in \mathcal{I}$.
(2) Para todo $a \in \mathcal{I}$ y $r \in A$, $ar \in \mathcal{I}$ y $ra \in \mathcal{I}$.

Obsérvese que todo ideal de A es un subanillo. El recíproco no es cierto, por ejemplo, $\mathbb{Z}$ es un subanillo de $\mathbb{Q}$, pero no es ideal de $\mathbb{Q}$ ya que

$$3 \in \mathbb{Z} \text{ y } \frac{2}{5} \in \mathbb{Q}, \text{ pero } 3 \cdot \frac{2}{5} = \frac{6}{5} \notin \mathbb{Z}.$$

Ejemplos 3.3. (1) El ejemplo clásico de ideal de $\mathbb{Z}$ es $k\mathbb{Z}$ para algún entero positivo k.

(2) Sea $\mathcal{I} = \{p(x) \in \mathbb{Q}[x] : \text{el término constante de } p(x) \text{ es } 0\}$. Entonces $\mathcal{I}$ es un ideal de $\mathbb{Q}[x]$.

(3) $\mathbb{Z} \times \{0\}$ es un ideal de $\mathbb{Z} \times \mathbb{Z}$.

(4) $\Delta = \{(n, n) : n \in \mathbb{Z}\}$ es un subanillo de $\mathbb{Z} \times \mathbb{Z}$ que no es un ideal de $\mathbb{Z} \times \mathbb{Z}$.

El siguiente lema es a veces útil, su demostración es obvia.

Lema 3.3. *Si $\mathcal{I}$ es un ideal del anillo unitario A y $\mathbf{1} \in \mathcal{I}$, entonces $\mathcal{I} = A$.*

2.2. Ideales Principales e Ideales Maximales. El siguiente teorema nos dice que la intersección de (un conjunto arbitrario de) ideales de un anillo es también un ideal.

Teorema 3.4. *Si para cada $j \in J$, $\mathcal{I}_j$ es un ideal, entonces $\mathcal{I} = \bigcap_{j \in J} \mathcal{I}_j$ es un ideal.*

Resulta natural preguntarse si la unión de ideales es o no un ideal. El siguiente ejemplo demuestra que ni siquiera la unión de sólo dos ideales tiene que ser un ideal.

Consideremos los ideales $2\mathbb{Z}$ y $3\mathbb{Z}$ de $\mathbb{Z}$. Entonces como $2, 3 \in 2\mathbb{Z} \cup 3\mathbb{Z}$, si éste fuera un ideal,

$$1 = 3 - 2 \in 2\mathbb{Z} \cup 3\mathbb{Z},$$

ya que los ideales son cerrados bajo diferencias, pero $1 \notin 2\mathbb{Z} \cup 3\mathbb{Z}$, luego $2\mathbb{Z} \cup 3\mathbb{Z}$ no es un ideal de $\mathbb{Z}$, de hecho ni siquiera es un subanillo de $\mathbb{Z}$.

Definición 3.5. Si $X \subset A$, llamamos *ideal generado por X* al menor ideal de A que contiene a X. Lo denotaremos $\langle X \rangle$.

Si $X = \{a\}$ el ideal generado por X se llama *ideal principal* generado por a y se le denota $\langle a \rangle$.

Es fácil ver que si $X \subseteq A$ entonces el ideal de A generado por X siempre existe, para ello basta considerar

$$\bigcap \{\mathcal{I} : \mathcal{I} \text{ es ideal de } A \text{ y } X \subseteq \mathcal{I}\}.$$

Por el teorema 3.4 esta intersección es un ideal que obviamente contiene a X.

Teorema 3.5. *Si A es un anillo conmutativo y unitario, entonces el ideal principal generado por a es*

$$\langle a \rangle = \{xa : x \in A\}.$$

Demostración. Sea $\mathcal{I} = \{xa : x \in A\}$.

Es claro que $\mathcal{I} \neq \emptyset$ ya que $a = \mathbf{1}a \in \mathcal{I}$.

Si $u = xa$ y $v = ya$ son elementos de $\mathcal{I}$, entonces $u - v = xa - ya = (x - y)a \in \mathcal{I}$.

Si $u = xa \in \mathcal{I}$ y $b \in A$, entonces $bu = ub = b(xa) = (bx)a \in \mathcal{I}$, ya que $bx \in \mathcal{I}$, o sea, $\mathcal{I}$ es un ideal de A que contiene a a. Es claro que cualquier ideal que contenga

a a, deberá contener a $\mathcal{I}$, luego este es el ideal más pequeño que contiene a a, es decir, $\mathcal{I} = \langle a \rangle$. □

Teorema 3.6.

(1) *Todos los ideales de* $\mathbb{Z}$ *son principales.*
(2) *Todos los ideales de* $\mathbb{Q}[x]$ *son principales.*

Demostración. Probaremos sólo (1) ya que la demostración de (2) es totalmente análoga.

Sea $\mathcal{I}$ un ideal de $\mathbb{Z}$. Si $\mathcal{I} = \{0\}$, entonces $I = 0\,\mathbb{Z}$ es un ideal principal.

Si no, existe $a \in \mathcal{I}$, $a \neq \mathbf{0}$, podemos suponer que a es positivo pues si no lo es, su inverso, que también pertenece a $\mathcal{I}$, es positivo. Por lo tanto

$$a \in A = \{m \in \mathcal{I} : m > 0\}.$$

Es decir, A es un conjunto no vacío de enteros positivos y, por lo tanto, tiene un menor elemento al que llamaremos n.

Demostraremos ahora que todo elemento de $\mathcal{I}$ es un múltiplo de n.

Sea $m \in \mathcal{I}$. Por el algoritmo de la división, existen enteros q y r, donde $0 \leq r < n$,tales que

$$m = nq + r.$$

Supongamos que $r \neq 0$. Entonces por la definición de ideal, como $n \in \mathcal{I}$, $nq \in \mathcal{I}$ y por lo tanto

$$0 < r = m - nq \in I.$$

Pero esto contradice la minimalidad de n. Luego $r = 0$ y m es un múltiplo de n. □

El lector podría quedarse con la idea de que todos lo ideales de cualquier anillo son principales, en efecto, no hemos dado todavía un ejemplo de un ideal no principal.

Ejemplo

Consideremos el anillo $\mathbb{Z}[x]$ y el ideal generado por $\{2, x\}$. Es fácil comprobar que

$$\langle \{2, x\} \rangle = \{2p(x) + xq(x) : p(x), q(x) \in \mathbb{Z}[x]\}.$$

En particular esto implica que, $\langle \{2, x\} \rangle \neq \mathbb{Z}[x]\}$, ya que, por ejemplo, $1 \notin \langle \{2, x\} \rangle$.

Supongamos que $\langle \{2, x\} \rangle$ es principal. Entonces existe un polinomio $p(x) \in \mathbb{Z}[x]$ tal que

$$\langle \{2, x\} \rangle = \langle p(x) \rangle.$$

Como $2 \in \langle \{2, x\} \rangle$, $p(x) \mid 2$, lo que implica que $p(x)$ es un polinomio constante. Es más, o bien $p(x) = 1$ o $p(x) = 2$.

Por otra parte, $x \in \langle \{2, x\} \rangle$, luego $p(x) \mid x$, vale decir, $p(x)$ debe ser 1. Pero entonces $\langle p(x) \rangle = \mathbb{Z}[x]$, lo que es una contradicción.

DEFINICIÓN 3.6. Un ideal $\mathcal{M}$ de un anillo A se dice *maximal* si y sólo si $\mathcal{M} \neq A$ y para todo ideal $\mathcal{N}$ de A, si $\mathcal{M} \subsetneqq \mathcal{N} \subseteq A$, entonces $\mathcal{N} = A$.

En otras palabras, un ideal es maximal si no esta contenido en nigún otro ideal no trivial.

EJEMPLOS 3.4. (1) El ideal $3\mathbb{Z}$ de $\mathbb{Z}$ es maximal.
(2) El ideal $\langle x^2 + 1 \rangle$ de $\mathbb{Q}[x]$ es maximal.
(3) El ideal $4\,\mathbb{Z}$ de $\mathbb{Z}$ no es maximal ya que $4\,\mathbb{Z} \subsetneqq 2\,\mathbb{Z} \neq \mathbb{Z}$.

Más generalmente podemos demostrar el siguiente teorema.

TEOREMA 3.7. (1) *Si $\mathcal{M}$ es un ideal de $\mathbb{Z}$, entonces $\mathcal{M}$ es maximal si sólo si $\mathcal{M} = p\,\mathbb{Z}$, para algún primo p.*
(2) *Si $\mathcal{M}$ es ideal de $\mathbb{Q}[x]$, entonces $\mathcal{M}$ es maximal si y sólo si $\mathcal{M} = \langle p(x) \rangle$, para algún polinomio irreducible $p(x)$.*

DEMOSTRACIÓN. (1) Sea $\mathcal{M}$ un ideal de $\mathbb{Z}$. Sabemos que todo ideal de $\mathbb{Z}$ es principal, o sea, $\mathcal{M} = m\,\mathbb{Z}$, para algún m.

Si m no es primo, digamos $m = pq$, donde $p \neq \pm 1$, $q \neq \pm 1$, entonces $p\,\mathbb{Z}$ es un ideal de $\mathbb{Z}$ tal que

$$\mathcal{M} \subsetneqq p\,\mathbb{Z} \neq \mathbb{Z},$$

luego $\mathcal{M}$ no es maximal.

Si m es primo y $\mathcal{N} = n\,\mathbb{Z}$ es otro ideal de $\mathbb{Z}$ tal que

$$\mathcal{M} = m\,\mathbb{Z} \subsetneqq m\,\mathbb{Z},$$

entonces $m \mid n$, luego $m = 1$, o sea, $N = \mathbb{Z}$, o sea $\mathcal{M}$ es maximal.

(2) La demostración es análoga a la de (1) y se deja como ejercicio. □

2.3. Anillos Cuociente.

TEOREMA 3.8. *Sea A un anillo, $\mathcal{I}$ un ideal de A, entonces la relación*

$$a \sim b \;\; \textit{si y sólo si} \;\; a - b \in \mathcal{I},$$

es una relación de equivalencia.

Más aún, si $a_1 \sim b_1$ y $a_2 \sim b_2$, entonces

$$-a_1 \sim -b_1 \tag{4}$$

$$a_1 + a_2 \sim b_1 + b_2 \tag{5}$$

$$a_1 a_2 \sim b_1 b_2. \tag{6}$$

DEMOSTRACIÓN. Para todo $a \in A$, $a - a = \mathbf{0} \in \mathcal{I}$, luego $\sim$ es reflexiva.

Si $a - b \in \mathcal{I}$, entonces $b - a \in \mathcal{I}$, luego $\sim$ es simétrica.

Si $a - b \in \mathcal{I}$ y $b - c \in \mathcal{I}$, luego su suma, $a - c \in \mathcal{I}$, o sea, $\sim$ es transitiva.

Supongamos ahora que $a_1 \sim b_1$. O sea, $a_1 - b_1 \in \mathcal{I}$. Pero entonces $-(a_1 - b_1) \in \mathcal{I}$, luego $-a_1 - (-b_1) \in \mathcal{I}$, o sea, $-a_1 \sim -b_1$.

Si $a_1 \sim b_1$ y $a_2 \sim b_2$, entonces

$$(a_1 + a_2) - (b_1 + b_2) = (a_1 - b_1) + (a_2 - b_2) \in \mathcal{I},$$

ya que $\mathcal{I}$ es cerrado bajo sumas.

Por ultimo, si $a_1 \sim b_1$ y $a_2 \sim b_2$, entonces como $\mathcal{I}$ es ideal

$$\begin{aligned} a_1a_2 - b_1a_2 &= (a_1 - b_1)a_2 \in \mathcal{I} \\ b_1a_2 - b_1b_2 &= b_1(a_2 - b_2) \in \mathcal{I}, \end{aligned}$$

y sumando,

$$a_1a_2 - b_1b_2 \in \mathcal{I}.$$

□

Obsérvese que en la demostración anterior hemos usado toda la fuerza de la definición de ideal.

También debemos notar que la clase de equivalencia de un elemento $a \in A$ es

$$\{b \in A : a \sim b\} = \{b \in A : a - b \in \mathcal{I}\} = \{a + i : i \in \mathcal{I}\}.$$

Esto motiva la siguiente notación.

Definición 3.7. Sea A un anillo, $\mathcal{I}$ un ideal de A, denotaremos $a + \mathcal{I}$ la clase de equivalencia de a y la llamaremos *clase de a módulo* $\mathcal{I}$. El conjunto de todas las clases de equivalencia se denotará $A \mid \mathcal{I}$.

Teorema 3.9. *Sea A un anillo, $\mathcal{I}$ un ideal de A, entonces $A \mid \mathcal{I}$ dotado de las operaciones*

$$\begin{aligned} (a + \mathcal{I}) + (b + \mathcal{I}) &= (a + b) + \mathcal{I} \\ (a + \mathcal{I}) \cdot (b + \mathcal{I}) &= ab + \mathcal{I}, \end{aligned}$$

es un anillo. Este se llama el anillo cuociente *de A por $\mathcal{I}$.*

En este anillo, el neutro aditivo es la clase de $\mathbf{0}$ es decir

$$\mathbf{0} + \mathcal{I} = \mathcal{I}.$$

Además

$$-(a + \mathcal{I}) = -a + \mathcal{I}.$$

Si A es conmutativo, entonces $A \mid \mathcal{I}$ es conmutativo.

Si A es unitario, entonces $A \mid \mathcal{I}$ es unitario.

Demostración. Ejercicio. □

Debemos observar que la relación definida anteriormente, en el caso de $\mathbb{Z}$ e $\mathcal{I} = n\,\mathbb{Z}$, coincide con las congruencias módulo n. Así mismo, $\mathbb{Z} \mid n\,\mathbb{Z} = \mathbb{Z}_n$.

Ejercicios 3.2. (1) Diga cuáles de los siguientes conjuntos con las operaciones matriciales habituales son subanillos de $M_2(\mathbb{R})$.

(a)
$$\left\{\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} : a, b \in \mathbb{Z}\right\},$$
(b)
$$\left\{\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} : a, b \in \mathbb{Z}\right\},$$
(c)
$$\left\{\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} : a, b \in \mathbb{Z}\right\},$$
(d)
$$\left\{\begin{pmatrix} a & b \\ c & 0 \end{pmatrix} : a, b, c \in \mathbb{R}\right\},$$
(e)
$$\left\{\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} : a, b, c \in \mathbb{R}\right\},$$
(f)
$$\left\{\begin{pmatrix} a & b \\ 0 & a \end{pmatrix} : a, b \in \mathbb{R}\right\},$$

(2) Encuentre todos los subanillos de $\mathbb{Z}_4$, $\mathbb{Z}_5$, $\mathbb{Z}_{12}$, $\mathbb{Z}$. Cuáles de estos son ideales?
(3) Encuentre el menor subanillo de $\mathbb{R}$ que contiene a $\mathbb{Z}$ y al número π.
(4) ¿ Es $\mathbb{Z}_3$ un subanillo de $\mathbb{Z}$? ¿ De $\mathbb{Z}_6$? ¿Por qué?
(5) Encuentre un anillo de 17 elementos. Encuentre un anillo de 17 elementos que no sea unitario.
(6) Suponga que S_1 es subanillo de A_1 y que S_2 es subanillo de A_2. Demuestre que $S_1 \times S_2$ es subanillo de $A_1 \times A_2$. ¿Es cualquier subanillo de $A_1 \times A_2$ de esa forma?
(7) En $\mathbb{Z}$ demuestre que $\langle m\rangle \cap \langle n\rangle = \langle [n, m]\rangle$, donde $[n, m]$ es el mínimo común múltiplo de n y m.
(8) En el anillo $C[0, 1]$ de todas las funciones reales continuas sobre $[0, 1]$ demuestre que $\mathcal{I} = \{f \in C[0, 1] : f(\frac{1}{2} = 0\}$ es un ideal.
(9) Demuestre que en $M_2(\mathbb{R})$ no hay ideales no triviales.
(10) Demuestre que en $\mathbb{Z}_n$, $\langle \underline{a}\rangle = \langle \underline{m - a}\rangle$. ¿Puede decir por qué ocurre esto? ¿Qué puede decir de elementos a, b tales que $\langle \underline{a}\rangle = \langle \underline{b}\rangle$? Demuestre el lema 3.3.
(11) Demuestre que el conjunto de los polinomios de $\mathbb{Z}[x]$ tales que todos sus coeficientes son divisibles por 3 es un ideal principal de $\mathbb{Z}[x]$.
(12) Demuestre el teorema 3.9.

3. Homomorfismos e Isomorfismos

DEFINICIÓN 3.8. Sean A y B dos anillos. Una función $f : A \longrightarrow B$ es un *homomorfismo* si y sólo si

$$\begin{aligned} f(x+y) &= f(x)+f(y) \\ f(xy) &= f(x)f(y). \end{aligned}$$

Es importante notar que las operaciones que aparecen a la izquierda de las ecuaciones anteriores no son las mismas que aparecen en el lado derecho. Las primeras corresponden a las operaciones del anillo A y las segundas a las del anillo B. En rigor deberiamos usar símbolos distintos, sin embargo, usamos los mismos ya que, como en general no hay posibilidad de confusión, esta es la práctica común.

TEOREMA 3.10. *Si f es un homomorfismo,*

(1) $f(\mathbf{0}) = \mathbf{0}$
(2) $f(-a) = -f(a)$

DEMOSTRACIÓN. Para demostrar (1),

$$f(\mathbf{0}) = f(\mathbf{0}+\mathbf{0}) = f(\mathbf{0}) + f(\mathbf{0}).$$

Restando $f(\mathbf{0})$ a cada lado,

$$\mathbf{0} = f(\mathbf{0}).$$

Para demostrar (2),

$$f(a) + f(-a) = f(a-a) = f(\mathbf{0}) = \mathbf{0},$$

$$f(-a) + f(a) = f(-a+a) = f(\mathbf{0}) = \mathbf{0},$$

luego por la unicidad del inverso aditivo, $f(-a) = -f(a)$. □

EJEMPLOS 3.5. (1)

$$\begin{aligned} f : \mathbb{Z} &\longrightarrow \mathbb{Z}_n \\ k &\longmapsto \underline{k} \end{aligned}$$

(2)

$$\begin{aligned} f : \mathbb{Z} &\longrightarrow \mathbb{Q}[x] \\ k &\longmapsto k \end{aligned}$$

(3)

$$\begin{aligned} f : \mathbb{Z} &\longrightarrow A \\ k &\longmapsto \mathbf{0} \end{aligned}$$

donde A es un anillo cualquiera. Este se llama el *homomorfismo trivial*.

(4)

$$\begin{array}{rcl} f:\mathbb{C} & \longrightarrow & M_2(\mathbb{R}) \\ a+bi & \longmapsto & \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \end{array}$$

La siguiente definición introduce cierta nomenclatura muy usada.

DEFINICIÓN 3.9. Si $f : A \longrightarrow B$ es un homomorfismo, diremos que f es:

(1) *monomorfismo* si f es inyectiva.
(2) *epimorfismo* si f es sobreyectiva.
(3) *isomorfismo* si f es biyectiva.
(4) *automorfismo* si f es isomorfismo y $A = B$.

DEFINICIÓN 3.10. Si $f : A \longrightarrow B$ es un homomorfismo,

(1)
$$ker\ f = \{a \in A : f(a) = \mathbf{0}\}$$
es el *núcleo* o *kernel* de f.

(2)
$$Im\ f = \{f(a) : a \in A\}$$
es la *imagen* de A por f.

TEOREMA 3.11. *Si $f : A \longrightarrow B$ es homomorfismo, entonces*

(1) *$ker\ f$ es un ideal de A.*
(2) *$Im\ f$ es un subanillo de A.*

DEMOSTRACIÓN. (1) En primer lugar, como $\mathbf{0} \in ker\ f$, éste no es vacío.
Sean a y b dos elementos del kernel de f. Entonces

$$f(a-b) = f(a) - f(b) = \mathbf{0} - \mathbf{0} = \mathbf{0},$$

luego $a - b \in ker\ f$.

Si $a \in ker\ f$ y $r \in A$, entonces

$$f(ar) = f(a)f(r) = \mathbf{0}f(r) = \mathbf{0},$$

luego $ar \in ker\ f$. Analogamente, $ra \in ker\ f$. Por lo tanto $ker\ f$ es un ideal de A.

(2) Como $f(\mathbf{0}) = \mathbf{0}$, $Im\ f$ no es vacío.

Sean r y s elementos de $Im\ f$. Entonces existen $a, b \in A$ tales que

$$r = f(a) \text{ y } s = f(b).$$

Por lo tanto

$$r - s = f(a) - f(b) = f(a-b) \in Im\ f$$

y

$$rs = f(a)f(b) = f(ab) \in Im\ f,$$

o sea, $Im\ f$ es cerrado bajo diferencias y productos, luego por el teorema 3.2, $Im\ f \leq B$. □

Luego de demostrar el teorema anterior, resulta natural preguntarse si $Im\ f$ es o no un ideal de B. El siguiente ejemplo responde esta pregunta.

Ejemplos 3.6. Consideremos la función

$$\begin{aligned} f : \mathbb{Z} &\longrightarrow \mathbb{Z} \times \mathbb{Z} \\ n &\longmapsto (n, n) \end{aligned}$$

f es un homomorfismo sin embargo $Im\ f$ no es un ideal de B ya que, por ejemplo,

$$(1, 0) \cdot (2, 2) = (2, 0) \notin Im\ B.$$

Teorema 3.12. *Sea $f : A \longrightarrow B$ un homomorfismo, entonces*

$$f \text{ es 1–1 si y sólo si } ker\ f = \{\mathbf{0}\}.$$

Demostración. Ejercicio. □

El siguiente teorema, conocido a veces como teorema del homomorfismo, es una suerte de recíproco del teorema 3.11 (1). En el demostramos que todo ideal es el núcleo de algún homomorfismo.

Teorema 3.13. *Sea $\mathcal{I}$ un ideal de A, entonces*

$$\begin{aligned} \pi : A &\longrightarrow A \mid \mathcal{I} \\ a &\longmapsto a + \mathcal{I} \end{aligned}$$

es un homomorfismo. Este se llama el homomorfismo canónico.
Más aún, $ker\ \pi = \mathcal{I}$.

Demostración. Por la forma en que se definieron las operaciones de $A \mid \mathcal{I}$, π es obviamente un homomorfismo.

Para ver que $ker\ \pi = \mathcal{I}$, basta notar que

$$\begin{aligned} a \in ker\ \pi \quad &\text{si y sólo si} \quad \pi(a) = \mathcal{I} \\ &\text{si y sólo si} \quad a + \mathcal{I} = \mathcal{I} \\ &\text{si y sólo si} \quad a \in \mathcal{I}. \end{aligned}$$

□

Teorema 3.14. **Primer Teorema de Isomorfismo**
Sea $f : A \longrightarrow B$ un epimorfismo, entonces

$$\begin{aligned} \varphi : A \mid ker\ f &\longrightarrow B \\ a + ker\ f &\longmapsto f(a) \end{aligned}$$

es un isomorfismo.

DEMOSTRACIÓN. Debemos demostrar primero que φ es una función bien definida, es decir, no depende del representante de la clase de equivalencia que estemos usando.

Tenemos que

$$\varphi(a + ker\ f) = \varphi(b + ker\ f)$$

si y sólo si

$$f(a) = f(b)$$

si y sólo si

$$f(a - b) = f(a) - f(b) = \mathbf{0}$$

si y sólo si

$$a - b \in ker\ f$$

si y sólo si

$$a + ker\ f = b + ker\ f,$$

y esto demuestra no sólo que φ está bien definida ($\Leftarrow$), sino también que es inyectiva ($\Rightarrow$).

Por otra parte, como

$$\begin{aligned} \varphi((a + ker\ f) + (b + ker\ f)) &= \varphi((a + b) + ker\ f) \\ &= f(a + b) \\ &= f(a) + f(b) \\ &= \varphi(a + ker\ f) + \varphi(b + ker\ f), \end{aligned}$$

$$\begin{aligned} \varphi((a + ker\ f) \cdot (b + ker\ f)) &= \varphi((ab) + ker\ f) \\ &= f(ab) \\ &= f(a)f(b) \\ &= \varphi(a + ker\ f)\varphi(b + ker\ f), \end{aligned}$$

φ es un homomorfismo.

Por último, si $b \in B$, como f es sobreyectiva, existe $a \in A$ tal que $b = f(a)$, luego

$$b = \varphi(a + ker\ f).$$

Por lo tanto φ es sobreyectiva. □

EJEMPLOS 3.7. Sea A el anillo de todas las funciones $f : \mathbb{R} \longrightarrow \mathbb{R}$ con las operaciones definidas como en el ejemplo 3.1 (5) y sea

$$\mathcal{I} = \{f \in A : f(0) = 0\}.$$

Podemos fácilmente verificar que $\mathcal{I}$ es un ideal de A. Si definimos

$$\begin{array}{rcl} \varphi : A & \longrightarrow & \mathbb{R} \\ f & \longmapsto & f(0), \end{array}$$

entonces

$$\varphi(f+g) = (f+g)(0) = f(0) + g(0) = \varphi(f) + \varphi(g)$$

$$\varphi(f \cdot g) = (f \cdot g)(0) = f(0)\ g(0) = \varphi(f)\ \varphi(g),$$

o sea, φ es un homomorfismo.

Obviamente φ es sobreyectiva, en efecto, si $r \in \mathbb{R}$ consideramos la función constante $f(x) = r$. Entonces

$$r = \varphi(f).$$

Sea $f \in ker\ \varphi$, entonces $f(0) = 0$, luego

$$ker\ \varphi = \mathcal{I}.$$

Por lo tanto, en virtud del teorema anterior,

$$A \mid I \ \text{ es isomorfo a } \ \mathbb{R}.$$

Ejercicios 3.3. (1) Para cada uno de los siguientes casos, determine si $\varphi : \mathbb{Z}_3 \longrightarrow \mathbb{Z}_3$ es inyectiva, sobreyectiva, homomorfismo, isomorfismo.
   (a) $\varphi(x) = 2x$,
   (b) $\varphi(x) = 2 + x$,
   (c) $\varphi(x) = -x$,
   (d) $\varphi(x) = x^2$,
   (e) $\varphi(x) = x^3$.

(2) Repita el ejercicio anterior con $\mathbb{Z}_3$ reemplazado por $\mathbb{Z}_5$, $\mathbb{Z}_6$, $\mathbb{Z}_m$.

(3) Verifique que la función

$$\begin{array}{rcl} \varphi : \mathbb{Z}_{18} & \longrightarrow & \mathbb{Z}_6 \\ \underline{a}_{18} & \longmapsto & \underline{a}_6, \end{array}$$

donde $\underline{a}_m$ es la clase de a módulo m, es un homomorfismo. ¿ Es φ sobreyectiva? ¿ Cuál es su kernel?

(4) Suponga que $m \mid n$. Generalizamos el problema anterior definiendo

$$\begin{array}{rcl} \varphi : \mathbb{Z}_n & \longrightarrow & \mathbb{Z}_m \\ \underline{a}_n & \longmapsto & \underline{a}_m. \end{array}$$

Demuestre que este es un epimorfismo. Encuentre su kernel.

¿Qué sucede si $m \nmid n$?

(5) Considere los anillos

$$\begin{aligned} \mathbb{Z}[i] &= \{a+bi : a,b \in \mathbb{Z}\}, \\ \mathbb{Z}[\sqrt{2}] &= \{a+b\sqrt{2} : a,b \in \mathbb{Z}\}, \\ \mathbb{Z}[\sqrt{3}] &= \{a+b\sqrt{3} : a,b \in \mathbb{Z}\}. \end{aligned}$$

¿Son algunos de estos isomorfos? Encuentre todos los isomorfismos de $\mathbb{Z}$ en $\mathbb{Z}$. De $\mathbb{Z}$ en $\mathbb{Z}_6$. De $\mathbb{Z}$ en $\mathbb{Z}_m$. De $\mathbb{Z}_n$ en $\mathbb{Z}_m$.

Indicación: Demuestre primero que todo homomorfismo φ con dominio $\mathbb{Z}$ o $\mathbb{Z}_n$ está determinado por $\varphi(1)$. ¿Es esto cierto si el dominio es otro anillo?

(6) Demuestre el teorema 3.12.

CAPITULO 4

Cuerpos

En este capítulo estudiaremos algunos aspectos relacionados con la división en un anillo, nos interesa por ejemplo estudiar anillos en los que todos sus elementos, o casi todos, son *unidades*, es decir, aquellos elementos $a \in A$, tales que existe $b \in A$ y

$$ab = ba = \mathbf{1}.$$

1. Definiciones y Ejemplos

DEFINICIÓN 4.1. Un anillo conmutativo y unitario es un *cuerpo* si todo elemento distinto de $\mathbf{0}$ tiene un inverso multiplicativo.

Es fácil ver que el inverso multiplicativo de a es único. Esto nos autoriza a denotarlo con un símbolo especial a^{-1}. Es decir, si $a \neq \mathbf{0}$,

$$aa^{-1} = a^{-1}a = \mathbf{1}.$$

EJEMPLOS 4.1.

(1) Los ejemplos clásicos son los cuerpos de números $\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{C}$.
(2) El subconjunto de $\mathbb{R}$

$$\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\},$$

dotado de las operaciones habituales, es un cuerpo. El inverso de $a + b\sqrt{2}$ es

$$\frac{a}{a^2 - 2b^2} - \frac{b}{a^2 - 2b^2}\sqrt{2}.$$

(3) Las clases residuales módulo un número primo, $\mathbb{Z}_p$, forman un cuerpo. Este es un caso particular de un teorema mucho más general, sin embargo daremos aquí una demostración directa.

Consideremos las clases residuales

$$\underline{1}, \underline{2}, \ldots, \underline{p-1},$$

Como p es primo, p es primo relativo con 1, 2, . . . ,$p - 1$, luego para $1 \leq a < p$, existen enteros m y n tales que

$$na + mp = 1,$$

o, lo que es lo mismo,

$$na \equiv 1 \ (\mod p),$$

es decir,

$$\underline{n}\ \underline{a} = \underline{na} = \underline{1},$$

o sea, $\underline{n}$ es el inverso de $\underline{a}$.

OBSERVACIÓN 4.1.

(1) En un cuerpo no hay divisores del cero, es decir, todo cuerpo es un dominio de integridad. En efecto, supongamos que $a \neq \mathbf{0}$ y existe b tal que

$$ab = \mathbf{0}.$$

Entonces, multiplicando ambos miembros por a^{-1} tenemos

$$a^{-1}(ab) = a^{-1}\mathbf{0} = \mathbf{0},$$

o sea,

$$b = \mathbf{0}.$$

(2) Un cuerpo no tiene ideales no triviales. Si I fuera un ideal distinto de $\{\mathbf{0}\}$ del cuerpo K, entonces existe $a \neq \mathbf{0}$ en I. Pero entonces

$$\mathbf{1} = a^{-1}a \in I,$$

luego $I = K$.

EJERCICIOS 4.1. (1) Demuestre que si $a \neq \mathbf{0}$, entonces su inverso multiplicativo es único.

(2) Una *función racional* sobre $\mathbb{Q}$ es una función del tipo

$$\frac{p(x)}{q(x)},$$

donde $p(x)$, $q(x) \in \mathbb{Q}[x]$, $q(x)$ no trivial. Demuestre que el conjunto $\mathbb{Q}(x)$ de todas las funciones racionales sobre $\mathbb{Q}$ dotado de las operaciones obvias es un cuerpo.

2. Cuerpo de Cuocientes

Como sabemos, existe una estrecha relación entre $\mathbb{Q}$ y $\mathbb{Z}$, a saber, $\mathbb{Q}$ es el cuerpo más pequeño que contiene a $\mathbb{Z}$. Probablemente el lector conoce la construcción de los números racionales a partir de los enteros, (si no la conoce, no importa, será un caso particular de lo que haremos aquí). Esa construcción se puede generalizar a cualquier dominio de integridad D y se conoce como el *cuerpo de cuocientes* de D.

La idea es muy sencilla, se trata de agregar los inversos multiplicativos de todos aquellos elementos de D que no lo tengan.

Sea D un dominio de integridad. Sobre $D \times (D - \{\mathbf{0}\})$ definimos la siguiente relación:

$$(a, b) \sim (c, d) \text{ si y sólo si } ad = cb.$$

La demostración de que esta es una relación de equivalencia es muy fácil y se deja como ejercicio. Denotaremos la clase de equivalencia del par (a, b) con el símbolo $\frac{a}{b}$, i.e.

$$\frac{a}{b} = \{(c, d) \in D \times (D - \{\mathbf{0}\}) : ad = cb\}.$$

TEOREMA 4.1. *Sea D un dominio de integridad. Sobre el conjunto F de las clases de equivalencia del párrafo anterior definimos las operaciones:*

$$\begin{aligned} \frac{a}{b} + \frac{c}{d} &= \frac{ad + cb}{bd} \\ \frac{a}{b} \cdot \frac{c}{d} &= \frac{ac}{bd}. \end{aligned}$$

Entonces F con estas operaciones es un cuerpo.

DEMOSTRACIÓN. Esta demostración es muy sencilla y rutinaria. La única sutileza es que debemos demostrar que las operaciones están bien definidas, es decir, que no dependen del representante de las clases de equivalencia que hayamos usado. (Algo similar a lo que se hizo para las operaciones entre clases residuales). Observemos primero que como D es dominio de integridad y b,d son no nulos, entonces $bd \neq \mathbf{0}$. Supongamos ahora que

$$(a, b) \sim (a', b') \text{ y } (c, d) \sim (c', d'),$$

o sea,

$$ab' = a'b \text{ y } cd' = c'd.$$

Entonces, multiplicando la primera ecuación por dd', la segunda por bb' y sumando miembro a miembro,

$$ab'dd' + cd'bb' = a'bdd' + c'dbb',$$

luego

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

o sea,

$$\frac{ad + cb}{bd} = \frac{a'd' + c'b'}{b'd'}.$$

Luego la suma de clases de equivalencia no depende de los representantes usados. Algo similar se demuestra para el producto de clases.

La asociatividad y la conmutatividad de ambas operaciones, así como la distributividad del producto sobre la suma no las demostraremos aquí .

El neutro aditivo es la clase $\frac{\mathbf{0}}{\mathbf{1}}$. Obsérvese que $\frac{a}{b}$ es la clase nula si y sólo si $a = \mathbf{0}$. En efecto,

$$\frac{a}{b} = \frac{\mathbf{0}}{\mathbf{1}}$$

si y sólo si

$$a\mathbf{1} = \mathbf{0}b$$

si y sólo si

$$a = \mathbf{0}.$$

El neutro multiplicativo es la clase $\frac{\mathbf{1}}{\mathbf{1}}$. Podemos observar que $\frac{a}{b}$ es la clase neutra si y sólo si $a = b$.

Está claro que F no hay divisores del cero, ya que $\frac{a}{b} \cdot \frac{c}{d}$ es la clase nula si y sólo si $ac = \mathbf{0}$. Pero como D es dominio de integridad, esto implica que $a = \mathbf{0}$ o bien $c = \mathbf{0}$, o sea, $\frac{a}{b} = \mathbf{0}$ o bien $\frac{c}{d} = \mathbf{0}$. Luego F es un dominio de integridad.

Por último, debemos ver que las clases no nulas tienen inverso multiplicativo. Para ello basta comprobar que

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

Observemos que $\frac{b}{a}$ está bien definido ya que $a \neq \mathbf{0}$.

Esto completa la demostración de que F es un cuerpo. □

El cuerpo F del teorema anterior se llama el *cuerpo de cuocientes* de D y tiene con este una estrecha relación. En un sentido que precisaremos a continuación, es el cuerpo más pequeño que "contiene" a D. Notemos que F es en particular un anillo y que la función

$$\begin{array}{rcl} f : D & \longrightarrow & F \\ a & \longmapsto & \dfrac{a}{\mathbf{1}} \end{array}$$

es un monomorfismo de anillos. Luego, si identificamos D con su imagen isomorfa $f(D)$, podemos decir que F contiene a D. Aunque esto no es estrictamente correcto, no se corre ningún peligro ya que los anillos D y $f(D)$ son "iguales" desde el punto de vista algebraico. Como sabemos, el cuerpo de cuocientes de $\mathbb{Z}$ es $\mathbb{Q}$ y estamos acostumbrados a identificar el entero n con el racional $\frac{n}{1}$, de hecho, usamos el mismo símbolo para ambos.

TEOREMA 4.2. *Sea D un dominio de integridad y F su cuerpo de cuocientes. Entonces F contiene un subanillo D^* isomorfo a D.*

El siguiente teorema nos dice que el cuerpo de cuociente de D es el más pequeño cuerpo que lo contiene.

TEOREMA 4.3. *Sea D un dominio de integridad y F su cuerpo de cuocientes. Si K es un cuerpo que contiene a D, entonces K contiene un subcuerpo F^* isomorfo a F y tal que $D \subseteq F^* \subseteq K$.*

DEMOSTRACIÓN. La función

$$\begin{array}{rcl} f : F & \longrightarrow & K \\ \frac{a}{b} & \longmapsto & ab^{-1} \end{array}$$

es claramente un monomorfismo, luego F es isomorfo a $F^* = f(F) \subseteq K$.

Es claro también que si $a \in D$, entonces $a = f(\frac{a}{\mathbf{1}}) \in F^*$, luego $D \subseteq F^*$. □

COROLARIO 4.4. *El cuerpo de cuocientes de un cuerpo es (isomorfo a) el mismo cuerpo.*

EJEMPLOS 4.2. (1) El cuerpo de cuocientes de $\mathbb{Z}$ es $\mathbb{Q}$.

(2) El cuerpo de cuocientes de $\mathbb{Q}[x]$ es el cuerpo de las llamadas *funciones racionales* sobre $\mathbb{Q}$:

$$\mathbb{Q}(x) = \{\frac{p(x)}{q(x)} : p(x) \in \mathbb{Q}[x],\ q(x) \in \mathbb{Q}[x]^*, q(x) \neq 0\}.$$

EJERCICIOS 4.2. (1) Demuestre que la relación $\sim$ definida al principio de esta sección es de equivalencia.

(2) Demuestre que el producto de clases de equivalencia definido al principio de esta sección está bien definido.

(3) Demuestre que el cuerpo de cuocientes de un dominio D con las operaciones definidas verifican todos los axiomas de un anillo conmutativo y unitario.

3. Característica de un Cuerpo

DEFINICIÓN 4.2. Se dice que un cuerpo K tiene *característica* p si p es el menor entero tal que para todo $x \in K$,

$$px = \underbrace{x + x + \cdots + x}_{p} = 0.$$

Si tal p no existe, la característica de K es 0.

EJEMPLOS 4.3. (1) $\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{C}$ tienen característica 0.

(2) El cuerpo $\mathbb{Q}(x)$ de las funciones racionales sobre $\mathbb{Q}$ también tiene característica 0.

(3) $\mathbb{Z}_p$, donde p es primo tiene característica p.

TEOREMA 4.5. *La característica de un cuerpo es* 0 *o un número primo.*

DEMOSTRACIÓN. Si la característica del cuerpo K no es 0, entonces sea p el menor entero tal que $px = 0$ para todo $x \in K$. Tal entero tiene que existir por el Principio de Buen Orden.

Supongamos que $p = mn$, con m, $n < p$, entonces,

$$(m\mathbf{1})(n\mathbf{1}) = (\underbrace{\mathbf{1} + \mathbf{1} + \cdots + \mathbf{1}}_{m})(\underbrace{\mathbf{1} + \mathbf{1} + \cdots + \mathbf{1}}_{n}) = (\underbrace{\mathbf{1} + \mathbf{1} + \cdots + \mathbf{1}}_{p}) = p\mathbf{1} = \mathbf{0}.$$

Pero K es un cuerpo luego no tiene divisores del cero, por lo tanto

$$m\mathbf{1} = \mathbf{0} \text{ o bien } n\mathbf{1} = \mathbf{0}.$$

Si tomamos cualquier $x \in K$, $x = \mathbf{1}x$, luego

$$mx = \underbrace{x + x + \cdots x}_{m} = \underbrace{\mathbf{1}x + \mathbf{1}x + \cdots + \mathbf{1}x}_{m} = (\underbrace{\mathbf{1} + \mathbf{1} + \cdots + \mathbf{1}}_{m})x = (m\mathbf{1})x = \mathbf{0},$$

o bien

$$nx = \underbrace{x + x + \cdots x}_{n} = \underbrace{\mathbf{1}x + \mathbf{1}x + \cdots + \mathbf{1}x}_{n} = (\underbrace{\mathbf{1} + \mathbf{1} + \cdots + \mathbf{1}}_{n})x = (n\mathbf{1})x = \mathbf{0},$$

y esto contradice la minimalidad de p. □

Observación 4.2. Observemos que en el último teorema no usamos toda la fuerza del cuerpo K sino sólo el hecho de que K no tiene divisores del cero. De hecho, es habitual definir de la misma manera la característica de un dominio de integridad y el teorema anterior también es válido.

Teorema 4.6. *Todo cuerpo contiene un subcuerpo isomorfo a $\mathbb{Q}$ o un subcuerpo isomorfo a $\mathbb{Z}_p$, para algún primo p.*

Demostración. La idea es encontrar el menor subcuerpo del cuerpo K. En primer lugar, denotemos

$$\boldsymbol{n} = \begin{cases} \underbrace{\mathbf{1} + \mathbf{1} + \cdots + \mathbf{1}}_{n}, & \text{si } n > 0 \\ \underbrace{(-\mathbf{1}) + (-\mathbf{1}) + \cdots + (-\mathbf{1})}_{n}, & \text{si } n < 0. \end{cases}$$

Si K tiene característica un primo p, entonces el conjunto

$$\{\mathbf{0}, \mathbf{1}, \ldots, \boldsymbol{p-1}\},$$

es un subcuerpo obviamente isomorfo a $\mathbb{Z}_p$.

Si K tiene característica 0, entonces

$$A = \{\boldsymbol{n} : n \in \mathbb{Z}\},$$

es un subanillo de K y es obviamente isomorfo a $\mathbb{Z}$. Por lo tanto A es un dominio de integridad contenido en K luego (una copia isomorfa de) el cuerpo de cuocientes de A esta contenido en K. Por supuesto el cuerpo de cuocientes de A tiene que ser isomorfo al cuerpo de cuocientes de $\mathbb{Z}$, vale decir, a $\mathbb{Q}$.

Podemos ser más explícitos y definir

$$\begin{array}{rcl} f : \mathbb{Q} & \longrightarrow & K \\ \dfrac{m}{n} & \longmapsto & \boldsymbol{m}(\boldsymbol{n})^{-1}. \end{array}$$

Esta función provee el isomorfismo mencionado. □

EJERCICIOS 4.3. (1) Demuéstre que en un cuerpo de característica $p \neq 0$, para todo a, b

$$(a+b)^p = a^p + b^p.$$

(2) Si K es un cuerpo de característica $p \neq 0$, y definimos

$$\begin{aligned} f : K &\longrightarrow K \\ a &\longmapsto a^p \end{aligned}$$

entonces f es un isomorfismo.

4. Extensiones Simples de $\mathbb{Q}$

DEFINICIÓN 4.3. Un número $\alpha \in \mathbb{C}$ se dice *algebraico sobre* $\mathbb{Q}$ si existe un polinomio $p(x) \in \mathbb{Q}[x]$ tal que $p(\alpha) = 0$.

Si α no es algebraico sobre $\mathbb{Q}$ se dice que es *trascendente sobre* $\mathbb{Q}$.

EJEMPLOS 4.4. (1) $\sqrt{2}$ es algebraico sobre $\mathbb{Q}$ ya que es raiz de $x^2 - 1$.

(2) i es algebraico sobre $\mathbb{Q}$ ya que es raiz de $x^2 + 1$.

(3) los números reales π y e son trascendentes sobre $\mathbb{Q}$. La demostración de este resultado es muy difícil, sólo se logró durante el siglo pasado.

TEOREMA 4.7. *Si α es algebraico sobre $\mathbb{Q}$, entonces existe un (único) polinomio mónico irreducible del cual α es raiz. Este se llama* polinomio mínimal *de α.*

Si $p(x)$ es el polinomio minimal de α y $f(x)$ es un polinomio tal que $f(\alpha) = 0$, entonces $p(x) \mid f(x)$.

DEMOSTRACIÓN. Consideremos el ideal

$$I = \{f(x) \in \mathbb{Q}[x] : f(\alpha) = 0\}$$

de $\mathbb{Q}[x]$.

Como $\mathbb{Q}[x]$ es un dominio de ideales principales, I es el ideal generado por un polinomio $p(x)$. Dividiendo por el coeficiente del término de mayor grado obtenemos un polinomio mónico.

Es claro que $p(x)$ es irreducible ya que es de grado minimal en el ideal y si no fuera irreducible, existirían polinomios $r(x)$ y $s(x)$ de grado menor tales que $p(x) = r(x)\ s(x)$, luego

$$r(\alpha)\ s(\alpha) = p(\alpha) = 0.$$

o sea,

$$r(\alpha) = 0 \text{ o bien } s(\alpha) = 0,$$

contradiciendo la minimalidad del grado de $p(x)$.

Por último, si $f(\alpha) = 0$, entonces $f(x) \in I$, luego $p(x) \mid f(x)$. □

DEFINICIÓN 4.4. El *grado* de α es el grado de su polinomio minimal.

Definición 4.5. Sea $\alpha \in \mathbb{C}$. Definimos $\mathbb{Q}(\alpha)$ como el menor cuerpo que contiene a $\mathbb{Q}$ y a α.

En tal caso $\mathbb{Q}(\alpha)$ se dice una em extensión simple de $\mathbb{Q}$.

En el próximo teorema veremos que $\mathbb{Q}(\alpha)$ existe para cualquier α, sin embargo, obtenemos cuerpos muy distintos dependiendo de si α es algebraico o trascendente.

Teorema 4.8.

(1) *Si α es algebraico y su polinomio minimal es de grado n, entonces*

$$\mathbb{Q}(\alpha) = \{a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} : a_i \in \mathbb{Q}, 0 \leq i < n\}.$$

(2) *Si α es trascendente, entonces*

$$\mathbb{Q}(\alpha) \cong \mathbb{Q}(x).$$

Demostración. (1)

Sea $K = \{a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} : a_i \in \mathbb{Q}, 0 \leq i < n\}$.

Es fácil ver que K es un subanillo (conmutativo y) unitario de $\mathbb{C}$ que contiene a α y a $\mathbb{Q}$. Para ver que se trata de un cuerpo, basta verificar que todo elemento no nulo tiene inverso multiplicativo.

Para demostrar esto, sea

$$\beta = a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} \in K,$$

y sea $p(x)$ el polinomio minimal de α.

Llamemos $q(x)$ al polinomio de grado $n-1$ asociado con β de la manera obvia:

$$q(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1}.$$

Como $p(x)$ es irreducible y $\partial q(x) < n$, $p(x)$ y $q(x)$ son primos relativos, luego existen polinomios $r(x)$ y $s(x)$ tales que

$$1 = r(x)q(x) + s(x)p(x).$$

Es claro que podemos suponer que $\partial r(x) < \partial p(x)$, pues si no,

$$r(x) = p(x)r'(x) + r''(x), \text{ con } \partial r''(x) < \partial p(x),$$

y

$$1 = (p(x)r'(x) + r''(x))q(x) + s(x)p(x) = r''(x)q(x) + (s(x) + r'(x)q(x))p(x).$$

Pero entonces

$$1 = r(\alpha)q(\alpha) + s(\alpha)p(\alpha) = r(\alpha)q(\alpha),$$

ya que $p(\alpha) = 0$, luego

$$[q(\alpha)]^{-1} = r(\alpha) \in K.$$

Finalmente basta observar que todo cuerpo que contiene a α y a $\mathbb{Q}$ debe contener a K, luego este es el menor cuerpo que los contiene, es decir, $K = \mathbb{Q}(\alpha)$.

(2)

En primer lugar, debemos observar que

$$\mathbb{Q}(\alpha) = \{\frac{p(\alpha)}{q(\alpha)} : p(x), q(x) \in \mathbb{Q}[x] \text{ y } q(x) \neq 0\},$$

donde

$$\frac{p(\alpha)}{q(\alpha)} = p(\alpha)(q(\alpha))^{-1}.$$

En efecto, como α es trascendente,

$$p(\alpha) = 0 \text{ si y sólo si } p(x) = 0,$$

o sea, $p(x)$ es el polinomio nulo. Luego si $q(x) \neq 0$, $q(\alpha)$ tiene inverso multiplicativo (en $\mathbb{C}$). Enseguida es fácil ver que el conjunto arriba definido es el menor cuerpo que contiene a $\mathbb{Q}$ y a α. Definimos ahora

$$\begin{array}{rccc} F : \mathbb{Q}(x) & \longrightarrow & \mathbb{Q}(\alpha) \\ \dfrac{p(x)}{q(x)} & \longmapsto & \dfrac{p(\alpha)}{q(\alpha)}. \end{array}$$

La función está bien definida, ya que si

$$\frac{p(x)}{q(x)} = \frac{p'(x)}{q'(x)},$$

$$p(x)q'(x) = p'(x)q(x),$$

luego como

$$q(\alpha) \neq 0 \text{ y } q'(\alpha) \neq 0,$$

existen sus inversos multiplicativos y obtenemos

$$\frac{p(\alpha)}{q(\alpha)} = \frac{p'(\alpha)}{q'(\alpha)}.$$

La función así definida es obviamente sobreyectiva. Para verificar que F es inyectiva, supongamos que

$$F(\frac{p(x)}{q(x)}) = F(\frac{p'(x)}{q'(x)}),$$

o sea,

$$\frac{p(\alpha)}{q(\alpha)} = \frac{p'(\alpha)}{q'(\alpha)},$$

o bien,

$$p(\alpha)q'(\alpha) = p'(\alpha)q(\alpha),$$

es decir, α es raiz del polinomio

$$p(x)q'(x) - p'(x)q(x),$$

lo que es una contradicción a menos que este sea el polinomio nulo, o sea,

$$\frac{p(x)}{q(x)} = \frac{p'(x)}{q'(x)},$$

y la función es inyectiva.

Por último debemos verificar que F es un homomorfismo. Esto es evidente dado cómo se definieron las operaciones en $\mathbb{Q}(x)$. □

Ejemplos 4.5. El teorema anterior nos da además un algoritmo para encontrar el inverso multiplicativo de cualquier elemento de una extensión simple. El caso interesante es el de las extensiones algebraicas, ya que para una extensión trascendente, el inverso se encuentra simplemente intercambiando numerador y denominador de la función racional respectiva.

Encontremos por ejemplo el inverso de $a = 1 - \sqrt[3]{3} + \sqrt[3]{9} \in \mathbb{Q}(\sqrt[3]{3})$.

Como el polinomio minimal de $\sqrt[3]{3}$ es $x^3 - 3$, de acuerdo con la demostración del teorema anterior, sólo tenemos que encontrar polinomios $\alpha(x)$ y $\beta(x)$ tales que

$$\alpha(x)\ x^3 - 3 + \beta(x)\ x^2 - x + 1 = 1.$$

$\alpha(\sqrt[3]{3})$ será el inverso de a.

Para encontrar esos polinomios, aplicamos el algoritmo de Euclides lo que nos da

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

El lector puede verificar fácilmente que $\frac{1}{4}\sqrt[3]{3} + \frac{1}{4}$ es el inverso multiplicativo de a.

Ejercicios 4.4.

(1) Demuestre que los siguientes números son algebraicos sobre $\mathbb{Q}$.
   (a) $\sqrt{2} + \sqrt{3}$.
   (b) $2 - 3i$.
   (c) $\sqrt{a} + \sqrt{b}$, para cualquier par de enteros positivos a y b.
   (d) $a + bi$ para cualquier par de racionales a y b.
(2) Encuentre los grados de los números del ejercicio anterior.
(3) Demuestre que π^2 y $\frac{\pi+1}{\pi}$ son trascendentes sobre $\mathbb{Q}$.
(4) Considere el polinomio $p(x) = x^4 - 3x^3 + 2x^2 + x - 1$ y evalúelo en a para los siguientes casos.
   (a) $a = 3 - 2\sqrt{2}$ en $\mathbb{Q}(\sqrt{2})$
   (b) $a = 1 - \sqrt[4]{2} + \sqrt[4]{8}$ en $\mathbb{Q}(\sqrt[4]{2})$.
   (c) $a = \sqrt[3]{3} - \sqrt[3]{9}$ en $\mathbb{Q}(\sqrt[3]{3})$.
   (d) $\frac{\pi+1}{\pi-1}$ en $\mathbb{Q}(\pi)$.
(5) Describa los siguientes ejemplos y demuestre directamente que son cuerpos.
   (a) $\mathbb{Q}(\sqrt{3})$

(b) $\mathbb{Q}(\sqrt[3]{2})$
(c) $\mathbb{Q}(\pi)$

(6) Encuentre los inversos multiplicativos siguientes.
(a) $3\sqrt{3}-1$ en $\mathbb{Q}(\sqrt{3})$
(b) $1-\sqrt[4]{2}+\sqrt[4]{4}-\sqrt[4]{8}$ en $\mathbb{Q}(\sqrt[4]{2})$.
(c) $\frac{\pi^3+1}{\pi^2+1}$ en $\mathbb{Q}(\pi)$

(7) Para los lectores que sepan lo que es un espacio vectorial.
Demuestre que si a es algebraico de grado n sobre $\mathbb{Q}$, entonces $\mathbb{Q}(a)$ es un espacio vectorial de dimensión n sobre $\mathbb{Q}$.

5. Obtención de Raices de Polinomios sobre $\mathbb{Q}$

En esta sección construiremos a partir de $\mathbb{Q}$ y de un polinomio cualquiera de $\mathbb{Q}[x]$ una extensión de $\mathbb{Q}$ que contiene una raiz de ese polinomio.

Necesitamos primero un lema y un teorema que relacionan varios conceptos anteriores.

LEMA 4.9. *Un anillo conmutativo y unitario es un cuerpo si y sólo si no tiene ideales no triviales.*

DEMOSTRACIÓN. Sea K un cuerpo y sea $I \neq \{\mathbf{0}\}$ un ideal de K. Entonces existe $a \neq \mathbf{0}$ en I. Pero entonces

$$\mathbf{1} = a^{-1}a \in I.$$

Luego para todo $b \in K$

$$b = b\mathbf{1} \in I,$$

es decir, $I = K$.

Sea ahora A un anillo conmutativo y unitario que no tiene ideales no triviales. Consideremos el ideal generado por cualquier elemento no nulo $a \in A$. Como sabemos,

$$\langle a \rangle = \{ax : x \in A\}.$$

Entonces $\langle a \rangle \neq \{\mathbf{0}\}$ ya que $a \in \langle a \rangle$, luego $\mathbf{1} \in \langle a \rangle$ o sea, existe $b \in A$ tal que

$$ab = ba = \mathbf{1},$$

es decir todo elemento no nulo de A tiene inverso multiplicativo y por lo tanto A es un cuerpo. □

TEOREMA 4.10. *Sea A un anillo conmutativo y unitario y sea M un ideal de A. Entonces M es maximal si y sólo si $A \mid M$ es un cuerpo.*

DEMOSTRACIÓN. Si M es in ideal maximal de A, debemos demostrar que todo elemento no nulo del anillo conmutativo y unitario $A \mid M$ tiene inverso multiplicativo. Obsérvese que si todo elemento no nulo tiene inverso, el anillo no contiene divisores del cero. Recordando que en $A \mid M$, $\mathbf{0} = M$, sea

$$a + M \in A \mid M,$$

donde $a + M \neq M$. Entonces $a \notin M$. Sea

$$N = \{xa + m : x \in A \text{ y } m \in M\}.$$

Entonces N es un ideal de A. En efecto, $a \in N$ ya que

$$a = \mathbf{1}a + \mathbf{0} \in N,$$

luego $N \neq \emptyset$. Además

$$x_1a + m_1 - (x_2a + m_2) = (x_1 - x_2)a + (m_1 - m_2) \in N,$$

luego N es cerrado bajo diferencias. Por otra parte, si $b \in A$,

$$(xa + m)b = b(xa + m) = (bx)a + bm \in N,$$

ya que M es ideal y por lo tanto $bm \in M$.

Obviamente $M \subseteq N$, ya que si $m \in M$,

$$m = \mathbf{0}a + m \in N.$$

Pero como $a \in N - M$, $N \neq M$, y como M es maximal, $N = A$.

En particular esto implica que $\mathbf{1} \in N$, luego

$$\mathbf{1} = ba + m,$$

para algún $b \in A$ y algún $m \in M$. Es decir

$$\mathbf{1} + M = ba + M = (b + M)(a + M),$$

o sea,

$$(a + M)^{-1} = b + M.$$

Esto completa la demostración de que $A \mid M$ es un cuerpo.

Supongamos ahora que $A \mid M$ es un cuerpo.

Sea N un ideal de A talque $M \subseteq N$. Queremos demostrar que o bien $M = N$, obien $N = A$.

Para ello observemos que $N \mid M$ es un ideal de $A \mid M$. En efecto, $N \mid M \neq \emptyset$ ya que $M \in N \mid M$. Además

$$(a + M) - (b + M) = a - b + M \in N \mid M,$$

para todo a, $b \in N$, o sea, $N \mid M$ es cerrado bajo diferencias. También, si $n + M \in N \mid M$ y $a + M \in A \mid M$, entonces

$$(a + M)(n + M) = an + M \in N \mid M,$$

y

$$(n + M)(a + M) = na + M \in N \mid M,$$

ya que N es ideal, luego $N \mid M$ absorve los elementos de $A \mid M$ y por lo tanto es un ideal.

Pero $A \mid M$ es un cuerpo así es que por el lema 4.9, sólo tiene ideales triviales, luego

$$N \mid M = \{M\},$$

en cuyo caso $N = M$, o bien

$$N \mid M = A \mid M,$$

es decir, $N = A$. Esto completa la demostración de que M es maximal. □

TEOREMA 4.11. *Sea $f(x) \in \mathbb{Q}[x]$. Entonces existe una extensión simple de $\mathbb{Q}$ que contiene una raiz de $f(x)$.*

DEMOSTRACIÓN. Sea $p(x) = a_0 + a_1x + \cdots + a_nx^n \in \mathbb{Q}[x]$ un polinomio irreducible tal que $p(x) \mid f(x)$. Obsérvese que cualquier raiz α de $p(x)$ es también una raiz de $f(x)$.

Consideremos ahora el ideal principal M de $\mathbb{Q}[x]$ generado por $p(x)$. Como M es maximal por el teorema 4.10, $K = \mathbb{Q}[x] \mid M$ es un cuerpo.

Es claro que K contiene una copia isomorfa de $\mathbb{Q}$ ya que la función

$$\begin{aligned} F : \mathbb{Q} &\longrightarrow \mathbb{Q}[x] \mid M \\ q &\longmapsto q + M, \end{aligned}$$

es un monomorfismo, podemos entonces considerar a K como una extensión de $\mathbb{Q}$.

Por último para ver que $p(x)$ tiene una raiz en K, basta notar que

$$\mathbf{0} = M = p(x) + M,$$

ya que $p(x) \in M$. Entonces, si $\alpha = x + M \in K$,

$$\mathbf{0} = p(x) + M = a_0 + a_1(x + M) + a_2(x + M)^2 \cdots + a_n(x + M)^n,$$

o sea, α es una raiz en K de $p(x)$. □

EJERCICIOS 4.5.

(1) Demuéstrese la afirmación hecha en el teorema 4.10: Si todo elemento no nulo de un anillo tiene inverso multiplicativo, entonces el anillo no tiene divisores del cero.
(2) Describa el cuerpo $\mathbb{Q}[x] \mid \langle x + 1\rangle$.
(3) Demuestre que $\mathbb{Q}(\sqrt{3})$ es isomorfo a $\mathbb{Q}[x] \mid \langle x^2 - 3\rangle$.
(4) Demuestre que $\mathbb{Q}[x] \mid \langle x^2 - 2\rangle$ no es isomorfo a $\mathbb{Q}[x] \mid \langle x^2 - 3\rangle$.
(5) Sea $A = \{a + bi : a,\ b \in \mathbb{Z}$ e $\mathcal{M} = \{a + bi : 3 \mid a$ y $3 \mid b\}$. Demuestre
    (a) A es un anillo conmutativo y unitario.
    (b) $\mathcal{M}$ es un ideal maximal.

(c) Por el teorema 4.10, $K = A \mid \mathcal{I}$ es un cuerpo. ¿Cuál es su característica? Demuestre que K tiene 9 elementos. Descríbalo apropiadamente y haga una tabla con sus operaciones.

CAPITULO 5

Grupos

En este capítulo desarrollaremos los rudimentos de una de las teorías más elegantes de la matemática, la teoría de grupos. La teoría de grupos es de la mayor importancia en el álgebra moderna y tiene gran cantidad de aplicaciones dentro y fuera de la matemática. A diferencia de los capítulos anteriores, en los que introdujimos primero los ejemplos concretos y luego los conceptos abstractos de anillo, ideal etc., procederemos a dar la definición abstracta, ejemplos y algunas propiedades generales elementales para luego en una extensa segunda sección desarrollar en detalle tres ejemplos que creemos constituyen el núcleo de la idea de grupo. El motivo de proceder así en este caso es principalmente para beneficiarnos de la nomenclatura estándar en el área.

1. Definiciones y Ejemplos

DEFINICIÓN 5.1. Un *grupo* es un conjunto no vacío G dotado de una operación $*$ que verifica las siguientes condiciones:

(1) La operación $*$ es asociativa, o sea, para todo x,y,$z \in G$,

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

(2) Existe un elemento $e \in G$ tal que para todo $x \in G$,

$$e * x = x * e = x.$$

e se llama el *elemento neutro* de G.

(3) Para todo $x \in G$, existe $y \in G$ tal que

$$x * y = y * x = e.$$

Si además para todo x, $y \in G$,

$$x * y = y * x,$$

decimos que G es un grupo *conmutativo* o *abeliano*.

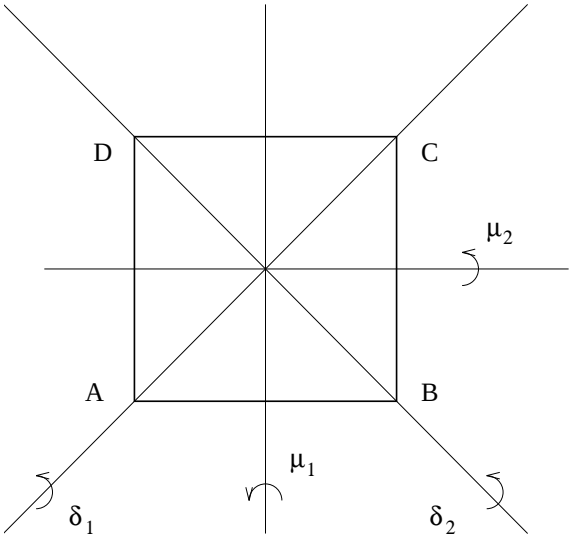
En rigor, un grupo está formado por un conjunto y una operación por lo que deberiamos hablar del par $\langle G, * \rangle$. Sin embargo, cuando la operación que estamos considerando se subentiende, hablamos simplemente del grupo G. Debemos observar que sobre un mismo conjunto se puede definir distintas operaciones que lo convierten, por ende, en grupos distintos.

Los tres primeros ejemplos dados a continuación serán desarrollados con detalle en la próxima sección.

EJEMPLOS 5.1. (1) El conjunto S_n de todas las permutaciones del conjunto $\{1, 2, \ldots, n\}$, con la composición de funciones como operación es un grupo. En efecto, la composición de funciones es asociativa, la función identidad es una biyección que actua como elemento neutro y por último toda biyección tiene una inversa. En general, este no es un grupo conmutativo. De hecho es conmutativo sólo si $n \leq 2$.

(2) El conjunto de todas las isometrías del plano euclidiano, con la composición como operación es un grupo.

(3) El conjunto de los movimientos rígidos del cuadrado, formado por todas aquellas transformaciones del plano que llevan los vértices y los lados del cuadrado ABCD de la figura sobre los vértices y lados, respectivamente, del cuadrado sin romper o deformar la figura.



Simetrías del Cuadrado

Este grupo se llama el *grupo diédrico* de grado 4 y lo denotaremos por D_4. Si $\sigma, \tau \in D_4$ la operación $\sigma * \tau$, o simplemente $\sigma\tau$, es el movimiento rígido que se obtiene al efectuar primero τ y en seguida σ.

Entonces, D_4 es un grupo con la operación dada por la tabla siguiente.

$*$	Id	ρ	ρ^2	ρ^3	μ_1	μ_2	δ_1	δ_2
Id	Id	ρ	ρ^2	ρ^3	μ_1	μ_2	δ_1	δ_2
ρ	ρ	ρ^2	ρ^3	Id	δ_1	δ_2	μ_2	μ_1
ρ^2	ρ^2	ρ^3	Id	ρ	μ_2	μ_1	δ_2	δ_1
ρ^3	ρ^3	Id	ρ	ρ^2	δ_2	δ_1	μ_1	μ_2
μ_1	μ_1	δ_2	μ_2	δ_1	Id	ρ^2	ρ	ρ^3
μ_2	μ_2	δ_1	μ_1	δ_2	ρ^2	Id	ρ^3	ρ
δ_1	δ_1	μ_1	δ_2	μ_2	ρ^3	ρ	Id	ρ^2
δ_2	δ_2	μ_2	δ_1	μ_1	ρ	ρ^3	ρ^2	Id

(4) Más generalmente, podemos definir D_n, el grupo diédrico de grado n, como el grupo de todas las simetrías del polígono regular de n lados. Tal grupo tiene 2n elementos, n rotaciones en 0°, $\frac{360}{n}^\circ, \ldots, (n-1)\frac{360}{n}^\circ$ y n reflexiones.

(5) $\langle \mathbb{Z}, + \rangle$, o simplemente $\mathbb{Z}$, es un grupo. También lo son $\langle \mathbb{Q}, + \rangle$, $\langle \mathbb{R}, + \rangle$ y $\langle \mathbb{C}, + \rangle$. Más generalmente,

(6) Si A es un anillo y nos olvidamos del producto, entonces $\langle A, + \rangle$ es un grupo abeliano. $\langle \mathbb{Z}, \cdot \rangle$, no es un grupo pues a pesar de cumplir con las dos primeras condiciones, no cumple la tercera, hay enteros, por ejemplo el 2, que no tienen inverso.

(7) Ya vimos que cualquier anillo es, en particular, un grupo abeliano si consideramos sólo la suma. El ejemplo anterior muestra que esto no es así si consideramos sólo la multiplicación. El problema en muchos casos es que algunos elementos del anillo no tienen inverso multiplicativo. Sin embargo hay un grupo asociado naturalmente a la parte multiplicativa de todo anillo unitario. Para esto sea A un anillo unitario y definamos

$$A^* = \{a \in A : a \text{ es una unidad de } A\}.$$

O sea, A^* es el subconjunto de A formado por todos los elementos que tienen un inverso multiplicativo. Entonces $\langle A^*, \cdot \rangle$ es un grupo.

Lo primero que debemos recordar es que el producto de dos unidades de un anillo es también una unidad, así la operación está bien definida.

La demostración de que es un grupo sigue fácilmente. Basta notar que el producto heredado del anillo es asociativo, **1** es una unidad y actua como neutro y finalmente, como nos hemos restringido precisamente al conjunto de los elementos invertibles, y el producto de dos elementos invertibles, A^* es un grupo.

Veremos a continuación tres ejemplos de este tipo de grupo.

(8) Si K es un cuerpo, entonces $K^* = K - \{0\}$, luego $\langle K^*, \cdot \rangle$ es un grupo abeliano.

(9) El anillo de las matrices reales de orden dos.

$$M_2(\mathbb{R})^* = \{ \text{ matrices invertibles de orden } 2\}.$$

Este grupo es muy importante y recibe el nombre de *grupo lineal de orden 2* y se le denota $GL_2(\mathbb{R})$.

Podemos generalizar este ejemplo para obtener $GL_n(\mathbb{R})$, el grupo de las matrices invertibles de orden n.

Todos estos son grupos no abelianos.

(10) Consideremos ahora $\mathbb{Z}^* = \{1, -1\}$ dotado de la multiplicación. Este es un grupo de dos elementos cuyo neutro es el 1 y en el que cada elemento es su propio inverso.

(11) Las clases residuales $\mathbb{Z}_n$ con la adición son también un ejemplo muy interesante y de él se pueden sacar muchas conclusiones en teoría de números. Asociado con ellas está el grupo de sus unidades con el producto como operación

$$\mathbb{Z}_n^* = \{\underline{m} \in \mathbb{Z}_n : (m, n) = 1\}.$$

TEOREMA 5.1. *Sea G un grupo. Entonces*

(1) *El elemento neutro, e, es único.*

(2) *El inverso a^{-1} de a, es único.*

(3) *Para todo a,*

$$(a^{-1})^{-1} = a.$$

(4) *Para todo a, b,*

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

(5) *La ley de cancelación es válida, es decir, Si $a * b = a * c$, entonces $b = c$ y si $b * a = c * a$, entonces $b = c$.*

(6) *Las ecuaciones*

$$x * a = b \quad y \quad a * x = b,$$

tienen solución única.

DEMOSTRACIÓN. (1) Supongamos que hay dos neutros e y e'. Entonces

$$e = e * e' = e'.$$

(2) Si b y c son dos inversos de a, entonces

$$a * b = e = a * c,$$

luego

$$b = b * e = b * (a * c) = (b * a) * c = e * c = c.$$

(3) Basta notar que por definición

$$a^{-1} * (a^{-1})^{-1} = (a^{-1})^{-1} * a^{-1} = e,$$

o sea, $(a^{-1})^{-1}$ es un inverso de a^{-1}. Pero obviamente a también es un inverso de a^{-1}, luego ambos inversos son iguales.

(4) Como

$$(a * b) * (b^{-1} * a^{-1}) = (b^{-1} * a^{-1}) * (a * b) = e,$$

por la unicidad del inverso,

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

(5) Supongamos que

$$a * b = a * c$$

luego operando por a^{-1} por la izquierda, obtenemos

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

La otra cancelación se procede igual pero operando por la derecha.

(6) Para la primera ecuación,perando por a^{-1} por la izquierda obtenemos

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

Para la otra ecuación se procede igual operando por la derecha. En ambos casos el resultado es obviamente único

□

En general se puede dar distintas estructuras de grupo a un mismo conjunto, basta para ello dotarlo de distintas operaciones. Por ejemplo, si definimos sobre $\mathbb{Q}$ la operación

$$a * b = \frac{ab}{2},$$

$\langle \mathbb{Q}^*, * \rangle$ es un grupo cuyo neutro es 2 y tal que

$$a^{-1} = \frac{2}{a},$$

por lo tanto $\langle \mathbb{Q}^*, \cdot \rangle$ y $\langle \mathbb{Q}^*, * \rangle$ son dos grupos distintos definidos sobre el mismo conjunto.

Para conjuntos muy pequeños, se puede estudiar todas las posibles operaciones escribiendo todas las posibles tablas, tal como hicimos anteriormente las tablas de $\mathbb{Z}_2$, $\mathbb{Z}_3$ etc.

Por ejemplo veamos el caso de un conjunto de dos elementos. Como uno (y sólo uno) de ellos debe ser el neutro, lo designaremos con la letra e y llamaremos a al otro elemento. La tabla empieza así :

$*$	e	a
e	e	a
a	a	?

ya que e es el elemento neutro. Ahora es cosa de observar que puesto que a debe tener un inverso, debe haber algún elemento que operado con a sea el neutro, luego hay una sóla forma de llenar el casillero marcado con ? , la única posibilidad es que a sea su propio inverso. Por lo tanto la única tabla sobre un conjunto de dos elementos que define una operación de grupo es

$*$	e	a
e	e	a
a	a	e

Debemos verificar que efectivamente la operación definida por la tabla anterior es asociativa. Esto es muy fácil de ver.

Obsérvese que hemos demostrado que, esencialmente, hay un único grupo de dos elementos.

Veamos ahora el caso de un conjunto con tres elementos e, a y b y veamos su tabla.

$*$	e	a	b
e	e	a	b
a	a	?	
b	b		

Debemos observar ahora que por el teorema 5.1 (6), en cada línea (o columna) de la tabla debe aparecer cada elemento del conjunto. Por otra parte, por la ley de cancelación, en cada línea (o columna) cada elemento puede aparecer sólo una vez.

Por lo tanto en ? no puedo poner a, porque aparecería dos veces en la línea. Tampoco puedo poner e, porque en ese caso, b tendríque aparecer dos veces en la tercera columna, luego la única posibilidad es poner b en ?.

Por supuesto, esto obliga a que los otros tres lugares sean llenados como sigue

$*$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

El lector puede como ejercicio intentar llenar las tablas para conjuntos con cuatro, cinco y seis elementos. Por ejemplo, hay sólo dos grupos con cuatro elementos, estos estan dados por las tablas siguientes.

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

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

Esencialmente, hay sólo dos grupos de cuatro elementos, uno de cinco elementos y dos de seis elementos.

Notación:

Si no hay confusión posible usaremos la notación

$$a * b = ab.$$

En este caso hablaremos del *producto* de a y b.

En caso de que el grupo tenga un símbolo de operación conocido, por ejemplo $+$ o $\circ$, usaremos ese símbolo.

Algunos autores usan la convención de denotar la operación de los grupos abelianos con el símbolo $+$ de la adición, o sea,

$$\begin{aligned} a * b &= a + b \\ a^{-1} &= -a. \end{aligned}$$

EJERCICIOS 5.1. (1) Demuestre que hay sólo dos grupos de cuatro elementos, uno de cinco elementos y dos de seis elementos.

2. Permutaciones, Isometrías, Simetrías.

En esta sección estudiaremos ciertos grupos de biyecciones de un conjunto A en sí mismo, dotados de la operación binaria natural, la composición de funciones. Como sabemos, sin importar cuál es el conjunto A, la composición de dos biyecciones es también una biyección. Habitualmente nos referiremos a la composición de dos biyecciones σ y τ como el *producto* de σ y τ.

Como veremos, estos conjuntos dotados de esta operación tienen una serie de propiedades que pueden ser analizadas desde el punto de vista algebraico. El propósito de este capítulo es estudiar en forma intuitiva algunos de estos ejemplos, que suponemos más o menos conocidos por el lector, y hacer notar su estructura de grupo. De hecho, los trabajos de Lagrange, Abel y Galois a fines del siglo XVIII y comienzos del XIX sobre grupos de permutaciones, son el origen de toda la teoría abstracta de grupos desarrollada más tarde por Cayley.

Nos referiremos en primer lugar a algunas propiedades de todos estos ejemplos. En primer lugar, si f, g y h son funciones de un conjunto cualquiera en si mismo, entonces

$$f \circ (g \circ h) = (f \circ g) \circ h,$$

es decir, la composición de funciones es asociativa, sin embargo, en general

$$f \circ g \neq g \circ f,$$

es decir, la composición de funciones no es conmutativa.

También sabemos que existe una biyección, la función identidad Id, que no produce ningún efecto en el conjunto A y que, por lo tanto, al componerla con cualquier otra biyección σ, el resultado sobre A es el mismo que si hiciéramos actuar sólo a σ, esto es,

$$\sigma \circ Id = Id \circ \sigma = \sigma.$$

Nos referiremos a ella como la *identidad* o la biyección *trivial*.

Por último, toda biyección tiene una inversa, es decir, dada una biyección σ, existe otra, habitualmente denotada σ^{-1} que invierte la acción de σ sobre A, es decir, si $\sigma(a) = b$, entonces $\sigma^{-1}(b) = a$, esto se resume en las siguientes ecuaciones

$$\sigma \circ \sigma^{-1} = \sigma^{-1} \circ \sigma = Id.$$

Estas tres propiedades, asociatividad de la composición, existencia de un elemento que no altera el resultado al ser operado con cualquier otro, (similar al 0 en la suma de los números enteros), y la existencia para cada elemento de otro que, por así decirlo, actua al revés, son las propiedades que definen a un grupo.

TEOREMA 5.2. *Sea G es un conjunto de biyecciones $f : A \longrightarrow A$ tal que*

(1) $Id \in G$,
(2) *G es cerrado bajo composiciones,*
(3) *G es cerrado bajo inversas.*

En tonces $\langle G, \circ \rangle$ es un grupo.

2.1. Permutaciones. En esta sección estudiaremos el conjunto de todas las biyecciones de un conjunto en sí mismo a las que llamaremos *permutaciones*. Nos limitaremos aquí al caso de un conjunto finito.

$$A = \{a_1, a_2, \ldots, a_n\},$$

de hecho, sin pérdida de generalidad, consideremos el conjunto de todas las permutaciones del conjunto

$$\{1, 2, \ldots, n\},$$

es decir,

$$\mathcal{S}_n = \{f : \{1, 2, \ldots, n\} \longrightarrow \{1, 2, \ldots, n\} : f \text{ es biyectiva}\}.$$

Es claro que $\mathcal{S}_n$, que contiene a todas las biyecciones posibles, es cerrado bajo composiciones, inversos y contiene a la identidad, luego $\mathcal{S}_n$ es un grupo al que llamaremos el grupo simétrico sobre n objetos.

Existe una notación muy práctica para representar un elemento σ de $\mathcal{S}_n$. Simplemente escribimos dos renglones con los números $\{1, 2, \ldots, n\}$, de tal manera que debajo de k aparece su imagen $\sigma(k)$:

$$\begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}.$$

Así por ejemplo, la permutación

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix},$$

corresponde a la función

$$\begin{aligned} \tau(1) &= 2 \\ \tau(2) &= 4 \\ \tau(3) &= 3 \\ \tau(4) &= 1. \end{aligned}$$

Es claro también que el orden en que se escriban los elementos de la permutación no es importante mientras la imagen de cada número aparezca debajo del mismo, así

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 4 & 3 & 1 \\ 4 & 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 4 & 3 & 2 & 1 \\ 1 & 3 & 4 & 2 \end{pmatrix}.$$

Usando esta notación, la función identidad será:

$$Id = \begin{pmatrix} 1 & 2 & \cdots & n \\ 1 & 2 & \cdots & n \end{pmatrix},$$

mientras que la inversa de

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}.$$

será

$$\sigma^{-1} = \begin{pmatrix} \sigma(1) & \sigma(2) & \cdots & \sigma(n) \\ 1 & 2 & \cdots & n \end{pmatrix}.$$

El lector probablemente ha visto el siguiente resultado en algún curso de algebra elemental.

TEOREMA 5.3. *$\mathcal{S}_n$ tiene $n!$ elementos.*

2.1.1. *Ciclos y Transposiciones.* Entre las permutaciones, hay algunas que merecen un estudio especial, se trata de los *ciclos* y el caso particular de éstos, las *transposiciones*.

DEFINICIÓN 5.2. Una permutación σ de $\mathcal{S}_n$ cuyos valores sobre $\{a_1, a_2, \ldots, a_k\} \subseteq \{1, 2, \ldots, n\}$ están dados por

$$a_1 \overset{\sigma}{\longmapsto} a_2 \overset{\sigma}{\longmapsto} a_3 \cdots \overset{\sigma}{\longmapsto} a_k \overset{\sigma}{\longmapsto} a_1$$

y tal que para todo otro $x \in \{1, 2, \ldots, n\}$, $\sigma(x) = x$, se denomina *ciclo de largo k*.

Un ciclo de largo dos es una *transposición*.

El ciclo anterior lo denotaremos

$$(a_1\ a_2,\ \ldots\ a_k).$$

Por ejemplo, la permutacion τ de S_4 que escribimos arriba, es un ciclo de largo tres ya que

$$1 \overset{\tau}{\longmapsto} 2 \overset{\tau}{\longmapsto} 4 \overset{\tau}{\longmapsto} 1$$

y $\tau(3) = 3$. De acuerdo con esta nueva notación,

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix} = (1\ 2\ 4).$$

Debemos observar que esta notación simplificada para un ciclo es ambigua. En efecto, el ciclo (1 2 4) representa también a la permutación

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 3 & 1 & 5 \end{pmatrix},$$

de S_5 y también a una de S_6 o a una permutación de cualquier número de elementos. Sólo sabiendo de antemano el contexto en el que se está trabajando se podrá determinar si el ciclo anterior representa a una permutación de $\mathcal{S}_4$ o de $\mathcal{S}_5$ o de $\mathcal{S}_n$, para algún n.

Al igual que en la notación anterior, más completa, no nos interesa cuál es el primer elemento del ciclo sino sólo el orden en que aparecen,

$$(1\ 2\ 4) = (2\ 4\ 1) = (4\ 1\ 2).$$

Resulta claro que no toda permutación es un ciclo, por ejemplo

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 5 & 1 & 3 \end{pmatrix},$$

no es un ciclo.

DEFINICIÓN 5.3. Dos ciclos se dicen *disjuntos*, si no comparten ningún elemento.

Por ejemplo

$$(1\ 3\ 4\ 6)\ \text{ y }\ (2\ 7\ 8),$$

son ciclos disjuntos.

El próximo teorema es más o menos obvio.

TEOREMA 5.4. *La composición de ciclos disjuntos es conmutativa.*

DEMOSTRACIÓN. Sean $(a_1\ \ldots\ a_{k_1})$ y $(b_1\ \ldots\ b_{k_2})$ dos ciclos disjuntos de $\mathcal{S}_n$. Para verificar que conmutan, basta ver cuál es la acción sobre $1, 2, \ldots, n$ de las permutaciones $(a_1\ \ldots\ a_{k_1})(b_1\ \ldots\ b_{k_2})$ y $(b_1\ \ldots\ b_{k_2})(a_1\ \ldots\ a_{k_1})$ es fácil ver que

$$(a_1\ \ldots\ a_{k_1})(b_1\ \ldots\ b_{k_2})(k) = \begin{cases} b_{i+1}, & \text{si } k = b_i \\ b_1, & \text{si } k = b_{k_1} \\ a_{i+1}, & \text{si } k = a_i \\ a_1, & \text{si } k = a_{k2} \\ k, & \text{en cualquier otro caso,} \end{cases}$$

y que $(b_1\ \ldots, b_{k_2})(a_1, \ldots\ a_{k_1})$ toma los mismos valores, luego ambas permutaciones son iguales. □

Los ciclos juegan dentro de la teoría de permutaciones un papel similar al de los números primos en la teoría de números, son los ladrillos con los que se construyen todas las permutaciones. Esto lo precisaremos en el próximo teorema.

TEOREMA 5.5. *Toda permutación no trivial se puede descomponer como producto de ciclos disjuntos. Tal descomposición es única salvo por el orden de los ciclos.*

DEMOSTRACIÓN. Sea σ una permutación no trivial de $\mathcal{S}_n$. Procederemos por inducción sobre el número de elementos de $\{1, 2, \ldots, n\}$ que son "movidos" por σ, es decir, tales que $\sigma(x) \neq x$. Sean $\{a_1, a_2, \ldots, a_k\}$ los elementos movidos por σ.

Observemos que el número mínimo de elementos que una permutación no trivial mueve es dos, y esto ocurre cuando se trata de una transposición. Luego si $k = 2$, o sea, σ mueve sólo dos elementos, es una transposición y, por lo tanto, un ciclo. Esto da cuenta del primer paso de la inducción.

Supongamos ahora nuestra hipótesis de inducción, a saber, toda permutación que mueve menos de k elementos, $k \geq 2$, se descompone como producto de ciclos disjuntos.

Sea a_1 uno cualquiera de los elementos movidos por σ. Si observamos la siguiente sucesión

$$a_1 \longmapsto \sigma(a_1) \longmapsto \sigma(\sigma(a_1)) \longmapsto \cdots \longmapsto \sigma^m(a_1)$$

entonces, como el conjunto es finito y σ es una biyección, para algún $m \leq k$, $\sigma^m(a_1) = a_1$. Notemos que $m \geq 2$.

Tenemos entonces dos posibilidades, si $m = k$, entonces σ es un ciclo y el teorema se verifica. Si $m < k$ entonces consideramos la permutación definida por

$$\hat{\sigma} = \begin{cases} x, & \text{si } x \in \{a_1, \sigma(a_1), \ldots, \sigma^{m-1}(a_1)\}, \\ \sigma(x) & \text{en otro caso.} \end{cases}$$

Como vemos, $\hat{\sigma}$ es una permutación de $\mathcal{S}_n$ que difiere de σ sólo en los valores que toma sobre $\{a_1, \sigma(a_1), \ldots, \sigma^{m-1}(a_1)\}$. También es fácil comprobar que

$$\sigma = (a_1\ \sigma(a_1)\ \ldots\ \sigma^{m-1}(a_1)\}\hat{\sigma}.$$

Pero ahora podemos aplicar nuestra hipótesis de inducción ya que $\hat{\sigma}$ obviamente mueve menos de k elementos, luego es el producto de ciclos disjuntos. Como estos necesariamente son disjuntos de $(a_1\ \sigma(a_1)\ \ldots\ \sigma^{m-1}(a_1))$, el teorema queda demostrado.

La unicidad de la descomposición es consecuencia directa del teorema 5.4. □

La demostración del teorema anterior nos da una suerte de algoritmo para calcular la descomposición en ciclos de una permutación σ. Tomamos un elemento a cualquiera. Si $\sigma(a) = a$, no nos interesa y tomamos otro. Si $\sigma(a) \neq a$, procedemos con el teorema definiendo el ciclo

$$(a\ \sigma(a)\ \ldots\ \sigma^{m-1}(a)),$$

De los elementos que aún no han sido considerados, escogemos otro y procedemos como con a. Eventualmente ya no quedarán elementos por considerar, ya sea porque ya aparecieron en un ciclo o porque no son movidos por σ.

Ejemplos 5.2.

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 9 & 5 & 7 & 3 & 6 & 8 & 4 & 1 \end{pmatrix} = (1\ 2\ 9)(3\ 5)(7\ 8\ 4).$$

Existe otro interesante teorema de descomposición de permutaciones como producto de transposiciones. Intuitivamente, esto significa que podemos ordenar un conjunto finito de cualquier manera intercambiando sucesivamente sólo dos de ellos cada vez. En este caso no se tiene unicidad ya que si multiplicamos cualquier permutación por

$$(1\ 2)(1\ 2) = Id,$$

obteniendo una descomposición distinta.

Tampoco esta descomposición es independiente del orden en que aparecen las transposiciones ya que, en general, éstas no son disjuntas.

Teorema 5.6. *Toda permutación se puede descomponer como producto de transposiciones.*

Demostración. En virtud del teorema anterior basta demostrar que todo ciclo se puede descomponer como producto de transposiciones. Es fácil comprobar que la siguiente descomposición sirve para nuestro propósito.

$$(a_1\ a_2\ \ldots\ a_k) = (a_1\ a_k)\cdots(a_1\ a_3)(a_1\ a_2).$$

□

Así por ejemplo,

$$(2\ 5\ 6\ 8) = (2\ 8)(2\ 6)(2\ 5).$$

Usando la descomposición como producto de transposiciones es muy sencillo encontrar la permutación inversa. Baste observar que la inversa de una transposición es ella misma, en efecto, calcúlese el producto de (k, l) por si misma y se obtendrá la identidad. Ahora bien, si

$$\sigma = (a_1\ b_1)(a_2\ b_2)\cdots(a_k\ b_k),$$

entonces

$$\sigma^{-1} = (a_k\ b_k)(a_{k-1}\ b_{k-1})\cdots(a_1\ b_1),$$

como se puede verificar fácilmente, al calcular el producto de ambas permutaciones, obtenemos la identidad, luego como el inverso de todo elemento es único, ésta debe ser la inversa de σ.

La descomposición de una permutación como producto de transposiciones, si bien no es única, tiene una interesante propiedad, que no es en absoluto fácil de detectar (¡ni de demostrar!), el número de transposiciones de una descomposición de una permutación es siempre par o siempre impar, o dicho de otra manera, ninguna permutación se descompone como producto de, por ejemplo, tres transposiciones y también como producto de ocho transposiciones, pero si podría tenerse una descomposición de nueve y otra de treinta y siete transposiciones. Demostraremos primero este hecho para la identidad.

Lema 5.7. *La identidad no se puede descomponer como producto de un número impar de transposiciones.*

Demostración. Supongamos que

$$Id = \tau_m\tau_{m-1}\cdots\tau_1,$$

donde las τ_i son transposiciones.

Sea k un elemento que aparece en alguna transposición. Sea $\tau_i = (k\ l)$ la transposición de índice más pequeño en la que k aparece. Es claro que $i \neq m$ porque, si no, $Id(k) = l$, una contradicción.

Entonces, hay cuatro posibilidades para τ_{i+1}, a saber $(x\ y)$, $(x\ k)$, $(x\ l$ y $(k\ l)$, donde x, y, l y k son todos distintos. Obervamos que en las tres primeras posibilidades,

$$\begin{aligned}(x\ y)(k\ l) &= (k\ l)(x\ y) &(7)\\ (x\ k)(k\ l) &= (k\ l)(x\ l) &(8)\\ (x\ l)(k\ l) &= (k\ x)(x\ l), &(9)\end{aligned}$$

luego si ocurre cualquiera de estos casos, tenemos una descomposición de Id como producto de m transposiciones en las que k ocurre por primera vez en una transposición más a la izquierda. Como esto no puede repetirse más que hasta τ_{m-1}, eventualmente debe producirse el cuarto caso. Observemos entonces que

$$\tau_{i+1}\tau_i = Id,$$

y por lo tanto podemos eliminarlas de la descomposición obteniendo una con $m-2$ transposiciones. Obviamente el proceso anterior se puede repetir con cualquier k, luego si se repite el proceso empezando con un número impar de transposiciones, eliminando dos a la vez, nos quedaremos con una sola, lo cual es imposible. □

Teorema 5.8. *Ninguna permutación se puede escribir como producto de un número impar y también como producto de un número par de transposiciones.*

Demostración. Supongamos por el contrario que

$$\alpha = \tau_m \cdots \tau_1 = \sigma_n \cdots \sigma_1,$$

donde las τ_i y las σ_j son transposiciones, m es par y n es impar. Entonces

$$\begin{aligned}Id = \alpha\alpha^{-1} &= \tau_m \cdots \tau_1(\sigma_n \cdots \sigma_1)^{-1}\\ &= \tau_m \cdots \tau_1\sigma_1^{-1} \cdots \sigma_n^{-1},\end{aligned}$$

es el producto de un número impar de transposiciones contradiciendo el lema anterior. □

Definición 5.4. Diremos que una permutación es par si se puede descomponer como producto de un número par de transposiciones. En caso contrario diremos que la permutación es impar.

El conjunto de las permutaciones pares de $\mathcal{S}_n$ se denotará $\mathcal{A}_n$.

El conjunto $\mathcal{A}_n$ definido arriba es de suma importancia y lo estudiaremos con detención. Observemos que el producto de dos permutaciones pares es par, la inversa de una permutación par es par y que la identidad es tambien par ya que, por ejemplo, $Id = (1\ 2)(1\ 2)$. Por el teorema 5.2 $\mathcal{A}_n$ es un grupo al que llamaremos el *grupo alternante de n objetos*.

Por otra parte, el producto de permutaciones impares es par, es decir, el conjunto de las permutaciones impares no es cerrado bajo productos y por lo tanto no es un grupo.

Un resultado que no debe sorprender demasiado es que la mitad de las permutaciones son pares y la mitad son impares.

TEOREMA 5.9. *Si $n > 1$, la cardinalidad de $\mathcal{A}_n$ es $\frac{n!}{2}$.*

DEMOSTRACIÓN. Sea B el conjunto de todas las permutaciones impares y consideremos la siguiente función:

$$\begin{array}{rcl} f : \mathcal{A}_n & \longrightarrow & B \\ \sigma & \longmapsto & \sigma(1\ 2) \end{array}$$

La función está bien definida ya que si σ es par, el producto de σ por una transposición es impar.

La función es inyectiva, ya que si

$$\begin{array}{rcl} \sigma(1\ 2) & = & \tau(1\ 2), \\ \sigma(1\ 2)(1\ 2) & = & \tau(1\ 2)(1\ 2), \\ \sigma Id & = & \tau Id, \\ \sigma & = & \tau. \end{array}$$

La función es sobreyectiva, puesto que si τ es una permutación impar, $\tau(1\ 2)$ es par, y por lo tanto

$$f(\tau(1\ 2)) = \tau(1\ 2)(1\ 2) = \tau.$$

Esta función demuestra que hay tantas permutaciones pares como impares, y como toda permutación es par o impar, hay la mitad de cada una. □

EJERCICIOS 5.2.

(1) Demuestre que no hay una permutación σ tal que $\sigma^{-1}(1\ 2)\sigma = (1\ 2\ 3)$.
(2) Si σ y τ son dos transposiciones entonces $\sigma\tau$ es un producto de ciclos de largo 3, no necesariamente disjuntos.

    Si $n \geq 3$, entonces todo elemento de $\mathcal{A}_n$ es el producto de ciclos de largo 3.
(3) El siguiente ejemplo es una demostración alternativa, más elemental pero también más engorrosa, de que toda permutación es par o impar.

    Dada una permutación $\sigma \in \mathcal{S}_n$ y n números distintos $k_1, \ldots, k_n$, defina

$$\sigma^* \prod_{1 \leq i < j \leq n} k_j - k_i = \prod_{1 \leq i < j \leq n} \sigma(k_j) - \sigma(k_i)$$
$$= (\sigma(k_2) - \sigma(k_1))(\sigma(k_3) - \sigma(k_1))(\sigma(k_3) - \sigma(k_2)) \cdots (\sigma(k_n) - \sigma(k_{n-1})).$$

Entonces si

$$\Delta = \prod_{1\leq i<j\leq n} j-i = (2-1)(3-1)(3-2)\cdots(n-(n-1)),$$

$$\sigma^*\Delta = \prod_{1\leq i<j\leq n} \sigma(j)-\sigma(i) = (\sigma(2)-\sigma(1))(\sigma(3)-\sigma(1))(\sigma(3)-\sigma(2))\cdots(\sigma(n)-\sigma(n-1)).$$

(a) Demuestre que si σ, $\tau \in \mathcal{S}_n$, entonces

$$\sigma^*\tau^*\Delta = (\sigma\tau)^*\Delta.$$

(b) Demuestre que si $\tau \in \mathcal{S}_n$ una transposición, entonces $\tau^*\Delta = -\Delta$.

(c) Use el teorema de descomposición en transposiciones para demostrar que toda permutación se descompone o bien como producto de un número par de transposiciones, o bien como producto de un número impar de transposiciones.

2.2. Isometrías. En esta sección estudiaremos otro conjunto interesante de biyecciones, esta vez se trata de aplicaciones del plano euclidiano en sí mismo que preservan distancias. Tales funciones se llaman *isometrías*.

DEFINICIÓN 5.5. Una *isometría* del plano $\mathbb{R}^2$ en sí mismo es una función

$$\sigma : \mathbb{R}^2 \longrightarrow \mathbb{R}^2,$$

tal que para todo par de puntos P y Q del plano,

$$d(\sigma(P), \sigma(Q)) = d(P, Q),$$

donde $d(P, Q)$ es la distancia euclidiana habitual, vale decir, si

$$P = P(x_1, y_1) \text{ y } Q = Q(x_2, y_2),$$

$$d(P, Q) = \sqrt{(x_2 - x_1)^2 + (y_2 - y_1)^2}.$$

Denotaremos $\mathcal{I}(\mathbb{R}^2)$ al conjunto de todas las isometrías del plano.

Debemos observar que la función identidad es obviamente una isometría.

Además, si σ y τ son isometrías, entonces

$$d(\sigma\tau(P), \sigma\tau(Q)) = d(\sigma(\tau(P)), \sigma(\tau(Q))) = d(\tau(P), \tau(Q)) = d(P, Q),$$

luego $\sigma\tau$ es también una isometría, en otras palabras, el conjunto de todas las isometrías del plano es cerrado bajo productos.

Como veremos más adelante, toda isometría es una biyección, luego tienen inversassi σ^{-1} es la inversa de σ,

$$d(\sigma^{-1}(P), \sigma^{-1}(Q)) = d(\sigma\sigma^{-1}(P), \sigma\sigma^{-1}(Q)) = d(P, Q),$$

o sea, σ^{-1} es una isometría, es decir $\mathcal{I}(\mathbb{R}^2)$ es cerrado bajo inversos. Luegho por el teorema 5.2 $\mathcal{I}(\mathbb{R}^2)$ es un grupo.

Ejemplos 5.3.

(1) **Traslaciones** Una traslación es una función que mueve todos los puntos del plano una cierta distancia en una dirección dada. Analíticamente,

$$(x, y) \longmapsto (x + a, y + b).$$

(2) **Rotaciones** Consiste en rotar el plano en un ángulo dado θ en torno a un punto fijo O. Analíticamente, si fijamos el origen de nuestro sistema de coordenadas en el punto O,

$$(x, y) \longmapsto (x\cos\theta - y\text{sen}\theta, x\text{sen}\theta + y\cos\theta).$$

Un poco de trigonometría elemental nos ayudará a demostrar que toda rotación es una isometría.

(3) **Reflexiones** Consiste en reflejar los puntos del plano con respecto a una recta arbitraria. Es decir, el punto P es enviado en el punto P' que se encuentra sobre la perpendicular por P a la recta y a la misma distancia de ella que P.

Como veremos un poco más adelante, esencialmente, estas son las únicas isometrías del plano. En efecto, toda isometría es el producto de una traslación, una rotación y una reflexión.

No es del todo obvio que una isometría es, como hemos dicho, una biyección en $\mathbb{R}^2$. Empezaremos con un lema que se desprende inmediatamente de la definición de isometría.

Lema 5.10. *La imagen del triángulo ABC por una isometría es un triángulo congruente con ABC.*

De hecho, se puede demostrar que la imagen de cualquier figura plana es congruente con la figura original.

Teorema 5.11. *Toda isometría del plano es una biyección que queda determinada por la imagen de tres puntos no colineales.*

Demostración. Sea σ una isometría. Si

$$\sigma(P) = \sigma(Q),$$

entonces

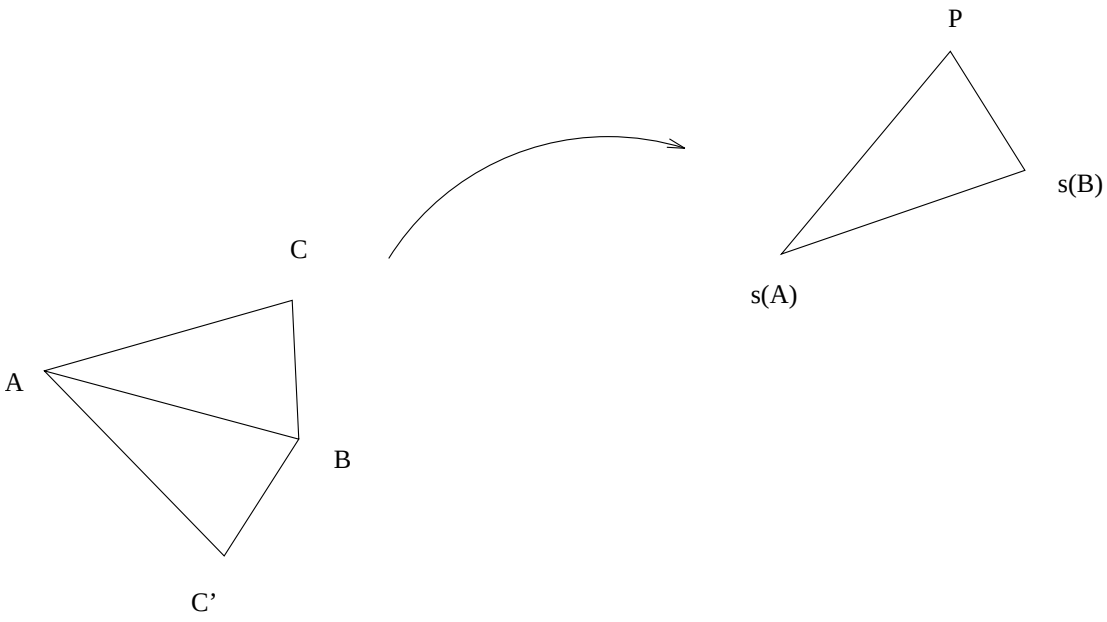
$$d(P, Q) = d(\sigma(P), \sigma(Q)) = 0,$$

luego $P = Q$ ya que están a distancia cero, por lo tanto, σ es inyectiva.

Para ver que σ es sobreyectiva, sea P un punto cualquiera del plano. Sean A y B dos puntos arbitrarios. Si $P \neq \sigma(A)$ y $P \neq \sigma(B)$. Sean $d_1 = d(P, \sigma(A))$ y $d_2 = d(P, \sigma(B))$. Observemos que P está en la intersección del círculo de centro en $\sigma(A)$ y radio d_1 con el círculo de centro en $\sigma(B)$ y radio d_2. Como σ es una isometría, la intersección del círculo de centro en A y radio d_1 con el círculo de

centro en B y radio d_2 es no vacía y consta de un punto C, si P está en la recta $\overline{\sigma(A)\sigma(B)}$, o de dos puntos C y C'.

En cualquier caso, o bien $P = \sigma(C)$ o bien $P = \sigma(C')$, luego la función es sobreyectiva.



Para demostrar que σ queda determinada por la imagen de tres puntos no colineales, sean A, B, y C estos tres puntos del plano. Por el lema 5.10 los triángulos ABC y $\sigma(A)\sigma(B)\sigma(C)$ son congruentes. Sea P un punto cualquiera del plano distinto de A, B, y C. Consideremos

$$\begin{aligned} d_1 &= d(P, A) \\ d_2 &= d(P, B) \\ d_3 &= d(P, C) \end{aligned}$$

Los círculos de centro A y radio d_1, de centro B y radio d_2 y de centro C y radio d_3 se intersectan en P y solamente en P, ya que si se intersectaran en dos puntos, sus centros A, B y C serían colineales.

La imagen de P por σ es entonces el único punto que está en la intersección de los círculos de centro $\sigma(A)$ y radio d_1, de centro $\sigma(B)$ y radio d_2 y de centro $\sigma(C)$ y radio d_3. Esto concluye nuestra demostración. □

Teorema 5.12. *Toda isometría es el producto de una traslación, una rotación y una reflexión.*

DEMOSTRACIÓN. Como hemos visto, una isometría σ queda determinada por su acción sobre tres puntos no colineales.

Sean A, B, y C tres puntos no colineales cualquiera del plano, y sea $\sigma(A)\sigma(B)\sigma(C)$ el triángulo congruente correspondiente.

Sea τ_A la traslación que lleva el punto A en el punto $\sigma(A)$. Tenemos entonces que

$$\tau_A(A) = \sigma(A),$$

y que por lo tanto los triángulos (¡congruentes!) $\sigma(A)\sigma(B)\sigma(C)$ y $\tau_A(A)\tau_A(B)\tau_A(C)$ comparten un vértice.

Sea ρ_θ la rotación de centro en $\sigma(A)$ y que lleva el lado $\overline{\tau_A(A)\tau_A(B)}$ sobre el lado $\overline{\sigma(A)\sigma(B)}$.

Ahora tenemos que

$$\begin{aligned} \sigma(A)\rho_\theta &= (\tau_A(A)) \\ \sigma(B)\rho_\theta &= (\tau_A(B)), \end{aligned}$$

es decir, los triángulos $\sigma(A)\sigma(B)\sigma(C)$ y $\rho_\theta(\tau_A(A))\rho_\theta(\tau_A(B))\rho_\theta(\tau_A(C))$ comparten dos vértices y como son congruentes, o bien

$$\rho_\theta(\tau_A(C)) = \sigma(C),$$

o bien $\rho_\theta(\tau_A(B))$ es simétrico de $\sigma(C)$ con respecto a la recta por $\sigma(A)$ y $\sigma(B)$. En el primer caso,

$$\sigma = \rho_\theta\tau_A$$

En el segundo,

$$\sigma = \mu_{\sigma(A)\sigma(B)}\rho_\theta\tau_A,$$

donde $\mu_{\sigma(A)\sigma(B)}$ es la reflexión con respecto al eje $\overline{\sigma(A)\sigma(B)}$. □

Las simetrías se diferencian en el numero de puntos que dejan fijos. Las traslaciones no fijan ningún punto. Las rotaciones fijan sólo un punto, el centro. Las reflexiones fijan todos los puntos sobre la recta de reflexión. La identidad obviamente fija todos los puntos del plano. Podemos concluir entonces que si la composición de dos o más simetrías no deja ningún punto fijo, se trata de una traslación, etc.

TEOREMA 5.13. *La composición de dos reflexiones es una rotación o una traslación.*

TEOREMA 5.14. *Toda traslación es la compuesta de dos reflexiones.*

EJERCICIOS 5.3.

(1) Demuestre que las traslaciones, rotaciones y reflexiones son isometrías.
(2) Dada una traslación τ y una rotación ρ, compute $\tau\ \rho$. ¿Cuál es su(s) punto(s) fijo(s)?
(3) Demuestre el teorema 5.13.
(4) Demuestre el teorema 5.14.

2.3. Simetrías. En esta sección estudiaremos conjuntos de funciones del plano en sí mismo que preservan una cierta figura, por ejemplo un triángulo, es decir, conjuntos de biyecciones del plano tales que la imagen de la figura dada coincida con ésta. Estas funciones se denominan *simetrías* de la figura; también se las conoce como *movimientos rígidos* ya que envián la figura sobre ella misma sin deformarla ni romperla.

Es claro que toda simetría es una isometría y que de éstas, ninguna traslación es una simetría. Por lo tanto las simetrías de una figura están constituidas por rotaciones, reflexiones y sus compuestas.

Usando el teorema 5.2, es fácil ver que las simetríi as de una figura cualquiera es un grupo.

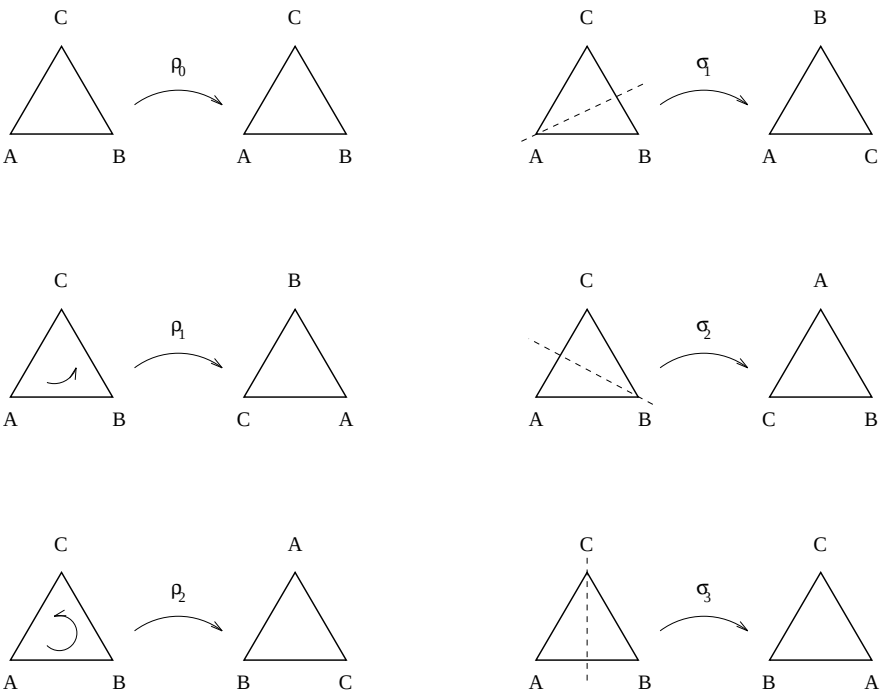
Se puede estudiar las simetrías de cualquier figura, sin embargo, mientras más regular sea ésta, más simetrías tendrá. De hecho, los ejemplos más interesantes son los polígonos regulares. El grupo de los movimientos rígidos o simetrías del polígono regular de n lados se denomina *grupo diédrico de grado n* y se le denota $\mathcal{D}_n$.

2.3.1. *Simetrías de un Triángulo Equilátero.* Existen tres rotaciones, en 0°, 120° y 240°. La primera no es sino la identidad Id, la segunda la denotamos ρ y como una rotación en 240° corresponde a efectuar dos veces la rotación en 120°, denotaremos ρ^2 a la tercera rotación. Observemos que

$$\rho\ \rho^2 = \rho^2\ \rho = Id,$$

ya que una rotación en 360° corresponde a una rotación en 0°.

Tenemos también tres reflexiones con respecto a las transversales de cada lado. En el cuadro siguiente se ilustran las seis simetríi as del triángulo equilátero. Es bastante obvio que éstas son las únicas simetrías, en efecto, es claro que las únicas reflexiones y rotaciones del plano que son simetrías del triángulo son las señaladas anteriormente. Si componemos cualquiera de ellas, obtenemos una reflexión o una rotación, luego tiene que ser una de las anteriores.



Movimientos Rígidos del Triángulo

Si componemos, por ejemplo ρ con μ_1 obtendremos

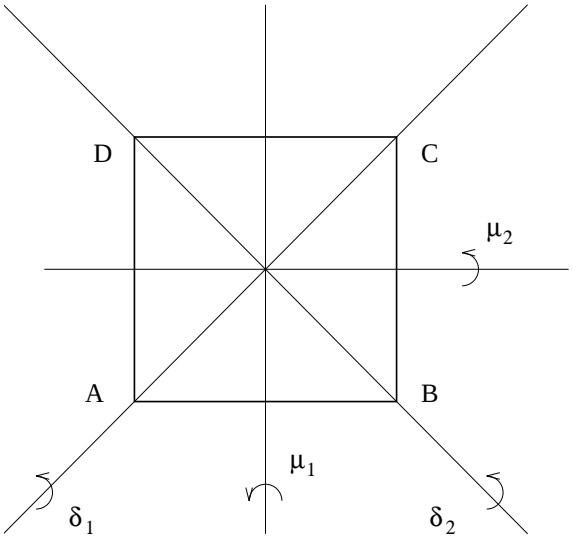
$$\rho\ \mu_1 = \mu_3 \ \text{ y } \ \mu_1\ \rho = \mu_2.$$

Podemos hacer una tabla en la que se resumen todas las posibles composiciones de las simetrías anteriores. Debe observarse que para obtener $\sigma\ \tau$ aplicamos primero τ y luego σ

$*$	Id	ρ	ρ^2	μ_1	μ_2	μ_3
Id	Id	ρ	ρ^2	μ_1	μ_2	μ_3
ρ	ρ	ρ^2	Id	μ_2	μ_3	μ_1
ρ^2	ρ^2	Id	ρ	μ_3	μ_1	μ_2
μ_1	μ_1	μ_2	μ_3	Id	ρ	ρ^2
μ_2	μ_2	μ_3	μ_1	ρ^2	Id	ρ
μ_3	μ_3	μ_1	μ_2	ρ	ρ^2	Id

El grupo $\mathcal{D}_3$ tiene seis elementos.

2.3.2. *Simetrías del Cuadrado.*

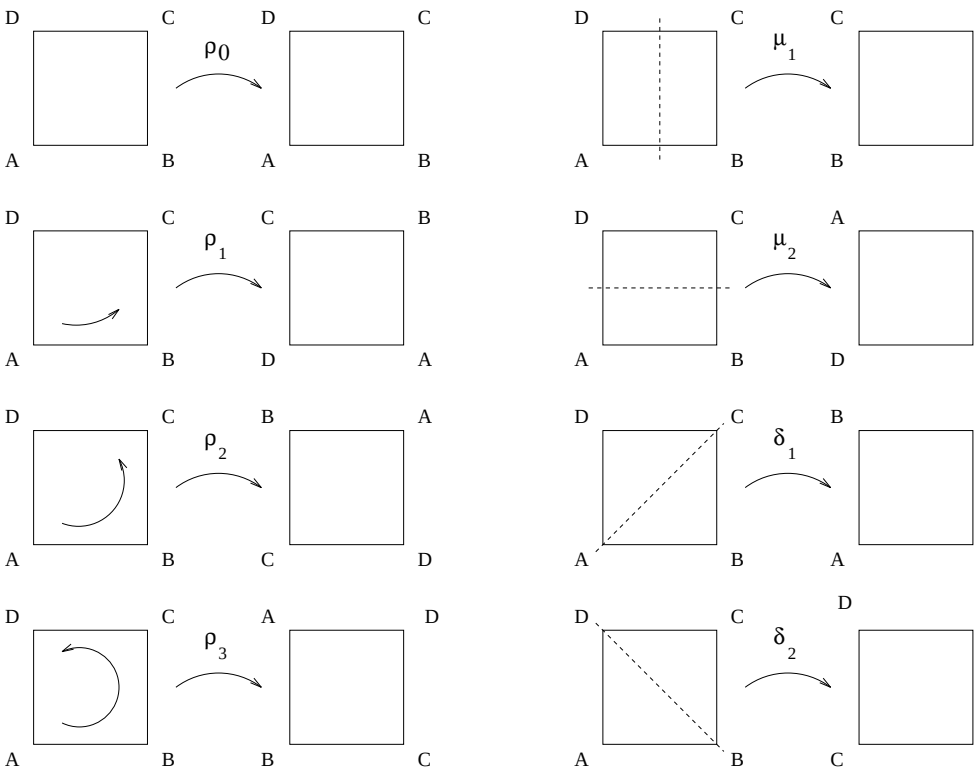


Simetrías del Cuadrado

Como se ilustra en la figura, en este caso tenemos cuatro rotaciones, en 0°, 90°, 180° y 270° las que, en forma análoga al caso del triángulo, denotaremos Id, ρ, ρ^2 y ρ^3, respectivamente. Es claro que no hay otras rotaciones.

También hay cuatro reflexiones, dos con respecto a las diagonales, denotadas δ_1 y δ_2, y dos con respecto a las simetrales de los lados opuestos, denotadas μ_1 y μ_2. Un argumento similar al dado en el caso del triángulo demuestra que las ocho simetrías señaladas son las únicas posibles, es decir $\mathcal{D}_4$ tiene ocho elementos.

El siguiente cuadro ilustra todas las simetrías del cuadrado.



Movimientos Rígidos del Cuadrado

También en este caso podemos hacer una tabla de todas las posibles composiciones.

$*$	Id	ρ	ρ^2	ρ^3	μ_1	μ_2	δ_1	δ_2
Id	Id	ρ	ρ^2	ρ^3	μ_1	μ_2	δ_1	δ_2
ρ	ρ	ρ^2	ρ^3	Id	δ_1	δ_2	μ_2	μ_1
ρ^2	ρ^2	ρ^3	Id	ρ	μ_2	μ_1	δ_2	δ_1
ρ^3	ρ^3	Id	ρ	ρ^2	δ_2	δ_1	μ_1	μ_2
μ_1	μ_1	δ_2	μ_2	δ_1	Id	ρ^2	ρ	ρ^3
μ_2	μ_2	δ_1	μ_1	δ_2	ρ^2	Id	ρ^3	ρ
δ_1	δ_1	μ_1	δ_2	μ_2	ρ^3	ρ	Id	ρ^2
δ_2	δ_2	μ_2	δ_1	μ_1	ρ	ρ^3	ρ^2	Id

2.3.3. *El grupo $\mathcal{D}_n$.* Al estudiar las simetrías de un polígono regular de n lados, observamos que existen exactamente n rotaciones en torno al centro de la figura, a saber, en $0°$, $\frac{360}{n}°, \ldots, (n-1)\frac{360}{n}°$.

Así mismo hay n reflexiones. Si n es impar, las reflexiones son con respecto a las simetrales de los lados. Obsérvese que éstas pasan por el vértice opuesto. Si n

es par las reflexiones son con respecto a las simetrales de los lados y con respecto a las rectas que pasan por vértices opuestos. Hay $\frac{n}{2}$ de cada una de ellas. Usando nuevamente los argumentos usados en en el caso del triángulo, vemos que éstas son las únicas simetrías del polígono de n lados.

TEOREMA 5.15. *El grupo diédrico de grado n tiene $2n$ elementos.*

Podemos observar que hay conjuntos más pequeños que $\mathcal{D}_n$ de simetrías que también son grupos, por ejemplo, las n rotaciones forman un grupo y $\{Id, \mu_1\}$ es también un grupo.

EJERCICIOS 5.4.

(1) Encuentre el grupo de todas las simetrías de:
   (a) Un triángulo isósceles.
   (b) Un rectángulo.
   (c) Las letras O , T , R.
(2) Encuentre todos los posibles grupos de simetrías del triángulo y del cuadrado.

3. Subgrupos y el Teorema de Lagrange

DEFINICIÓN 5.6. Un subconjunto no vacío H de un grupo G es un *subgrupo* de G si H dotado de la misma operación es un grupo.

Si H es subgrupo de G escribimos $H \leq G$.

EJEMPLOS 5.4.

(1) $\mathbb{Z}$ es un subgrupo de $\mathbb{Q}$.
(2) $2\mathbb{Z}$ es un subgrupo de $\mathbb{Z}$.
(3) Sea
$$H = \{\sigma \in S_n : \sigma(n) = n\}.$$
Entonces $H \leq S_n$.
(4) Sean
$$\begin{aligned} H_1 &= \{A \in GL_2(\mathbb{R}) : A \text{ es triangular superior}\}, \\ H_2 &= \{A \in GL_2(\mathbb{R}) : det(A) = 1\}. \end{aligned}$$
Entonces H_1 y H_2 son subgrupos de $GL_2(\mathbb{R})$.

Para verificar si un cierto subconjunto de un grupo es o no un subgrupo, conviene usar el siguiente teorema.

TEOREMA 5.16. *Sea G un grupo y sea $H \subseteq G$. Las siguientes proposiciones son equivalentes:*

(1) *H es subgrupo de G.*
(2)
   (i) *$H \neq \emptyset$.*
   (ii) *H es cerrado bajo productos, i.e., si $a, b \in H$, entonces $ab \in H$.*
   (iii) *H es cerrado bajo inversos, i.e., si $a \in H$, entonces $a^{-1} \in H$.*

(3)

(i') $H \neq \emptyset$.

(ii') *Si* $a, b \in H$, *entonces* $ab^{-1} \in H$.

DEMOSTRACIÓN. Está claro que (1) implica (2) (y también (3)), ya que la operación debe estar definida sobre H y todo elemento tiene que tener inverso.

Para verificar que (2) implica (1), sabemos por (i) que $H \neq \emptyset$.

También por (ii), la operación de G restringida a H es una operación asociativa.

Como $H \neq \emptyset$, existe $a \in H$ y por (iii), $a^{-1} \in H$, luego por (ii)

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

es decir H contiene al elemento neutro.

Por último (iii) nos dice que todo elemento tiene un inverso.

Todo lo anterior demuestra que si H verifica (i), (ii) y (iii), $H \leq G$.

Por su parte, está claro que (2) implica (3). Para ver el recíproco, notemos primero que (i) es válido.

Sea $a \in H$. Por (ii'),

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

y por lo tanto por (ii'),

$$a^{-1} = ea^{-1} \in H,$$

o sea, H es cerrado bajo inversos y (iii) es válido.

Por último, si $a, b \in H$, también $a, b^{-1} \in H$, y por (ii') nuevamente,

$$ab = a(b^{-1})^{-1} \in H,$$

o sea, H es cerrado bajo productos y (ii) es válido.

Esto completa la demostración del teorema. □

TEOREMA 5.17. *Sea G un grupo. Si $H \subseteq G$ es no vacío, finito y cerrado bajo productos, entonces $H \leq G$.*

DEMOSTRACIÓN. Por el teorema anterior, como H es no vacío y cerrado bajo productos, basta ver que también es cerrado bajo inversos.

Sea $a \in H$ y sea $n = |H|$ el número de elementos de H. Si definimos para todo j entero positivo

$$a^j = \underbrace{aa \cdots a}_{j},$$

entonces

$$a, a^2, a^3, \ldots, a^n, a^{n+1} \in H.$$

Pero tenemos sólo n elementos en H luego por lo menos dos de ellos tienen que ser iguales, digamos

$$a^i = a^k$$

para ciertos números $1 \leq i < k \leq n + 1$.

Pero entonces cancelando a i veces, obtenemos

$$e = a^{k-i} = aa^{k-i-1} = a^{k-i-1}a,$$

vale decir, si $k - i - 1 > 0$,

$$a^{-1} = a^{k-i-1} \in H.$$

Si $k - i - 1 = 0$, entonces $e = a^{k-i} = a$, por lo tanto $a^{-1} = e = a \in H$. □

TEOREMA 5.18. *Si para cada $i \in I$, H_i es un subgrupo del grupo G, entonces*

$$H = \bigcap_{i \in I} H_i \leq G.$$

DEMOSTRACIÓN. Es claro que $H \neq \emptyset$, ya que para todo $i \in I$, $e \in H_i$, luego $e \in H$.

Si x e $y \in H$, entonces para todo $i \in I$, x,$y \in H_i$, y por el teorema 5.16 (i"), $xy^{-1} \in H_i$, luego $xy^{-1} \in H$. Entonces por el mismo teorema, H es un subgrupo de G. □

Sean G un grupo y $X \subseteq G$ (X no necesariamente un subgrupo de G). Entonces

$$H = \bigcap_{i \in I} \{H \leq G : X \subset H\},$$

es un subgrupo de G que obviamente contiene a X, es más, este es el subgrupo más pequeño de G que contiene a X, ya que si $X \subset K \leq G$, entonces $K \subset H$ porque la intersección está contenida en cada uno de sus elementos.

Esto nos permite la siguiente definición.

DEFINICIÓN 5.7. Sea X un subconjunto del grupo G, definimos el *subgrupo generado por X* como el menor subgrupo de G que contiene a X.

Si $X = \{a\}$, hablamos del subgrupo cíclico generado por a, estudiaremos estos grupos con más detalle en la próxima sección.

Notación:

$$a^n = \begin{cases} \underbrace{aa \cdots a}_{n} & \text{si } n > 0 \\ e & \text{si } n = 0 \\ \underbrace{a^{-1}a^{-1} \cdots a^{-1}}_{n} & \text{si } n < 0 \end{cases}$$

TEOREMA 5.19. *Si G es un grupo y $X \subset G$, el subgrupo generado por X es*

$$H = \{x_1^{k_1} x_2^{k_2} \cdots x_n^{k_n} : n \in \mathbb{N}, k_i \in \mathbb{Z}, \text{ y } x_i \in X, \text{ para } 1 \leq i \leq n\}.$$

DEMOSTRACIÓN. Es claro que H es un subconjunto no vacío que contiene a X. También es claro que todo subgrupo que contiene a X, debe contener a H, ya que los subgrupos son cerrados bajo productos e inversos. Por lo tanto nos basta demostrar que H es un grupo.

Ya dijimos que H es no vacío. De la definición se obtiene en forma inmediata que H es cerrado bajo productos. Para ver que también es cerrado bajo inversos, si $h \in H$, digamos $h = x_1^{k_1} x_2^{k_2} \cdots x_n^{k_n}$, entonces

$$h^{-1} = x_n^{-k_n} x_{n-1}^{-k_{n-1}} \cdots x_1^{-k_1},$$

que también está en H. □

No existe un resultado análogo al teorema 5.18 para la unión de una familia de subgrupos, en general, la unión de dos subgrupos no es un subgrupo como lo demuestra el ejemplo siguiente.

Ejemplo Consideremos el grupo S_3 de todas las permutaciones de tres elementos. Si

$$H_1 = \{Id, \sigma_1\} \text{ y } H_2 = \{Id, \sigma_2\},$$

vemos que su unión no es cerrada bajo productos ya que

$$\sigma_1 \sigma_2 = \rho^2,$$

luego la unión no es un subgrupo de S_3.

Sin embargo, si para cada $i \in I$, H_i es un subgrupo del grupo G, entonces existe el menor subgrupo que los contiene a todos, a saber, el subgrupo generado por

$$X = \bigcup_{i \in I} H_i.$$

Definición 5.8. Sea G un grupo y $H \leq G$. Definimos la siguiente relación sobre G:

$$x \sim y \text{ si y sólo si } xy^{-1} \in H.$$

Decimos que x e y son *congruentes módulo* H.

Observemos que si usamos notación aditiva, lo anterior se escribe

$$x \sim y \text{ si y sólo si } x - y \in H,$$

así , si el grupo es $\mathbb{Z}$ y el subgrupo H es $n\mathbb{Z}$, lo que obtenemos es el ya conocido concepto de congruencia.

Lema 5.20. *La relación definida arriba es una relación de equivalencia.*

Demostración. Si $x \in G$ entonces $xx^{-1} = e \in H$, luego $x \sim x$, o sea, $\sim$ es reflexiva.

Supongamos que $x \sim y$, es decir, $xy^{-1} \in H$, pero como H es subgrupo, es cerrado bajo inversos, luego

$$yx^{-1} = (y^{-1})^{-1} x^{-1} = (xy^{-1})^{-1} \in H.$$

Esto prueba la simetría de $\sim$.

Por último, si $x \sim y$ y $y \sim z$,

$$xy^{-1} \in H \text{ y } yz^{-1} \in H,$$

y como H es cerrado bajo productos,

$$xz^{-1} = (xy^{-1})(yz^{-1}) \in H.$$

Luego $\sim$ es transitiva. □

Obsérvese que para demostrar que $\sim$ es relación de equivalencia, hemos usado todas las condiciones que definen un subgrupo.

DEFINICIÓN 5.9. Las clases de equivalencia de la relación de congruencia módulo H se denominan *clases laterales*.

La clase de a se denota Ha.

La notación anterior se justifica ya que la clase de a está dada por

$$\{x : xa^{-1} \in H\} = \{ha : h \in H\},$$

es decir, los elementos de la clase de a son de la forma "un elemento de H por a". Por ejemplo, la clase del elemento neutro e es

$$He = H.$$

Observemos que en notación aditiva la clase sería $H + a$ y como la operación se supone conmutativa, esto es lo mismo que $a + H$, que fue la notación empleada en el Capítulo 3 para la relación análoga, es decir, esta notación es consistente con la anterior.

LEMA 5.21. *Si $H \leq G$, $a \in G$, entonces*

$$|Ha| = |H|.$$

DEMOSTRACIÓN. Definimos

$$\begin{aligned} f : H &\longrightarrow Ha \\ h &\longmapsto ha. \end{aligned}$$

f es inyectiva ya que por la ley de cancelación, Si $ha = h'a$, entonces $h = h'$.

f es sobreyectiva ya que si $x \in Ha$, existe $h \in H$ tal que

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

□

OBSERVACIÓN 5.1. Las clases laterales que hemos definido en esta sección habitualmente se llaman *clases laterales derechas* ya que la clase de a se obtiene operando por la derecha todos los elementos de H por a.

Esto resultó de la relación de equivalencia usada. Si definimos

$$x \sim y \text{ si y sólo si } x^{-1}y \in H,$$

esta también es una relación de equivalencia. La única diferencia es que la clase de equivalencia de a ahora es

$$\{x : a^{-1}x \in H\} = \{ah : h \in H\}.$$

Estas se denominan *clases laterales izquierdas*.

Resulta claro que el teorema 5.21 es también valido para clases izquierdas, es decir, toda clase lateral, izquierda o derecha, tiene la misma cardinalidad que H.

Debemos hacer notar que en general, las clases laterales izquierdas y derechas no coinciden. Por ejemplo, si consideramos el subgrupo $H = \{Id, \mu_1\}$ de S_3, entonces las clases laterales derechas son

$$\{Id, \mu_1\},\ \{\rho, \mu_2\},\ \{\rho^2, \mu_3\},$$

y las clases laterales izquierdas son

$$\{Id, \mu_1\},\ \{\rho, \mu_3\},\ \{\rho^2, \mu_2\}.$$

TEOREMA 5.22. **Teorema de Lagrange**
Si G es un grupo finito y $H \leq G$, entonces $|H| \mid |G|$.

DEMOSTRACIÓN. Como $\sim$ es una relación de equivalencia, las clases laterales forman una partición de G. Además, como G es finito y cada clase es no vacía, hay un numero finito de clases, es decir,

$$G = Ha_1 \cup Ha_2 \cup \cdots \cup Ha_k,$$

para algún entero positivo k. Como las clases son disjuntas, esto implica que

$$|G| = |Ha_1| + |Ha_2| + \cdots + |Ha_k|,$$

luego

$$|G| = k|H|,$$

lo que termina la demostración. □

DEFINICIÓN 5.10. Sea G un grupo.

(1) El número de elementos de G, denotado $|G|$, se llama el *orden* de G.
(2) Si $H \leq G$, el *índice de H en G*, denotado $(G : H)$, es el número de clases laterales (izquierdas o derechas) módulo H.

COROLARIO 5.23. *Si G es un grupo finito y $H \leq G$, entonces*

$$(G : H) = \frac{|G|}{|H|}.$$

El recíproco del teorema de Lagrange no es verdadero, es decir, si n divide al orden de un grupo, este no necesariamente tiene un subgrupo de orden n. El contraejemplo más pequeño es el grupo alternante A_4, cuyo orden es 12 pero que no tiene subgrupos de orden 6.

Hay varios teoremas que dan respuesta parcial al recíproco del teorema de Lagrange. Mencionaremos algunos sin dar sus demostraciones, las que escapan al plan de esta obra. El lector interesado puede encontrarlas en [**2**].

TEOREMA 5.24. *Si G es un grupo finito conmutativo y $m \mid |G|$, entonces existe un subgrupo H de G talque $|H| = m$.*

TEOREMA 5.25. **Teorema de Cauchy**
Si G es un grupo finito y $p \mid |G|$, p primo, entonces G tiene un elemento de orden p. (Y por lo tanto contiene un subgrupo de orden p).

TEOREMA 5.26. **Teorema de Sylow**
Si $|G| = p^n m$ donde p es primo y $(p, m) = 1$, entonces G tiene subgrupos de orden p, $p^2, \ldots, p^n$.

4. Grupos Cíclicos

DEFINICIÓN 5.11. Un grupo G se dice *cíclico* si existe un elemento $a \in G$ tal que el subgrupo generado por a es todo G.

Observemos que como caso particular del teorema 5.19, el grupo cíclico generado por a está dado por

$$\{a^n : n \in \mathbb{Z}\}.$$

DEFINICIÓN 5.12. El *orden* de un elemento $a \in G$, denotado $|a|$, es el menor entero K tal que $a^k = e$.

TEOREMA 5.27. *Si $a \in G$, entonces $|a|$ es el orden del grupo cíclico generado por a.*

COROLARIO 5.28. *Si G es finito y $a \in G$, entonces $|a| \mid |G|$.*

COROLARIO 5.29. *Si $|G| = n$ y $a \in G$, entonces $a^n = e$.*

DEMOSTRACIÓN. Como $|a| \mid |G|$, existe entero k tal que $n = |a|k$, luego

$$a^n = a^{|a|k} = (a^{|a|})^k = e^k = e.$$

□

COROLARIO 5.30. **Teorema de Euler-Fermat**
Si $(a, n) = 1$, entonces

$$a^{\varphi(n)} \equiv 1 \ (\mod n).$$

DEMOSTRACIÓN. Consideremos el grupo $\mathbb{Z}_n^*$ de las unidades del anillo $\mathbb{Z}_n$. Como vimos en el Capítulo 1, este grupo tiene $\varphi(n)$ elementos.

Ahora bien, como $(a, n) = 1$, $\underline{a} \in \mathbb{Z}_n^*$, por lo tanto

$$\underline{a}^{\varphi(n)} = \underline{1},$$

o lo que es lo mismo,

$$a^{\varphi(n)} \equiv 1 \ (\mod n).$$

□

5. Subgrupos Normales

Si G es un grupo y $H \leq G$, queremos ver la posibilidad de dotar al conjunto de clases laterales módulo H de una operación tal que defina una estructura de grupo. Como en el caso de los anillos, o en el caso particular de las clases residuales estudiado en el Capítulo 1, el punto crucial es que la operación debe estar bien definida, es decir, no debe depender de los representantes de las clases que se está usando.

La definición intuitivamente más natural es:

$$Ha * Hb = Hab.$$

Lo que queremos entonces es que si

$$a_1 \sim a_2 \text{ y } b_1 \sim b_2,$$

entonces

$$Ha_1b_1 \sim Ha_2b_2.$$

Para que esto suceda, como

$$a_1 = ha_2 \text{ y } b_1 = kb_2,$$

para ciertos elementos h y k de H,

$$Ha_1b_1 = Hha_2kb_2 = Ha_2kb_2.$$

Si pudieramos conmutar los elementos a_2 y k tendriamos el resultado requerido. De hecho, bastaría que

$$a_2k = k'a_2$$

para algún $k' \in H$. Como a_2 es arbitrario, lo que se requiere es que para todo $a \in G$

$$Ha = aH.$$

Definición 5.13. Un subgrupo H del grupo G se dice *normal* si y sólo si para todo $g \in G$,

$$gHg^{-1} = H.$$

Si H es un subgrupo normal de G, escribiremos $H \lhd G$.

En realidad, para ver si un subgrupo es normal, basta demostrar que para todo $g \in G$, $gHg^{-1} \subset H$, ya que, entonces también $g^{-1}Hg \subset H$ y obtenemos la otra inclusión, $H \subset gHg^{-1}$.

Otra manera de presentar los subgrupos normales es como aquellos subgrupos para los cuales las clases laterales izquierdas y derechas coinciden. Más precisamente para cada $g \in G$,

$$Hg = gH.$$

Debe notarse que esta es una igualdad entre conjuntos, no estamos afirmando que para cada $h \in H$, $hg = gh$, sino que

$$hg \in gH \text{ y } gh \in Hg,$$

o bien, para cada $h \in H$, existen h', $h" \in H$ tales que

$$hg = gh' \text{ y } gh = h"g.$$

EJEMPLOS 5.5. (1) Si G es abeliano, entonces todo subgrupo es normal.
(2) Si $H = \{Id, \rho, \rho^2, \rho^3\}$, entonces $H \lhd D_4$.
(3) Si $H = \{Id, \mu_1\}$, entonces H no es un subgrupo normal de D_4 ya que

$$\rho\mu_1\rho^{-1} = \mu_2 \notin H.$$

(4) $A_n \lhd S_n$.

TEOREMA 5.31. *Sean G un grupo y $H \leq G$ tales que $(G : H) = 2$. Entonces $H \lhd G$.*

DEMOSTRACIÓN. Como $(G : H) = 2$, hay sólo dos clases laterales derechas y también hay sólo dos clases laterales izquierdas. Como H es una de ellas en ambos casos la otra clase lateral, ya sea izquierda o derecha es el complemento de H. Por lo tanto las clases laterales son H y H'.

Si $a \in H$, entonces $Ha = H = aH$.

Si $a \notin H$, entonces $Ha = H' = aH$, en cualquier caso,

$$Ha = aH,$$

luego el subgrupo es normal. □

TEOREMA 5.32. *Si $H \lhd G$, entonces*

$$G \,/\, H = \{Ha : a \in G\},$$

dotado de la operación

$$HaHb = Hab,$$

es un grupo llamado el grupo cuociente de G por H. El neutro de este grupo es

$$He = H,$$

y el inverso es

$$(Ha)^{-1} = Ha^{-1}.$$

Si G es abeliano, $G \,/\, H$, también lo es.

DEMOSTRACIÓN. Lo más importante es hacer notar que la operación está bien definida, pero eso es precisamente lo que motivó nuestra definición de subgrupo normal así es que eso está demostrado. El resto es trivial. □

6. Homomorfismos

DEFINICIÓN 5.14. Sean G y H dos grupos. Una función $f : G \longrightarrow H$ es un *homomorfismo* si y sólo si

$$f(xy) = f(x)f(y).$$

Al igual que en el caso de los anillos, usaremos las conceptos de monomorfismo, epimorfismo e isomorfismo.

EJEMPLOS 5.6. (1)

$$\begin{array}{rcl} f : \mathbb{Z} & \longrightarrow & \mathbb{Z}_n \\ k & \longmapsto & \underline{k} \end{array}$$

(2)

$$\begin{array}{rcl} f : G & \longrightarrow & G \\ g & \longmapsto & g. \end{array}$$

(3)

$$\begin{array}{rcl} f : G & \longrightarrow & H \\ g & \longmapsto & e, \end{array}$$

donde H es un grupo cualquiera. Este se llama el *homomorfismo trivial*.

(4)

$$\begin{array}{rcl} f : \mathbb{Z} & \longrightarrow & \mathbb{Z}_2 \\ n & \longmapsto & \begin{cases} 0 & \text{si } n \text{ es par,} \\ 1 & \text{si } n \text{ es impar.} \end{cases} \end{array}$$

(5)

$$\begin{array}{rcl} f : \mathbb{R} & \longrightarrow & \mathbb{C}^* \\ x & \longmapsto & cos\, x + isen\, x. \end{array}$$

(6)

$$\begin{array}{rcl} f : \{-1, 1\} & \longrightarrow & \mathbb{Z}_2 \\ n & \longmapsto & \begin{cases} 0 & \text{si } n \text{ es par,} \\ 1 & \text{si } n \text{ es impar.} \end{cases} \end{array}$$

(7)

$$\begin{array}{rcl} f : \mathbb{R}^+ & \longrightarrow & \langle \mathbb{R}, + \rangle \\ x & \longmapsto & log\, x, \end{array}$$

donde R^+ es el grupo de los números reales positivos con la multiplicación como operación.

(8)

$$\begin{aligned} f : GL_n(\mathbb{R}) &\longrightarrow \mathbb{R}^* \\ A &\longmapsto det\ (A). \end{aligned}$$

(9)

$$\begin{aligned} T_a : G &\longrightarrow G \\ g &\longmapsto ag. \end{aligned}$$

Este último ejemplo es particularmente interesante. Si definimos

$$L(G) = \{T_a : a \in G\},$$

y llamamos $S(G)$ al conjunto de todas las permutaciones de los elementos de G, entonces

$$L(G) \leq S(G).$$

En efecto, resulta obvio que para cualquier $a \in G$, T_a es inyectiva. Además, si $g \in G$, entonces

$$g = aa^{-1}g = T_a(a^{-1}g),$$

luego T_a es sobreyectiva, o sea, T_a es una permutación de los elementos de G, es decir, $L(G) \subset S(G)$.

También es claro que $L(G) \neq \emptyset$.

Por último, si T_a, $T_b \in L(G)$, entonces

$$(T_b)^{-1} = T_{b^{-1}} \in S(L),$$

ya que para todo x

$$T_b \circ T_{b^{-1}}(x) = T_b(b^{-1}x) = bb^{-1}x = x,$$

$$T_{b^{-1}} \circ T_b(x) = T_{b^{-1}}(bx) = b^{-1}bx = x,$$

además, como

$$T_a \circ T_b(x) = T_a(bx) = (ab)x = T_{ab}(x),$$

o sea,

$$T_a \circ T_b = T_{ab} \in S(L),$$

y por el teorema 5.16 $L(G) \leq S(G)$.

Esto nos permite demostrar un famoso teorema.

TEOREMA 5.33. **Teorema de Cayley**
Todo grupo es isomorfo a un subgrupo de un grupo de permutaciones.

DEMOSTRACIÓN. Definimos el isomorfismo de la manera obvia:

$$\begin{aligned} \Phi : G &\longrightarrow L(G) \\ a &\longmapsto T_a. \end{aligned}$$

Φ es inyectiva ya que si

$$\Phi(a) = \Phi(b),$$
$$T_a = T_b,$$

luego evaluando en e,

$$a = ae = T_a(e) = T_b(e) = be = b.$$

Φ es obviamente sobreyectiva, puesto que para cada $a \in G$,

$$T_a = \Phi(a).$$

Para verificar que Φ es un homomorfismo, como vimos en el párrafo anterior,

$$\Phi(ab) = T_{ab} = T_a \circ T_b.$$

Por lo tanto, G es isomorfo a $L(G)$ que es un subgrupo del grupo de permutaciones $S(G)$. □

TEOREMA 5.34. *Si $f : G \longrightarrow H$ es un homomorfismo,*

(1) $f(e) = e$
(2) $f(a^{-1}) = (f(a))^{-1}$

DEMOSTRACIÓN. Para demostrar 1),

$$f(e) = f(ee) = f(e)f(e).$$

Multiplicando por $(f(e))^{-1}$ a cada lado,

$$e = f(e).$$

Para demostrar 2),

$$f(a)f(a^{-1}) = f(aa^{-1}) = f(e) = e$$

y

$$f(a^{-1})f(a) = f(a^{-1}a) = f(e) = e,$$

o sea

$$f(a^{-1}) = (f(a))^{-1}.$$

□

DEFINICIÓN 5.15. Si G y H son dos grupos y $f : G \longrightarrow H$ es un homomorfismo,

(1)
$$ker\ f = \{g \in G : f(g) = e\}$$
es el *núcleo* o *kernel* de f.

(2)
$$Im\ f = \{f(g) : g \in G\}$$
es la *imagen* de G por f.

TEOREMA 5.35. *Si $f : G \longrightarrow H$ es homomorfismo, entonces*

(1) $ker\ f \lhd G$.
(2) $Im\ f \leq H$.

DEMOSTRACIÓN. 1) En primer lugar, como $e \in ker\ f$, éste no es vacío.

Sean a y b dos elementos del kernel de f. Entonces
$$f(ab^{-1}) = f(a)(f(b))^{-1} = ee = e,$$
luego $ab^{-1} \in ker\ f$ y por el teorema 5.16, $ker\ f \leq G$.

Para ver que $ker\ f$ es normal, sea $a \in ker\ f$ y $g \in G$, entonces
$$f(gag^{-1}) = f(g)f(a)(f(g))^{-1} = f(g)e(f(g))^{-1} = f(g)(f(g))^{-1} = e,$$
luego $gag^{-1} \in ker\ f$, es decir,
$$g\ ker\ f\ g^{-1} \subseteq ker\ f,$$
y el subgrupo es normal.

2) Como $f(e) = e$, $Im\ f$ no es vacío.

Sean h y k elementos de $Im\ f$. Entonces existen $a, b \in G$ tales que
$$h = f(a) \ \text{ y } \ k = f(b).$$
Por lo tanto
$$hk^{-1} = f(a)(f(b))^{-1} = f(ab^{-1}) \in Im\ f,$$
luego $Im\ f \leq H$. □

Luego de demostrar el teorema anterior, resulta natural preguntarse si $Im\ f$ es o no un subgrupo normal de H. El siguiente ejemplo responde esta pregunta.

EJEMPLOS 5.7. Consideremos la función
$$\begin{array}{rcl} f : \mathbb{Z}_2 & \longrightarrow & S_3 \\ n & \longmapsto & \begin{cases} Id & \text{si } n = 0, \\ \mu_1 & \text{si } n = 1. \end{cases} \end{array}$$
f es un homomorfismo sin embargo, como vimos en los ejemplos, $Im\ f$ no es un subgrupo normal de S_3.

TEOREMA 5.36. *Sea G un grupo y $N \lhd G$. Entonces*
$$\begin{array}{rcl} \Phi : G & \longrightarrow & G\ /\ N \\ g & \longmapsto & Ng \end{array}$$
es un homomorfismo.

El núcleo de este homomorfismo es N.

DEMOSTRACIÓN. Es claro que Φ es un homomorfismo ya que

$$\Phi(ab) = Nab = Na\ Nb = \Phi(a)\Phi(b).$$

Para encontrar el núcleo de Φ, notemos que $x \in ker\ \Phi$ si y sólo si $\Phi(x) = Nx = N$ si y sólo si $x \in N$. □

TEOREMA 5.37. *Sea $f : G \longrightarrow H$ un homomorfismo, entonces*

$$f \text{ es inyectiva si y sólo si } ker\ f = \{e\}.$$

DEMOSTRACIÓN. Supongamos que f es inyectiva. Entonces si $a \in ker\ f$,

$$f(a) = e = f(e),$$

luego $a = e$, o sea,

$$ker\ f = \{e\}.$$

Supongamos ahora que $ker\ f = \{e\}$. Entonces Si $f(a) = f(b)$,

$$f(a)(f(b))^{-1} = f(ab^{-1}) = e,$$

o sea,

$$ab^{-1} \in ker\ f = \{e\},$$

y entonces $a = b$, por lo tanto f es inyectiva. □

TEOREMA 5.38. *Sean G y H grupos, $f : G \longrightarrow H$ un homomorfismo. Entonces*

$$G\ /\ ker\ f \cong Im\ f.$$

DEMOSTRACIÓN. Para abreviar escribamos $N = ker\ f$ y definamos la función

$$\begin{aligned} \varphi : G\ /\ N &\longrightarrow Im\ f \\ Na &\longmapsto f(a). \end{aligned}$$

Entonces

$$\begin{aligned} \varphi(Na) = \varphi(Nb) \quad &\text{si y sólo si} \quad f(a) = f(b) \\ &\text{si y sólo si} \quad f(a)(f(b))^{-1} = e \\ &\text{si y sólo si} \quad f(ab^{-1}) = e \\ &\text{si y sólo si} \quad ab^{-1} \in ker\ f \\ &\text{si y sólo si} \quad Na = Nb, \end{aligned}$$

es decir, φ está bien definida ($\Leftarrow$) y es inyectiva ($\Rightarrow$).

Si $b \in Im\ f$, entonces $b = f(a)$ para algún $a \in G$. Por lo tanto

$$b = \varphi(Na),$$

y φ es sobreyectiva. □

COROLARIO 5.39. *Si G es un grupo finito y $f : G \longrightarrow H$ es un homomorfismo, entonces*

$$|G| = |Im\ f| \cdot |ker\ f|.$$

DEMOSTRACIÓN. Del teorema anterior obtenemos

$$|G\ /\ ker\ f| = |Im\ f|,$$

pero como sabemos

$$|G\ /\ ker\ f| = (G : ker\ f) = \frac{|G|}{|ker\ f|}.$$

□

EJERCICIOS 5.5.

(1) Haga una lista de todos los subgrupos de S_3. ¿Cuáles son normales?

Bibliografía

[1] Birkhoff G. y MacLane S., Algebra Moderna. Editorial Vicens-Vives, Barcelona, 1963.
[2] Fraleigh, J. B., Algebra Abstracta. Editorial Addison-Wesley Iberoamericana, 1988.
[3] Jones, B. J., Teoría de los Números. Editorial Trillas, México, 1969.
[4] Herstein, I. N., Algebra Abstracta. Grupo Editorial Iberoamérica, 1988.
[5] Herstein, I. N., Topics in Algebra.
[6] Hungerford, T.W., Abstract Algebra. An Introduction. Saunders College Publishing, 1990.
[7] Moh, T. T., Algebra. World Scientific Pub. Co., 1992.
[8] Niven, I. y Zuckerman, H. S., Introducción a la Teoría de los Números. Editorial Limusa-Wiley, Mexico, 1969.
[9] Ore, O., Number Theory and its History. MacGraw-Hill, 1948.
[10] Vinogradov, I., Fundamentos de la Teoría de los Números. Mir, Moscú,1971.